P2 Sentinel 4.6
User's Guide

P2 SENTINEL

User's Guide

Third Edition (January 2018)

This edition applies to Version 4.6 of P2 Sentinel and to all subsequent releases and modifications until otherwise indicated in new editions.

Level 1, 1195 Hay Street, West Perth, WA, 6005, Australia
PO Box 305, West Perth, WA, 6005, Australia
Phone +61 8 9241 0300 • Fax +61 8 9242 8121

Contents

Preface

This guide provides users with information on how to use P2 Sentinel.

P2 Sentinel monitors P2 Server entities and tags for compliance with specified thresholds, using a built-in event processing engine. P2 Sentinel automatically raises events when defined conditions are met. This document outlines how to configure and use P2 Sentinel.

Who Should Read This Guide

This guide is intended for those people who use P2 Sentinel to monitor P2 Server tags or entities for compliance with specified thresholds. It assumes working knowledge of:

- P2 Server
- Microsoft® Internet Explorer®

Related Documentation

You can find information on how to use P2 Sentinel in the **Explorer Help Center** at:

https://e4helpcenter.petroleumplace.com/help/sentinel

Other documents in the P2 Sentinel technical documentation suite are:

Title	Description
P2 Sentinel Release Notes	Release Notes for this version of P2 Sentinel.
P2 Sentinel Installation and Administration Guide	Installing P2 Sentinel components and configuring P2 Sentinel.

You may also find the following documents useful:

- P2 A-Plus Sentinel Integration Guide
- P2 Logger User's Guide
- Explorer Security: https://e4helpcenter.petroleumplace.com/help/p2-server/security/

These documents are available from P2 Customer Support.

User's Guide for P2 Sentinel Compatible with P2 Server 4

This User's Guide is intended for users of P2 Sentinel 4.6, compatible with P2 Explorer 4.6.4 or later.

If you are using P2 Sentinel compatible with earlier versions of P2 Explorer (P2 Server), you need to use those guides.

P2 Server 4 and P2 Server 2.6

If you are using P2 Sentinel compatible with P2 Server 2.6, you need the document *P2 Sentinel 4.6 for Server 2.6 User's Guide*, available from P2 Customer Support, instead of this one. If you are using P2 Sentinel compatible with P2 Server 2.6, you need the document *P2 Sentinel 4.6 for Server 2.6 User's Guide*, available from P2 Customer Support, instead of this one.

Help and Support

P2 Customer Support provides a central point of contact for software assistance and the resolution of software issues. As part of this, P2 Energy Solutions Pty Ltd offers a variety of professional services, online resources, and access to experienced product specialists who are able to assist with your service requests. For support and information regarding our products, the following resources are provided:

Free Documentation Resources

- PDF documentation supplied in the installation directory.
- Online help provided with the product (if supplied).

Online Support Portal

The P2 Support Portal (http://p2energysolutions.com/support) provides access to online support, where you can raise service requests for P2 software, track defects, get product information, and communicate with P2 Customer Support.

Customer Communities

P2's customer communities offer a networking environment for you and other P2 users. Our boards and user groups offer an informal setting to exchange information and discuss issues relevant to today's oil and gas companies. P2 is confident that together, we can create an interactive venue that will provide value by allowing our customers to communicate, collaborate and connect at multiple levels. For details, see www.p2energysolutions.com/services/customer-communities.

Training

P2 Energy Solutions Pty Ltd offers a variety of standard and customised training courses (ranging from introductory courses through to administrator courses) to help you learn how to use P2 products.

Contact Details

You can contact P2 Customer Support via phone or through the Customer Portal for technical support on any aspect of P2 Energy Solutions Pty Ltd's products. Please also contact P2 Customer Support for further information on the Customer Communities, access to the online support portal, and information on available training courses.

Phone:	1300 739 969 (Australia only) +61 8 9241 0314 (outside Australia)
Support Portal	https://p2energysolutions.secure.force.com/

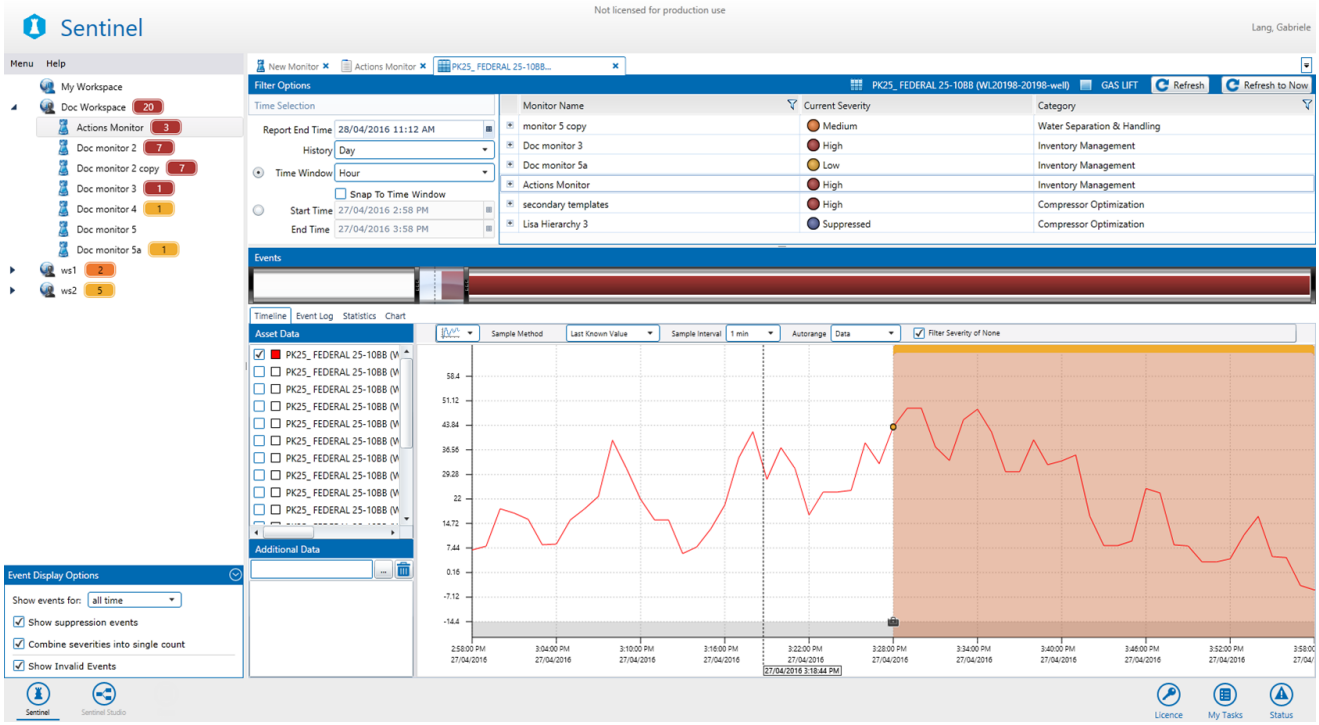
Introduction

P2 Sentinel's intelligent real-time Complex Event Processing engine rapidly accesses and analyses vast amounts of data from disparate sources, using the P2 Server Data Dictionary. P2 Sentinel provides event notification, as well as detailed reports, timelines, event views and statistics.

P2 Sentinel generates an event when an entity value breaches fixed or variable limits, or when specific conditions are met. In the P2 Sentinel interface, tests are defined with limits and conditions, as well as entities to be monitored, using rules defined in a selected P2 Sentinel process. Events give rise to a state; the different states for a test may be ranked by severity.

P2 Sentinel records events in a relational database and, depending on the test configuration, instigates actions: short message service (SMS) or email notifications are sent to designated personnel, or calls to a web service are made. Actions are configured in the interface, and can be prioritised according to state severity. Information associated with the event is stored, facilitating event subscriptions from external applications.

This guide explains how to create and configure monitors, and how to understand the events and reports generated by these monitors.



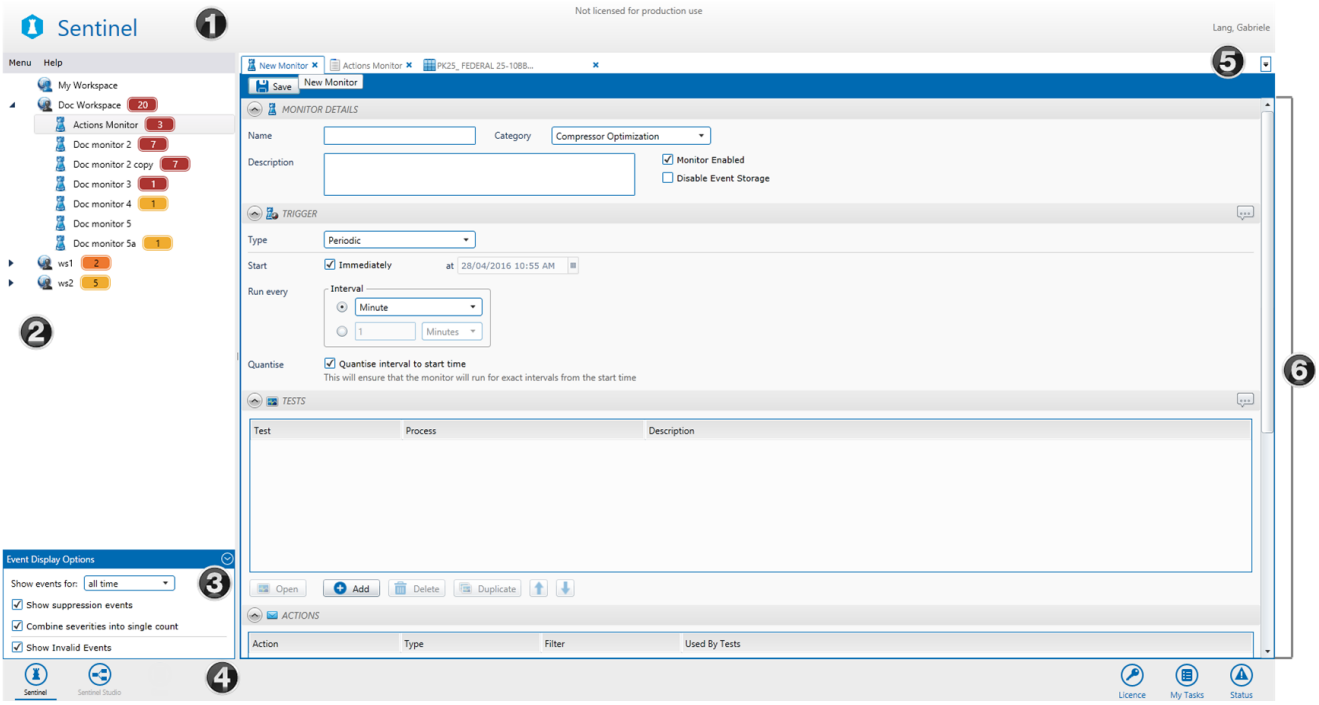
Overview of the Interface

P2 Sentinel runs in the Internet Explorer web browser, and allows you to create and edit workspaces and folders, add entities for monitoring, choose processes for monitoring the entities, set triggers for running tests, set notification conditions, view reports, create custom event views, copy monitors, re-run monitors, and perform export and import functions. From the web interface, you can perform all configuration options for P2 Sentinel.

The URL for accessing P2 Sentinel is:

`https://<ServerName>/Sentinel`

Note: If Sentinel is installed on a different website, the URL is `https://<ServerName>:<port>/Sentinel`. Speak to your System Administrator if you are unsure of what the port number is.



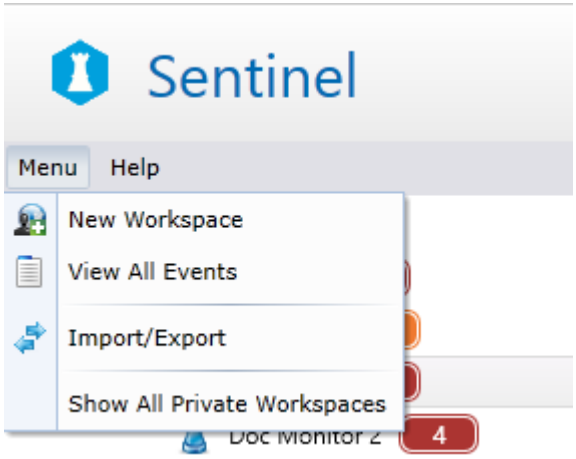
The important features of the P2 Sentinel interface are:

	Feature name	Description
1	Sentinel header	The Sentinel header frames the application at the top and displays the application name and the name of the current user. Clicking the Sentinel icon opens the **About** box, which contains copyright information, as well as product and licence information specific to the current software version. Directly below the header is the **Menu** and the **Help** link.
2	Workspace panel	The list of workspaces, folders, monitors and event views configured in P2 Sentinel. The number of events against each monitor, folder, or workspace is displayed in a coloured label next to each item. The colour of the label is determined by the highest event severity level within the monitor, folder, or workspace. Options on the **Event Display Options** panel allow you to modify the types of events displayed in the coloured labels.

	Feature name	Description
3	Event Display Options	This panel contains various options for which events to show in the workspace panel, and whether to combine the different severities into a single count. Click the collapse button to collapse this panel, and the expand button to expand it again.
4	Sentinel Footer	The Sentinel footer frames the application at the bottom and allows you to switch between Sentinel and Sentinel Studio (the process designer). It provides access to additional information. • Click **Sentinel** to open Sentinel. • Click **Sentinel Studio** to open the process designer. • Click **Status** to see the current P2 Sentinel online/offline status. • Click **My Tasks** to see a list of pending tasks. For example, these could be tasks relating to change management. • Click **Licence** to open the licence tab.
5	Tab strip	This strip contains tabs of every page (for example: monitor, report, pending approvals, licence tab) that you have already opened; each tab has an icon representing what type of page it is. You can view a page by clicking its tab, or click the drop-down list on the far right to navigate to a page.
6	Main panel	The Main panel contains the tabbed pages, for example: monitor details, events, reports, licenses.

Menu and Help

The Menu and Help buttons are directly below the Sentinel header.



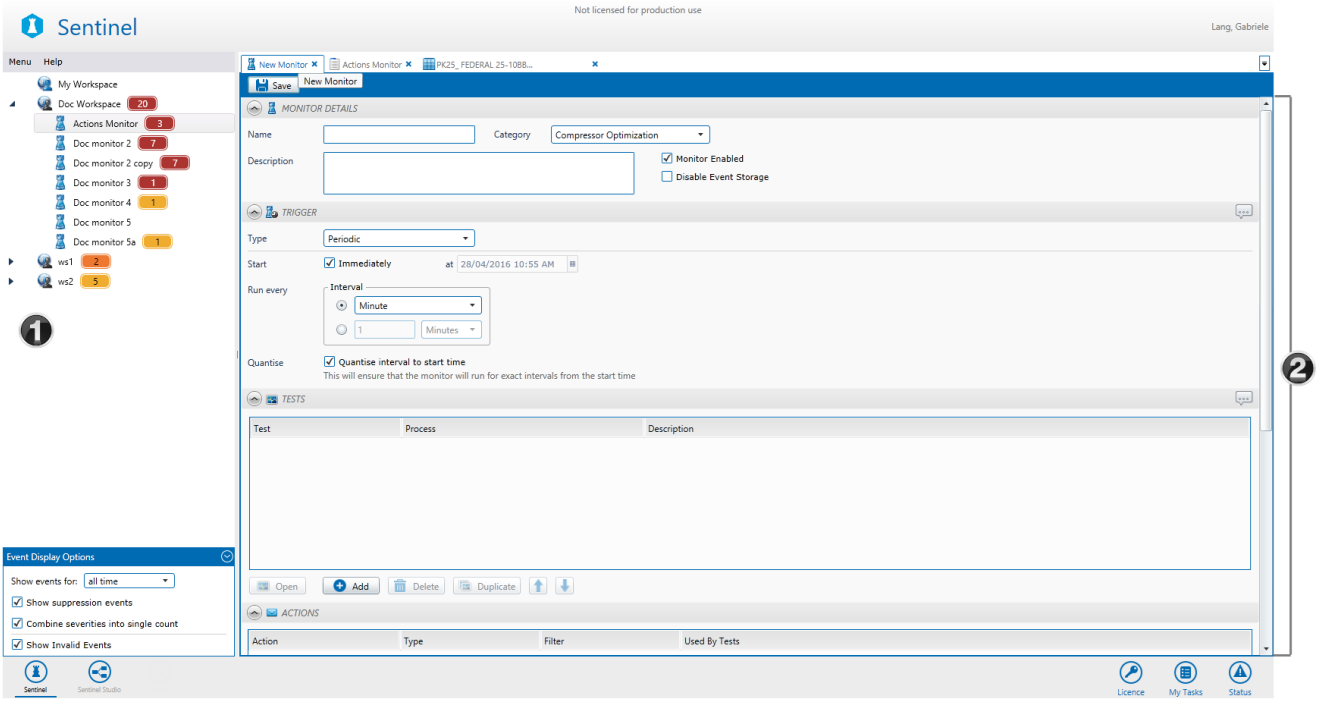
- Click on **Menu** to open the Sentinel menu:
  - New Workspace
  - View All Events
  - Import/Export
  - Show All Private Workspaces

1. Click the **Help** menu for a link to the P2 Sentinel User Guide.
2. Click **View P2 Sentinel User Guide** to open the PDF for the P2 Sentinel User's Guide (this document).

Workspace Panel

The Workspace panel is on the left side of the P2 Sentinel screen.

1. The Workspace panel
2. The Main panel



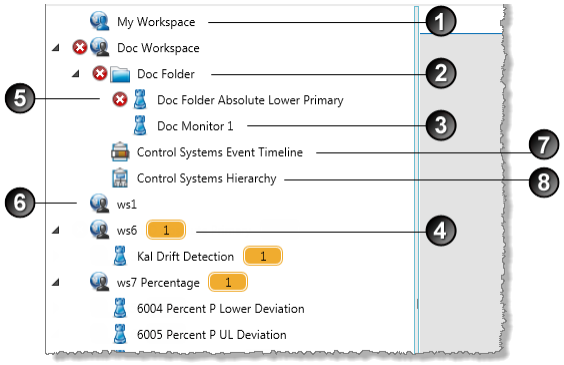
The Workspace panel contains a hierarchical list of all of the P2 Sentinel workspaces, folders, monitors, and event views.

Items in P2 Sentinel are arranged into a logical hierarchy of workspaces and folders.

This hierarchy assists in the management of monitors.

This screen image shows some examples of workspaces, folders, monitors, and event views, and how they are placed within the Workspace panel.

1. My Workspace
2. A folder
3. A monitor
4. An event notification for a workspace
5. A status icon for a monitor
6. A standard workspace
7. An event timeline event view
8. A hierarchy event view



Workspaces are provided as a way for you to logically group monitors and custom event views into a hierarchy that makes sense for your site. Workspaces are described only by a name and description, and you can create as many as you need for your site. Each workspace has its own workspace security roles, and own approver user groups (if Change Management is implemented).

As with a workspace, a folder provides a flexible way to group your monitors and event views in a way that makes sense for your site. Each folder can contain several monitors and event views.

You can move a folder to another folder, or to another workspace, without affecting the configuration of its sub-folders, monitors, and event views.

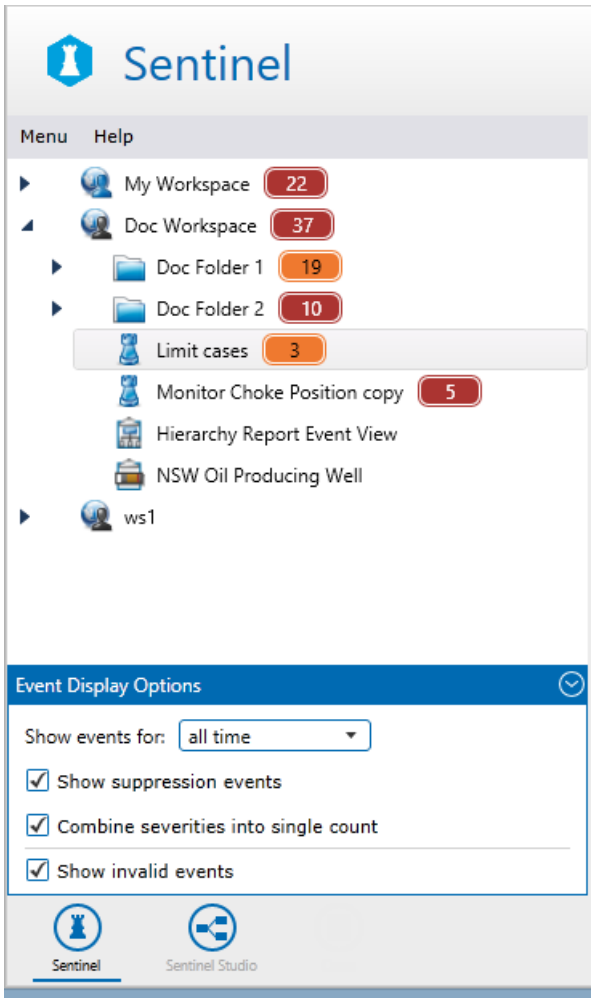
Note: A workspace cannot be moved within the workspace panel, whereas folders, monitors, and event views can. Workspaces are listed in alphabetical order in the workspace panel (apart from the private workspace, *My Workspace*, which is at the top of the workspace panel list). For Sentinel Administrators who have chosen to see all private workspaces, these are ordered alphabetically at the top of the workspace list, below My Workspace, and above all other workspaces.

The workspaces, folders, and monitors also contain the following as part of their label:

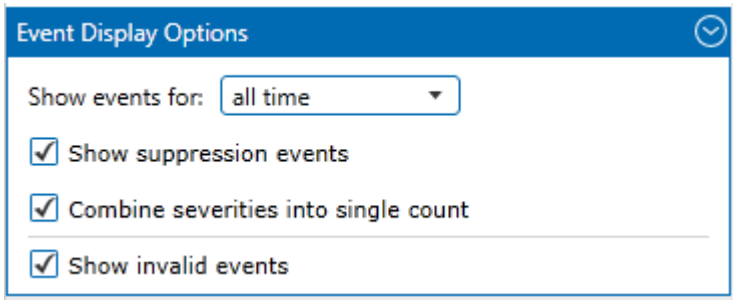
- Event notifications, where there are events.
- Status icons, where there is an error, warning, or information message.

Event Display Options

In the Workspace panel, below the folders and workspaces, there is an ***Event Display Options*** panel. This is expanded by default.



This panel contains different display options that you can use to filter which current events are counted, and how these counts are displayed. The section Adjust Event Display Options, shows which settings you can change.



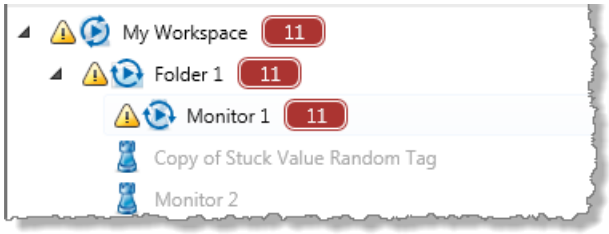
Enabled and Disabled Monitors in the Workspace Panel

A disabled monitor has a grey label in the Workspace panel. In the screenshot below, the monitors "*Copy of Stuck Value Random Tag*" and "*Monitor 2*" are both disabled. By contrast, "*Monitor 1*" has a black label, to indicate that it is enabled.

Monitors Currently Running

A rotating processing icon replaces the workspace icon, to indicate that monitors within this workspace are currently processing data. Folders within this workspace that contain currently processing monitors also have their folder icon replaced by the processing icon, and the actual monitors within these folders have their monitor icon replaced by the processing icon.

The screenshot below demonstrates how a currently processing monitor is traced by following the processing icon from the workstation to the folder to the monitor:



My Workspace

P2 Sentinel has a private workspace called **My Workspace**. This workspace differs from standard workspaces. *My Workspace* is created by the system for each user, and is only visible to that user, as well as to users who have a role with the **Sentinel Admin** privilege. Using *My Workspace* you can create and modify private monitors. When you are ready, you can move the monitor to another workspace where it can be accessed by anyone with privileges for that workspace.

Note the following:

- You cannot delete or edit *My Workspace*.
- Only you and users with the Sentinel Admin privilege can view the events for monitors running in your private workspace.
- You cannot move a monitor or folder from a public workspace to a private workspace.
- Users with the Sentinel Admin privilege are able to move folders and monitors between private workspaces.

Note: You can copy a monitor from another workspace to *My Workspace*.

Change Management

Whether or not Change Management is implemented, the monitor will run under My Workspace. Once you move it to another workspace, the normal rules of Change Management apply, if Change Management is in place.

Summary of Icons in the Workspace Panel

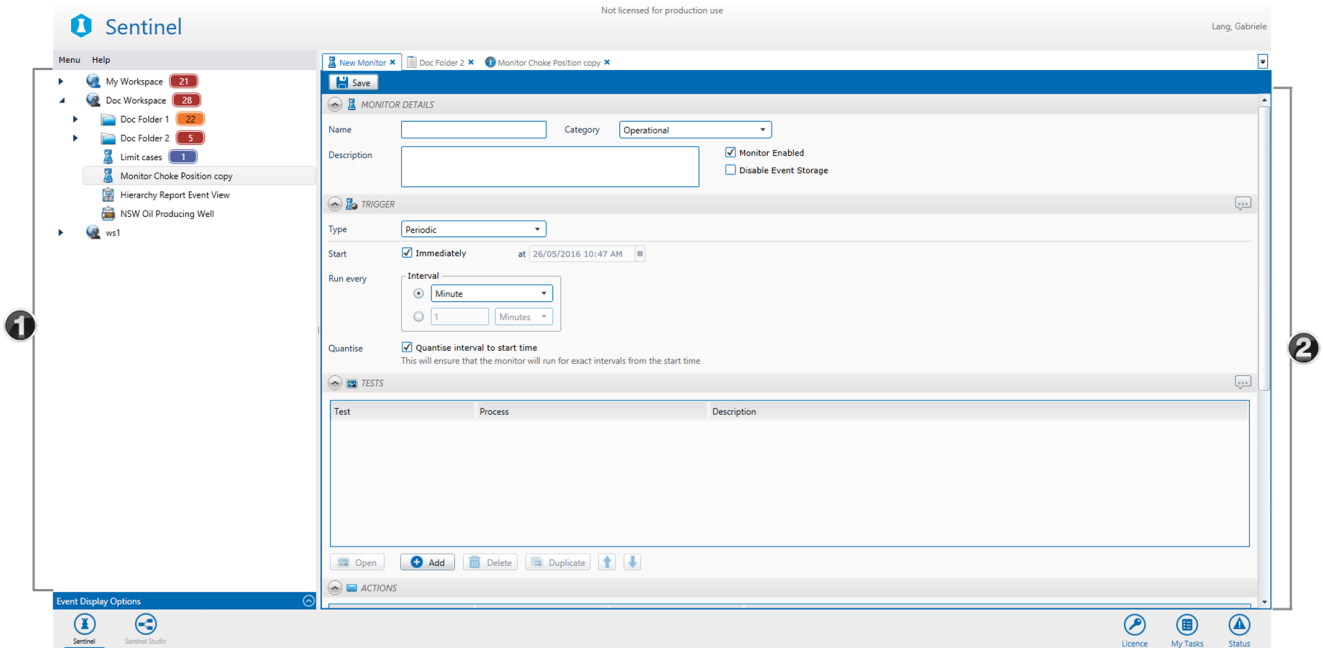
The various icons and labels that are used in the Workspace Panel are summarised in the table below:

Icon	What is represents	Special features / Examples
	Workspace	-
	Private Workspace (for example *My Workspace*)	-
	Folder	-
	Monitor Icon	-
	Status - Stopped	Indicates a stopped monitor within the workspace hierarchy.
	Status - Warning	Indicates a warning for one or more monitors within the workspace hierarchy.
	Processing	The rotating processing icon replaces the workspace, folder or monitor icon to signify a currently processing monitor within the workspace hierarchy.
	Event Notification	Colour based on highest severity event within the group (workspace, folder, monitor); the number indicates total current events (including those with a lower severity). The rules that drive the display of this icon are explained in the section Adjust the Event Display Options.
	Hierarchy Report	-
	Event View	-
	Licence Error	For example, the licence for the process 'Alarm' has expired.

Main Panel

The Main panel forms the right side of the Sentinel screen.

1. The Workspace panel
2. The Main panel



This is where monitors are set up, and also where events are viewed.

In the Main panel, you can:

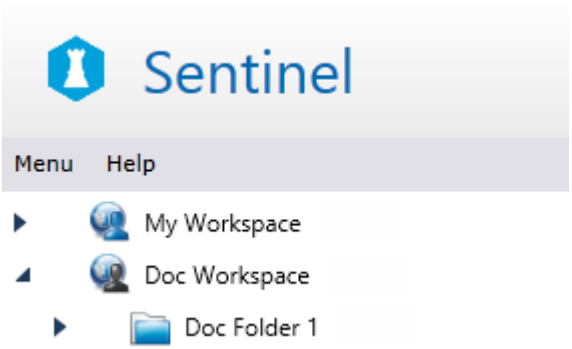
- Add or edit a monitor, submit a monitor for approval, or view the monitor configuration
- Approve monitors
- View events for a workspace, folder, or monitor
- View asset reports
- View monitor status
- Add, edit, or view custom event view reports
- View licence information.

Every time any of these functions are performed, a new tab opens in the Main panel.

About P2 Sentinel

The **About P2 Sentinel** window contains proprietary and version and licence information for P2 Sentinel. If the P2 Sentinel licence is about to expire, the **About P2 Sentinel** window contains a message showing how many days are left until the expiry date.

- To open the **About P2 Sentinel** window, click the Sentinel icon on the Sentinel header.



- To close the window, click the close button in the top right corner, or click the main Sentinel screen.

System Navigation

P2 Sentinel uses several controls throughout the application to perform various common functions. These are:

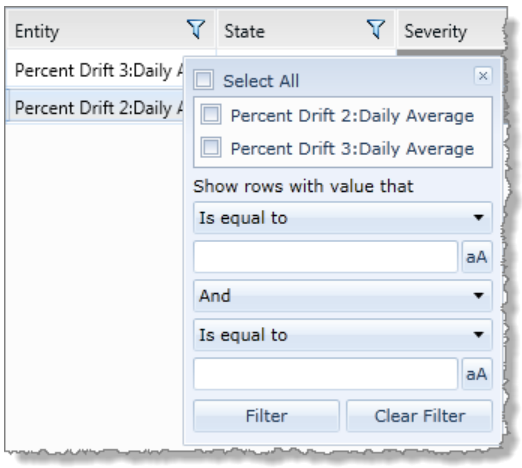
- Filtering
- Selecting a Date and Time
- Sorting Columns
- Grouping by a Column in a Grid
- Expanding and Collapsing Panels
- Exporting to a File
- Using the P2 Server Browser
- Selecting an Open Tab
- Closing Tabs
- Moving Tabs
- Using Panel Comments
- Using Report Hairlines
- Viewing the Licence Tab
- Viewing the Sentinel Status

Filtering

In P2 Sentinel, several column headers offer the ability to filter data according to specified criteria. This is indicated by the filter icon on the column header.

Note: A filtered column has an opaque filter; other filter icons are clear.

- To open the filter box, click the filter icon of a column header.



The filter box offers the following options:

Select All

All available options for this column are listed here. You can choose the *Select All* option, or you can select individual options from the list.

Show rows with value that

This section allows you to type a character or number to compare with the values in the filter column.

Note: If a column contains characters, the text box is followed by an alphabet aA icon. For case-sensitive matching, click on the alphabet icon. If there is no alphabet icon, type a number into the text box.

There are three optional fields to complete:

- Comparison 1
  - Select a comparison operator from the first drop-down list, directly below **Show rows with value that**. For example, *Is equal to*, *Starts with*, *Ends with*, and so on.
  - Type a comparison in the first text box.
- Select **And** or **Or**, if you want to compare two values.
- Comparison 2
  - Select a comparison operator from last drop-down list. For example, *Is equal to*, *Starts with*, *Ends with*, and so on.
  - Type a comparison in the second text box.

Filter

To apply the selected filters and options, click the **Filter** button.

Clear Filter

To clear the selected filters and options, click the **Clear Filter** button.

Close the filter

To close the filter box, click the **Close** button at the top right.

Selecting a Date and Time

To select a date and time:

1. Click the calendar icon next to a date edit box.

   A date and time (clock) panel opens.

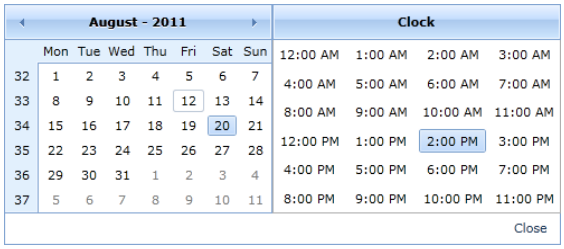
   Note: Where only a time is required, only the Clock panel is shown.

2. In the **Calendar** panel, click a date to select it.

   - Click the right arrow on the header to go forward a month.
   - Click the left arrow on the header to go back a month.

   The selected date is highlighted.

   Note: The current date is outlined.



3. In the **Clock** panel, click a time to select it.
4. Click **Close**.

The date and time panel closes, and the selected date and time appear in the date-time box.

For time selections only, the time is displayed in the time box.

Sorting Columns

Many of the columns in the Sentinel data grids can be sorted in ascending or descending order.

To sort by a column, click the column header to toggle through the various options:

- Click once to sort ascending.
- Click twice to sort descending.
- Click three times to remove sorting.

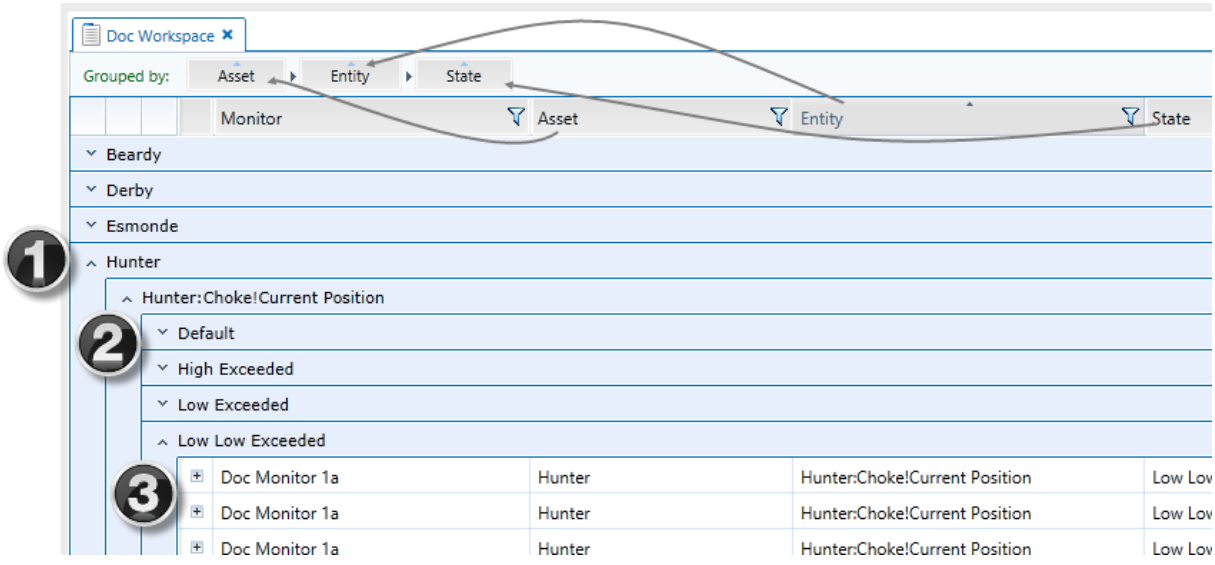
Grouping by a Column in a Grid

In P2 Sentinel, some of the grids have a grouping capability. For example, in the View Events screen you can group by a column header for the following columns:

- Monitor
- Asset
- Entity
- State
- Severity
- Test

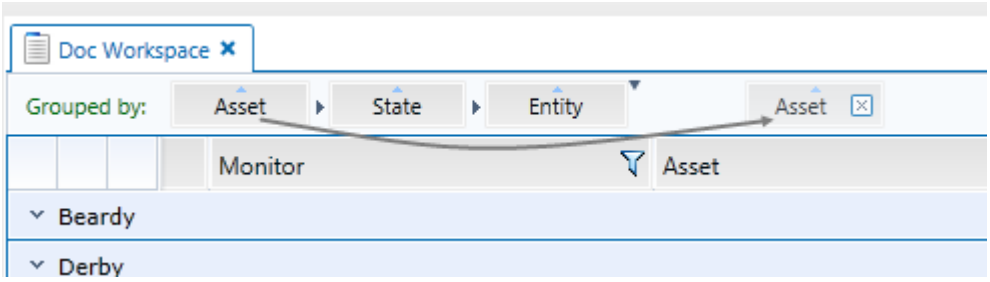
Grouped columns allow you to organise the contents of the grid more easily. For example, if you group by **Asset**, each different asset has a single row in the grid, which you can expand to view the different rows (or groups) within that asset.

In the screenshot below, you can see groupings of Asset, Entity and State. The groupings are nested in the same order that they appear in the grid header panel, with ❶ (Asset) forming the outermost group, ❷ (Entity) showing the middle group, and ❸ (State) showing the inner group. Within the inner group, items appear with full details.



- To group by a column header, click and drag the column header to the grid header (labelled *Grouped By*).
- To expand a grouped section, click the **Expand**, downward-pointing arrow.
- To collapse a grouped section, click the **Collapse**, upward-pointing arrow.
- To remove a grouping, hover over the relevant column grouping button on the header panel that you want to remove, and click the **Close** icon that appears.

- To re-order a column grouping, click and drag a column header button in the table header section, then release it in the new position. This changes the hierarchy of groupings in the grid.



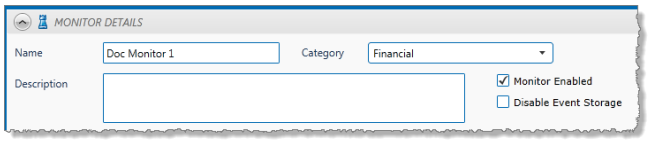
Moving the Asset Column Grouping

Expanding and Collapsing Panels

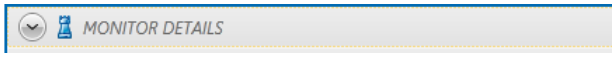
The monitor page, for adding or editing monitors, and the test page, for adding and editing tests, are both made up of many different panels. The different panels can be collapsed when they are not used, and expanded again when needed.

The expand icon / collapse icon is located on the upper left of each panel on a test or monitor page.

- If the panel is expanded, the **collapse** icon is shown.



- If the panel is collapsed, the **expand** icon is shown.



Collapse a Panel

- To collapse a panel, click the **collapse** icon.

The panel collapses to display only the panel title.

Expand a Panel

- Click the **expand** icon.

The panel expands to display the full panel.

Exporting to a File

Some of the Sentinel tables and graphs can be exported to a Microsoft® Excel® spreadsheet, or saved as a .png image file.

Export to a Microsoft Excel Spreadsheet

1. Click **Export to Excel** on the relevant page.

   A **Save As** dialog box opens.

2. Navigate to the folder where you want to save the file.

3. Type a file name in the **File name** box.
4. Click **Save** to save the file.

EXPORT TO AN IMAGE FILE

1. Click **Export to Image** on the relevant page.

   A **Save As** dialog box opens.
2. Navigate to the folder where you want to save the file.
3. Type a file name in the **File name** box.
4. Click **Save** to save the file.

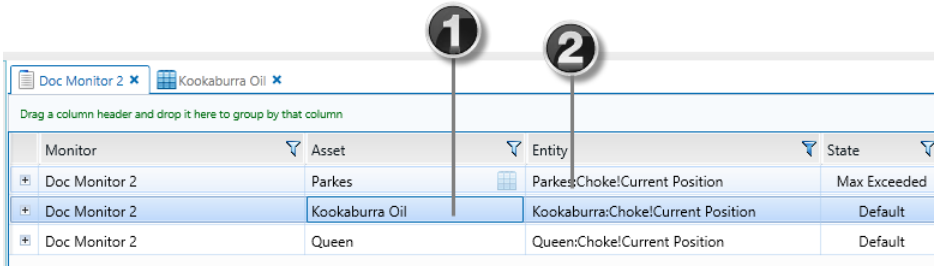
P2 Server Data

Sentinel's data (monitored data, data limits, precondition data, auxiliary data, additional data on the timeline, etc.) is all accessed via P2 Server. Sentinel allows you to browse P2 Server, to access tags or attributes that can be used as is or within calculations. You can also select whole groups of data by selecting hierarchies (whole hierarchies, or hierarchies from a starting point), and you can optionally specify which templates to use, when using attributes.

Entity Name VS Display Name

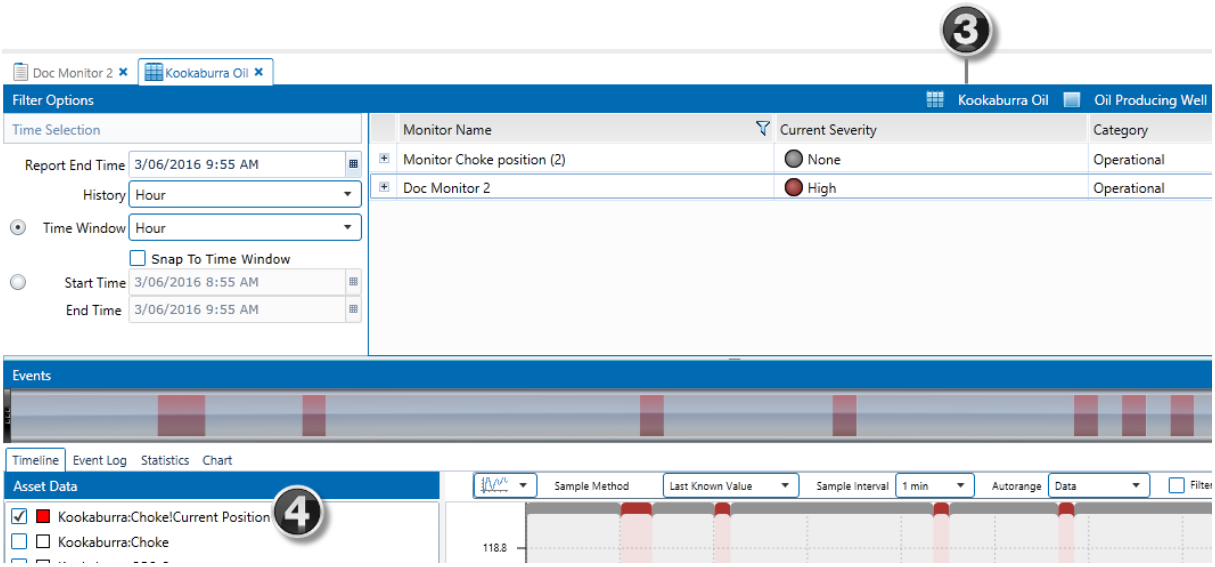
In Server, entities are given a unique name, as well as a more descriptive display name. In Sentinel, the **Display Name** is shown in the P2 Server Browser, and is also displayed as the Asset in the event reports. The **Name** is used in the entity description.

Consider the examples shown below, where the entity with **Name** *Kookaburra* and **Display Name**: *Kookaburra Oil* was used.



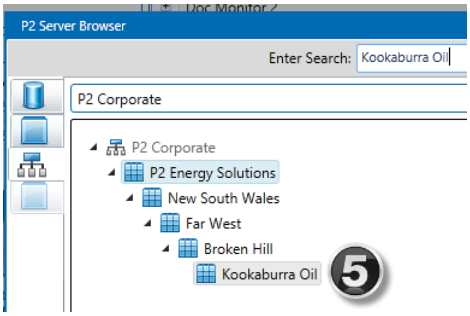
1 The **Asset** shows the **Display Name**.

2 The **Entity** uses the **Name**.



3 The **Display Name** is used for the Asset in the **Asset Report**

4 The **Name** is used as part of the attribute name



5 In **P2 Server Browser**, the **Display Name** appears in the hierarchy.

Accessing Data from P2 Server

P2 Server Browser

P2 Server Browser allows you to browse the P2 Server Data Dictionary for entities, tags and hierarchies, helping you to find them by data source, template, or hierarchy. You can also filter the entities to show only those that match specified criteria.

Note: If Sentinel is configured to cache hierarchies, the latest hierarchy is downloaded and cached at configured intervals (the default is every 30 minutes).

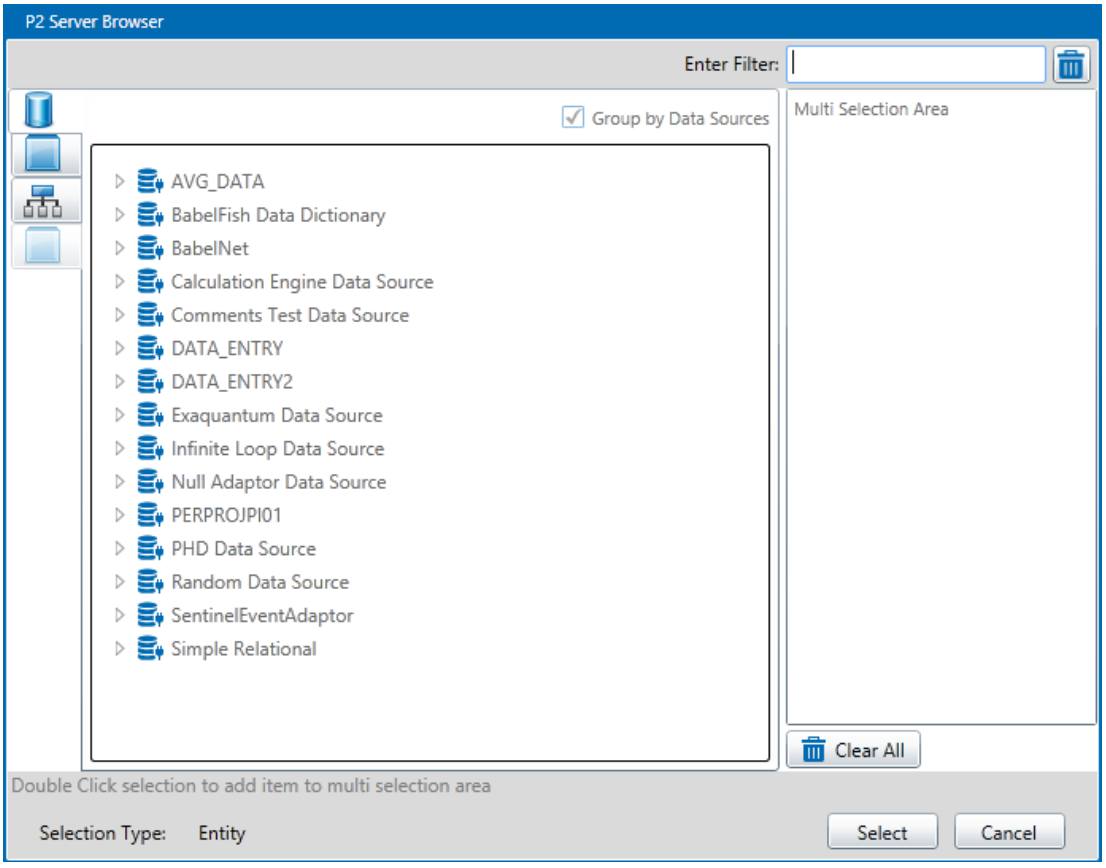
You can access the P2 Server Browser by clicking the ellipsis button next to the field you are editing. You will need to do this when selecting an Entity Name for a Test Source, for example.

Adding an Entity to a Test's Source

The P2 Server Browser allows you to select one or more entities.

- To select an entity, double-click the entity, and it will be added to the Multi Selection Area on the right. Continue adding entities as required, and then click **Select**.

Note: If you have specified a Hierarchy type data source, the Multi Selection Area will not be available.



ENTER FILTER

To restrict the display to only those entities that match the filter criteria, enter part of the name of an entity. This applies across all data sources, templates, and hierarchies. To clear the filter, click the trash can  icon.

DATA SOURCES

When you select the Data Sources tab, the drop-down list displays all the data sources configured in the P2 Server Data Dictionary. You can select a data source from the list and browse its entities, or use the filter to limit the displayed entities.

ENTITIES BY TEMPLATE

When you select the *Template* tab, the drop-down list displays all the templates configured in the P2 Server Data Dictionary. You can select one from the list and browse its entities, or use the filter to limit the displayed entities.

HIERARCHIES

When you select the *Hierarchies* tab, the drop-down list displays all the entity hierarchies configured in the P2 Server Data Dictionary. You can select a hierarchy from the list and browse its entities, or use the filter to limit the displayed entities.

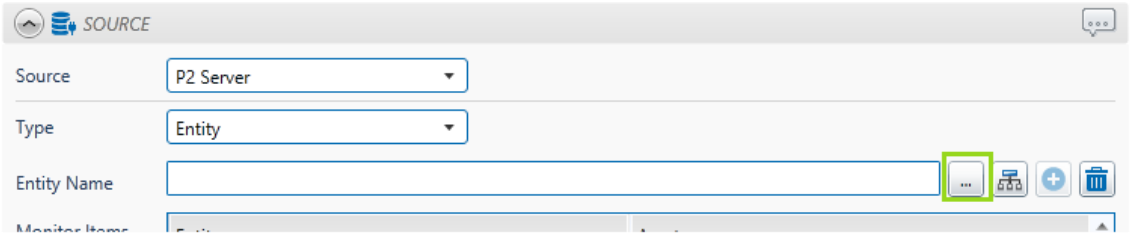
CLEAR ALL

Click the **Clear All** button to clear the current selection.

Selecting Entities

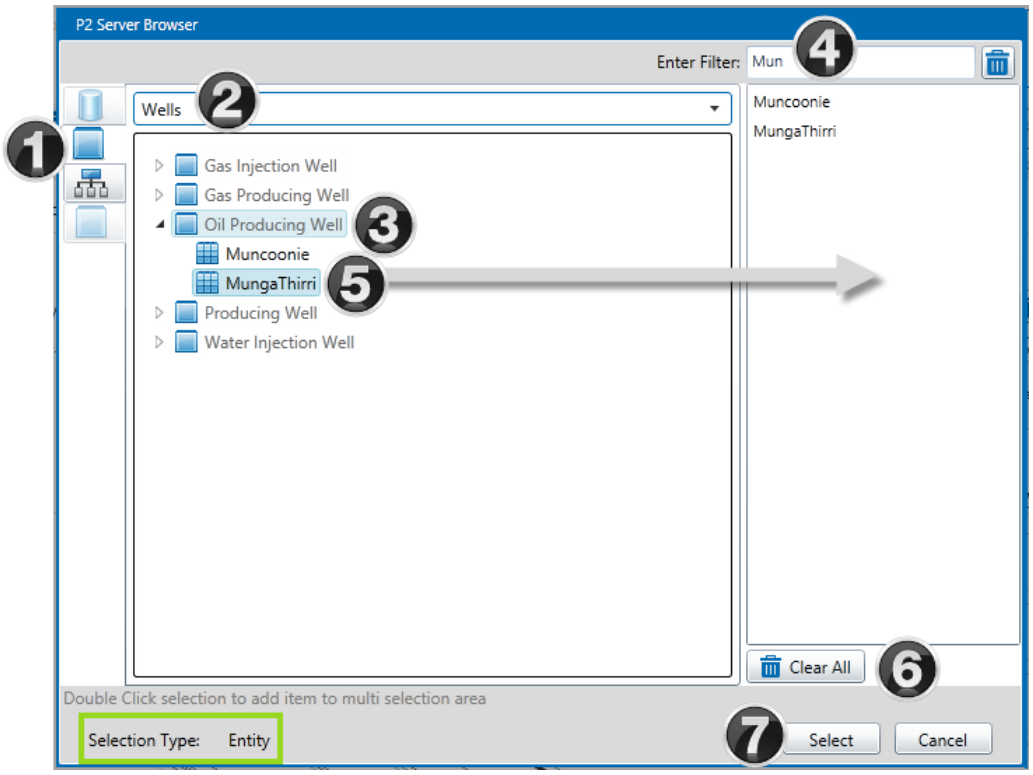
The P2 Server Browser can be used for selecting one or more entities. For example, when you are selecting an *Entity* source for a Test, click the ellipsis button next to Entity Name.

For example, when you are using the *Entity* type for a Test **Source**, click the ellipsis button next to **Entity Name** edit box.



This opens the P2 Server Browser, with the **Selection Type** of *Entity*.

SEARCH FOR ENTITIES BY TEMPLATE



Searching for Entities by Template

1. Click the **Template** button on the left.
2. Select a **Template Group** from the drop-down list.
3. Expand the **Template**, by clicking the little arrow ▷ to its left.
4. Locate an entity:
   a. Either use the filter (as shown). Type some matching letters into the **Enter Search** box. A list of matching entities appears below the expanded template. Scroll through this list to locate an entity.

      OR

b. Scroll through entities listed below the expanded template.

5. Select an entity:

   a. Double-click on an entity. This is added to the multi selection area, on the right.

      Or

   b. Click on an entity, then click **Select** to close the window, with this single entity selected.

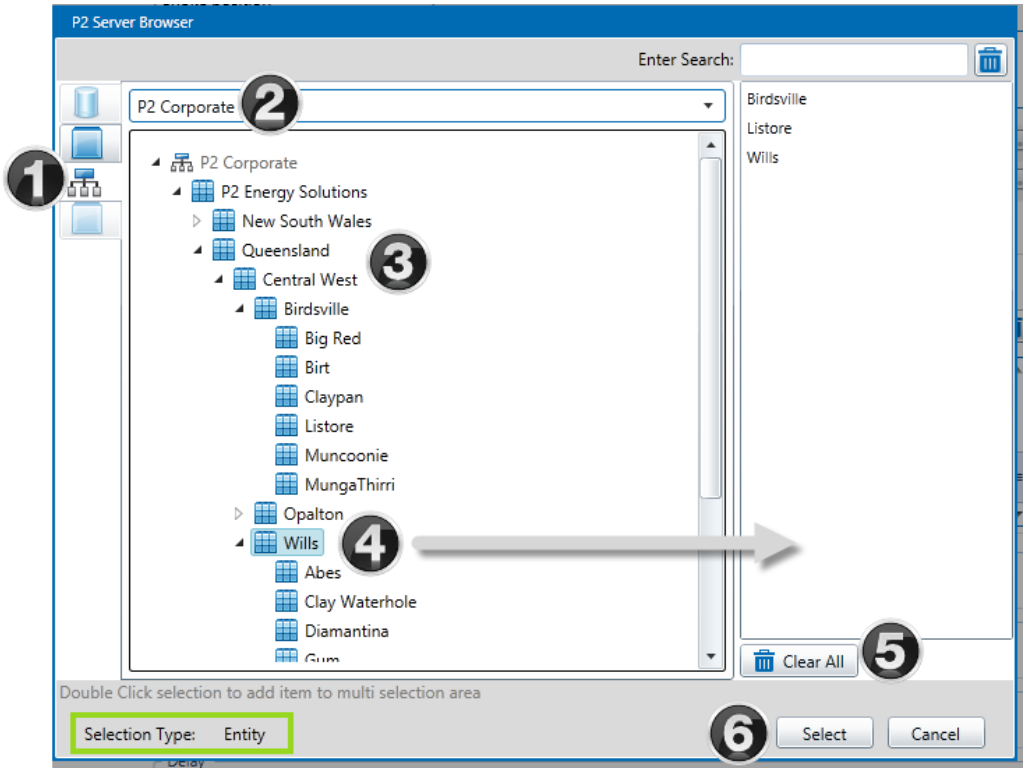
Continue to add entities, until you have all that you want to select.

6. Optionally click **Clear All** to clear the selection of entities from the multi selection area. Or remove a single entity from the list: click on an entity in the list and press the **Delete** key on your keyboard.

7. Click **Select**.

   The window closes and you are returned to the previous window, where the selected entities are added to the list.

SEARCH FOR ENTITIES BY HIERARCHY



Searching for Entities by Hierarchy

1. Click the **Hierarchy** button on the left.

2. Select a **Hierarchy** from the drop-down list.

3. Locate an entity:

   a. Either use the filter (as shown). Type into the **Enter Search** box and select an entity from the search result list. The entity is located on the hierarchy.

      Or

   b. Navigate through the hierarchy by clicking on the arrows next to the entities.

4. Select an entity:

   a. Double-click on an entity. This is added to the multi selection area, on the right.

   Or

   b. Click on an entity, then click **Select** to close the window, with this single entity selected.

Continue to add entities, until you have all that you want to select.

5. Optionally click **Clear All** to clear the selection of entities from the multi selection area. Or remove a single entity from the list: click on an entity in the list and press the **Delete** key on your keyboard.

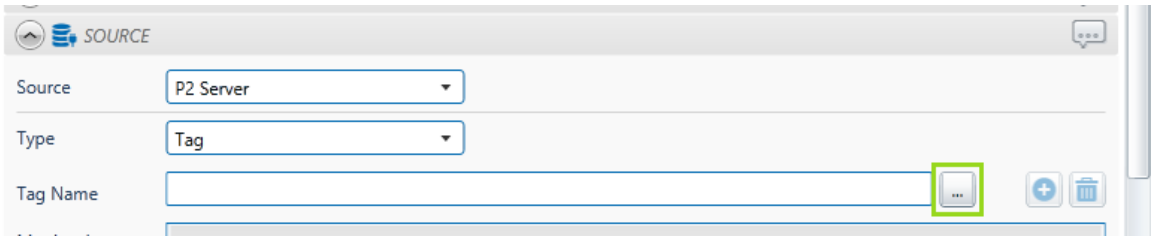
6. Click **Select**.

   The window closes and you are returned to the previous window, where the selected entities are added to the list.

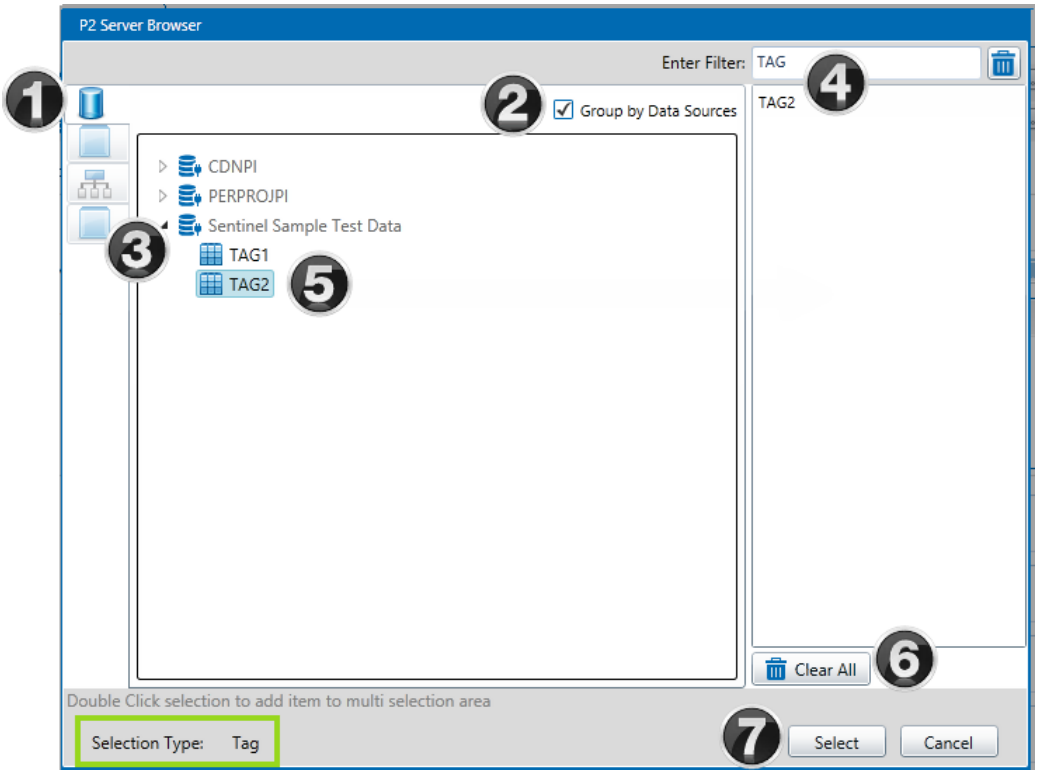
Selecting Tags

The P2 Server Browser can be used for selecting one or more tags.

For example, when you are using the *Tag* type for a Test **Source**, click the ellipsis button next to **Tag Name** edit box.



This opens the **P2 Server Browser**, with the **Selection Type** of *Tag*.



Searching for Tags by Data Sources

1. The **Data Sources** button on the left is already selected.
2. Select the **Group by Data Sources** check box (as shown), or clear it if you want a flat list of tags that are not each grouped under their applicable data source.

   Note: You need to have a filter before you can clear this check box.

3. Expand the **Data Source**, by clicking the little arrow ▷ to its left.

   The tags belonging to this data source are listed alphabetically below the data source.

4. Optionally type a filter into the **Enter Search** box, as shown.
5. Select a tag:

   a. Scroll down the list of tags (filtered or unfiltered) listed below the expanded data source to locate a tag, then double-click on the tag to add it the multi selection area, on the right.

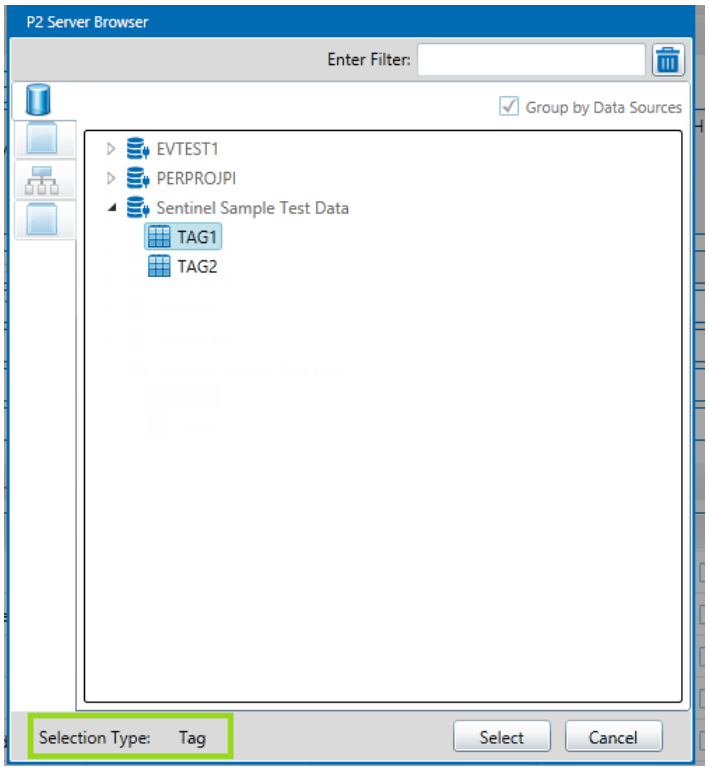
   Or

   b. Click on a tag, then click **Select** to close the window, with this single tag selected.

Continue to add tags, until you have all that you want to select.

6. Optionally click **Clear All** to clear the selection of tags. Or remove a single tag from the list: click on a tag in the list and press the **Delete** key on your keyboard.
7. Click **Select**.

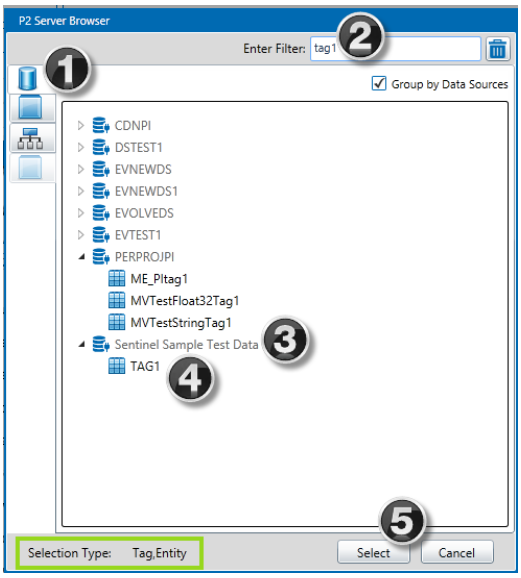
   The window closes and you are returned to the previous window, where the selected tags are added to the list.



Selecting a Single Tag

Selecting Tags or Entities

P2 Server Browser can also be used for selecting either an entity or a tag. For example, if you are adding data to a Timeline report, the P2 Server Browser opens for **Selection Type Tag, Entity**.

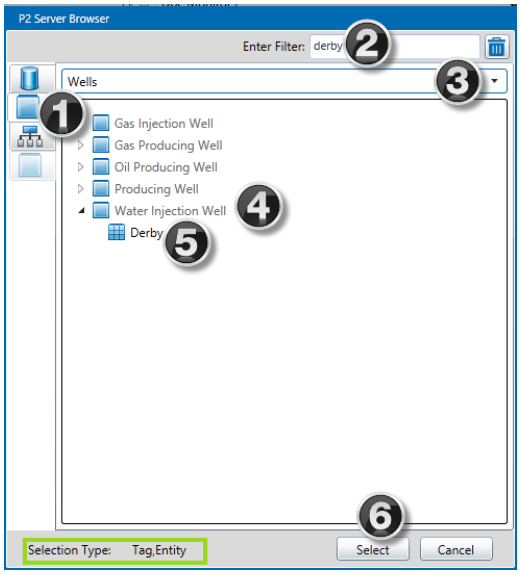


To select a tag:

1. Click the **Data Sources** button on the left.
2. Optionally type filter text into the **Enter Search** box, as shown.
3. Expand a data source (if **Group by Data Sources** is selected) and scroll down the list of tags (filtered or unfiltered) listed to locate your tag.

   Or

   Scroll down the ungrouped list of tags (filtered or unfiltered) to locate your tag.
4. Click on a tag.
5. Click **Select**.



To select an entity (by template):

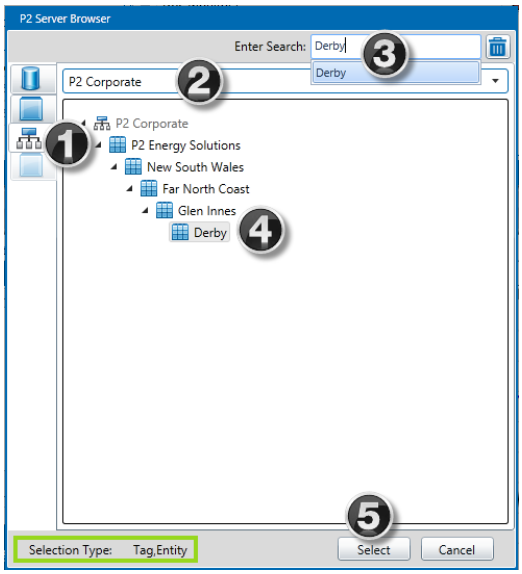
1. Click the **Templates** button on the left.
2. Optionally type filter text into the **Enter Search** box, as shown.
3. Select a template group from the drop-down list
4. Expand a template and scroll down the list of tags (filtered or unfiltered) listed to locate your entity.
5. Click on the entity.
6. Click **Select**.

To select an entity (by hierarchy):

1. Click the **Hierarchies** button on the left.
2. Select a hierarchy from the drop-down list.
3. Optionally type filter text into the **Enter Search** box, as shown, and select from the drop-down list.
4. The entity is auto-selected if there is a search match.

   Or

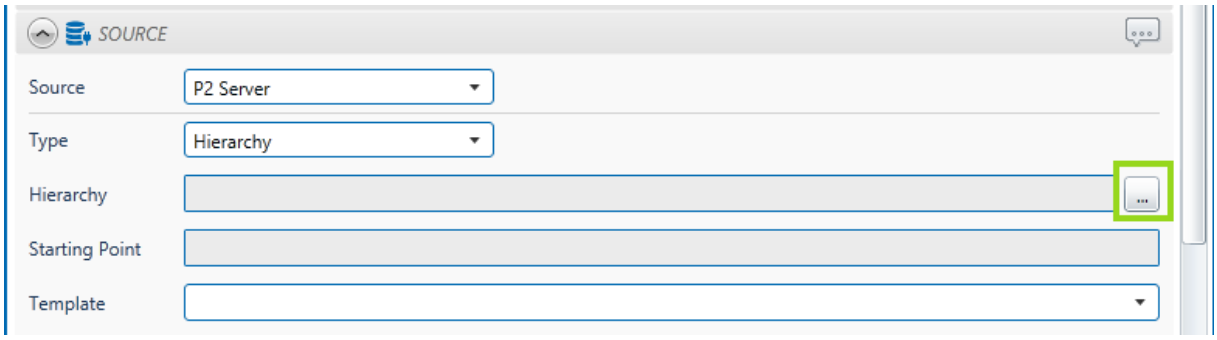
   Navigate through the hierarchies until you locate your entity, then click it.
5. Click **Select**.



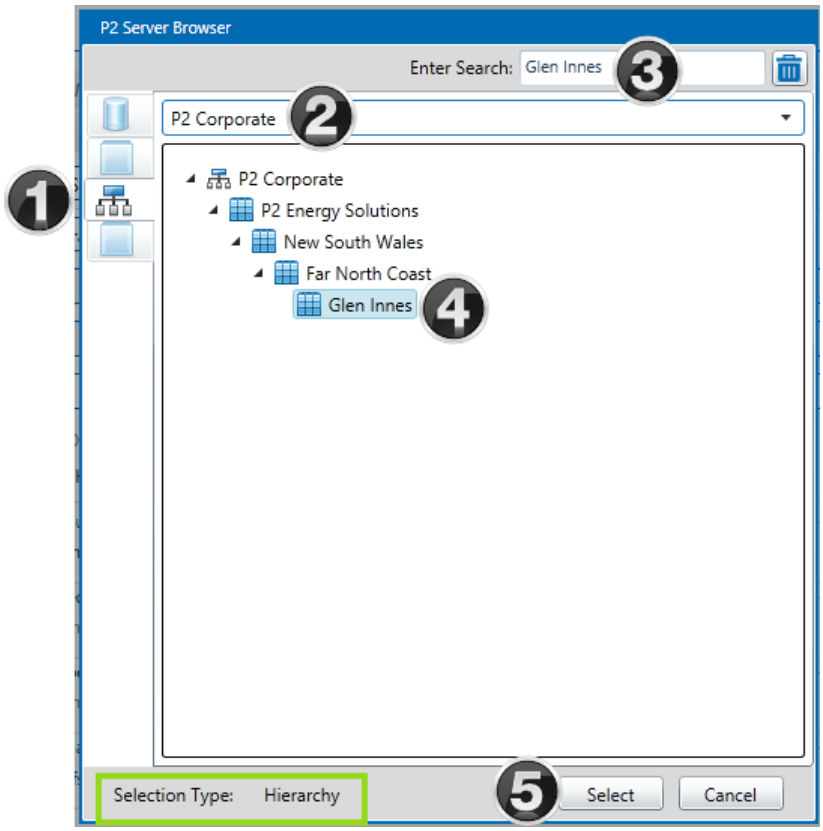
Selecting a Hierarchy

The P2 Server Browser can be used to select a Hierarchy to monitor, or to use for a custom event view, in a Hierarchy Report or an Event Timeline Report.

For example, when you are using the *Hierarchy* type for a Test **Source**, click the ellipsis button next to **Hierarchy** edit box.



This opens the P2 Server Browser, with the **Selection Type** of *Hierarchy*.



1. The **Hierarchy** button on the left is already selected.
2. Select a **Hierarchy** from the drop-down list.
3. Optionally locate a starting point:
    a. Either use the filter (as shown). Type into the **Enter Search** box and select an entity from the search result list. The entity is located on the hierarchy.

    OR

b. Navigate through the hierarchy by clicking on the arrow ▷ to the left of an entity.

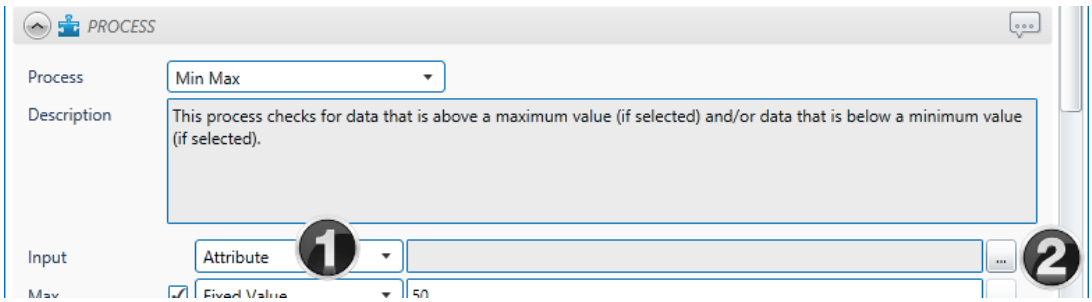
4. Optionally select a starting point. Click on an entity. This is the *starting point* for your selected hierarchy

5. Click **Select** to close the window, with the hierarchy and (optional) starting point selected.

P2 Server Attribute Picker

The P2 Attribute Picker is used for selecting an attribute. Attributes belong to entities.

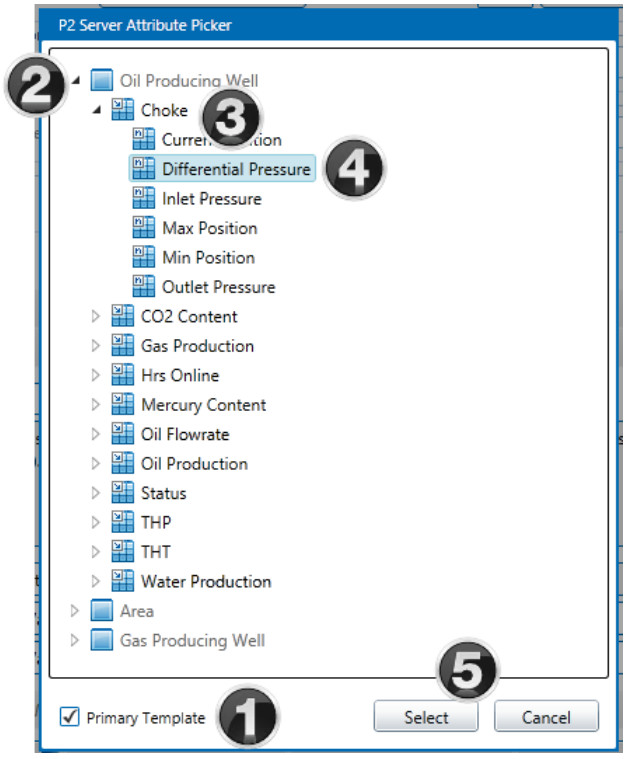
For example, to select an attribute as the **Input** for a process in a test:



1. Select Attribute from the drop-down list next to **Input**.

2. Click the ellipsis button.

The P2 Server Attribute Picker opens, with a list of templates.



1. Select the **Primary Template** check box to list attributes that belong to the primary template, or clear it to show all of the attributes that belong to the listed templates.

Note: By default, this option is **not** selected.

2. Expand a **Template**, by clicking the little arrow ▷ to its left.

3. Select an attribute or attribute value.

   a. Expand an Attribute by clicking the little arrow ▷ to its left.

      Or

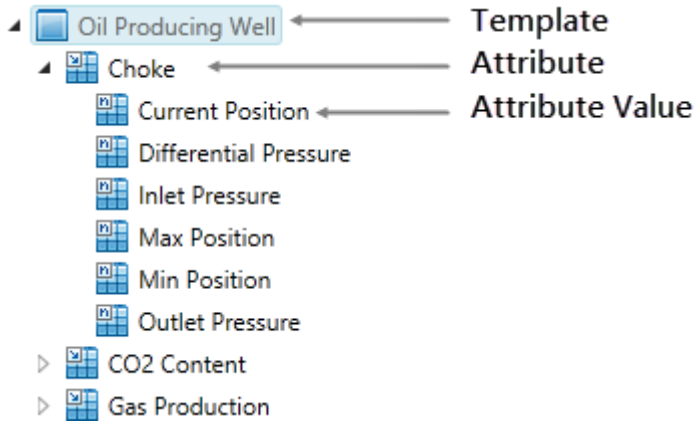
   b. Click on the attribute and click **Select** to close the window, with this attribute selected.

4. In the list, click an Attribute Value.

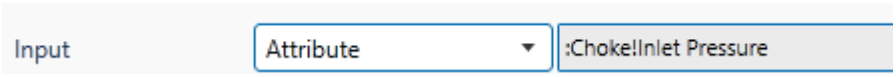
5. Click **Select** to close the window, with this Attribute Value selected.

ATTRIBUTES AND ATTRIBUTE VALUES

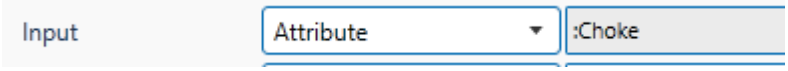
When you select an attribute from P2 Server Attribute Picker, you can select either the attribute or from the attribute values. For example, the screenshot below shows attributes, such as **Choke**, as well as attribute values of **Choke,** namely **Current Position, Differential Pressure, Inlet Pressure**, etc.



If you select just the **Choke** attribute, then Sentinel uses the current primary attribute value of **Choke** (this may change over time). If you select an attribute value, such as **Inlet Pressure** then Sentinel uses this.



A Sentinel Test Process using :Choke!Inlet Pressure attribute value



A Sentinel Test Process using the: Choke attribute

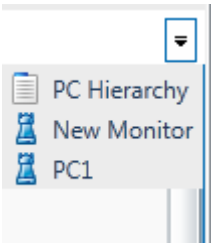
Selecting an Open Tab

When you are on a tab in the Main panel, you may navigate to any other open tab in the Main panel.

To navigate to another tab:

1. Click the down-arrow icon on the upper right of the Main panel.

   A list of all open tabs is displayed.



2. In the list, click the tab that you want to view.

The following icons indicate the type of tab that may appear in the list:

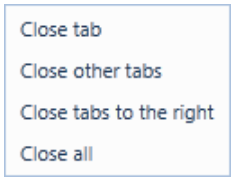
- The Events tab, for workspaces, folders, and monitors
- Monitor tab
- Monitor status tab
- Asset report tab
- Hierarchy report tab, Event report tab and Event History report tab
- Event timeline report tab
- Pending approvals tab
- Licence tab

Closing Tabs

To close tabs (pages) that are open in the Main panel:

1. Right-click on a tab header.

   The following menu is displayed:

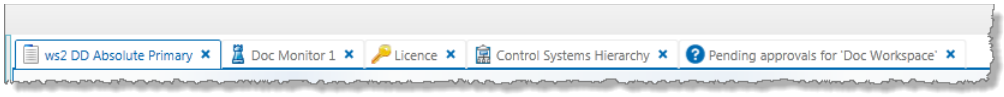


2. Click on one of the menu options:

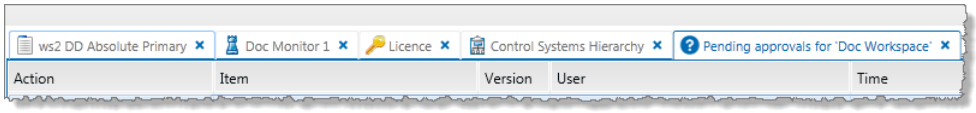
   - Click **Close tab** to close the selected tab.
   - Click **Close other tabs** to close all tabs except the selected tab.
   - Click **Close tabs to the right** to close all tabs displayed to the right of the selected tab.
   - Click **Close all** to close all tabs in the Main panel.

Moving Tabs

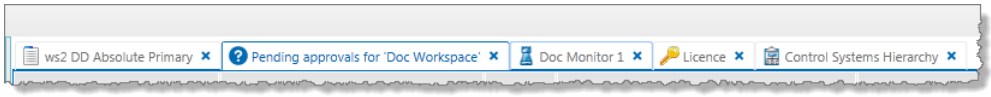
On the Main tab, you can organise the ordering of open pages, by moving page tabs to the left.



1. Click the tab that you want to move.



2. Drag it (*from right to left*) to the new position.



3. Release the mouse button.

Panel Comments

Many of the Sentinel panels have a comment box, where you can annotate why, for example, you have chosen to use the process, precondition, action, and so on, that you have used. If a panel has a comment box, this is depicted by a comment button on the upper right of the panel.

For example, the **Precondition** and the **Process** panels on the test screen each have a comment button (as shown in the screen image below).

If comments have already been added, the comment button is preceded by a *panel comments counter* button; the number on the button displays the number of separate comments for that panel.

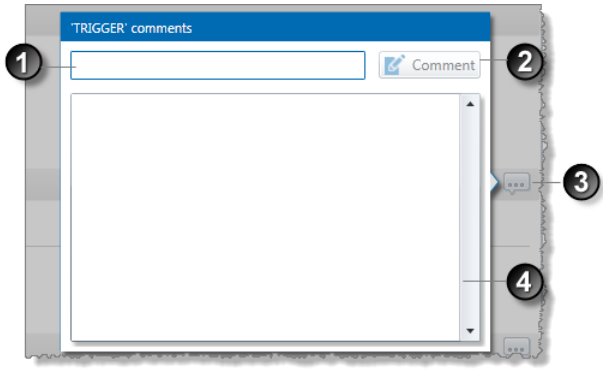
1. Comment button on the **Precondition** panel of a test.
2. Comment button on the **Process** panel of a test.
3. A *panel comments counter* icon, in this example indicating that there are already two comments for the precondition panel of this test. **Note:** This button only appears if there are already comments for this panel.

- To add or view comments, click the comment button, or click the comment counter button.

The *panel comment* window appears, with a title that includes the panel name.

The screen image below depicts the comment panel for a trigger. (In this example, the title is: *'Trigger' comments*).

1. Comment text box
2. Save comment button
3. Open and close comment panel button
4. Comment history list



Any existing comments appear in the comment history list, with the most recent comment listed at the top.

To add a new comment:

1. In the **Comment** text box, type a short comment explaining your choice of component.
2. Click the **Comment** button.

   The comment is saved, with a time stamp and your user name. This is displayed in the comment history list.

   The comment text box is cleared.
3. Continue to add comments using this method.

- To close the comment panel, click the comment button, or any part of the Sentinel screen (apart from the comment panel itself).

The number of comments, displayed in the *panel comments counter* icon, is incremented by the number of comments just added.

Note: Panel comments cannot be edited or deleted.

Report Hairlines

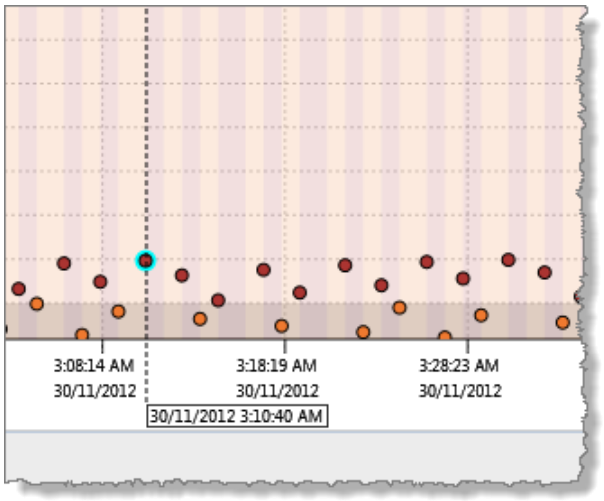
Report hairlines allow you to pinpoint an exact time on a graph.

In P2 Sentinel, the following graphs have a hairline:

- The *Event Timeline* section of the Statistics report, in the Asset report.
- The *Event Timeline* section of the custom Event Timeline report.
- The Timeline report, in Asset Reports.

To use the hairline in any of these reports:

1. Hover the mouse over the plot area of the graph (anywhere between the two axes), or in the magnifying pane of the time slider.



A fine, dashed line appears on the graph, vertically aligned to the tip of the cursor.

Alongside the dashed hairline is a text box, displaying the exact date and time (to the nearest second) of that point on the graph.

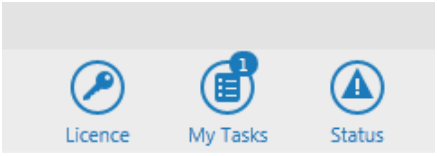
2. Move the mouse back and forth along the graph until you have the time you are interested in, or until you reach a point of interest (such as an event, for example).

   In the preceding screen image, the hairline highlights a point on the graph where the date and time is: 30/11/2012 3:10:40 AM.

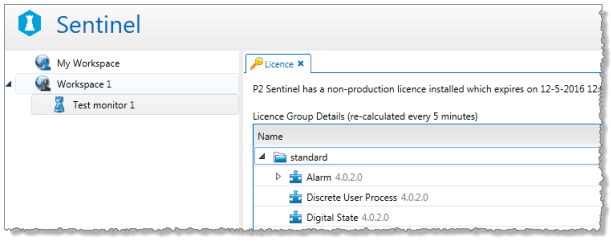
3. For the timeline report: to zoom into a period, click the hairline and drag it to the left or right, highlighting a section of the graph, then release the mouse button at your new start (if dragging to the left) or end time (if dragging to the right). The highlighted section of the graph replaces the original selection. To zoom back out to the original timeline, click **Refresh**, or **Refresh to Now** on the tab header bar.

The Licence Tab

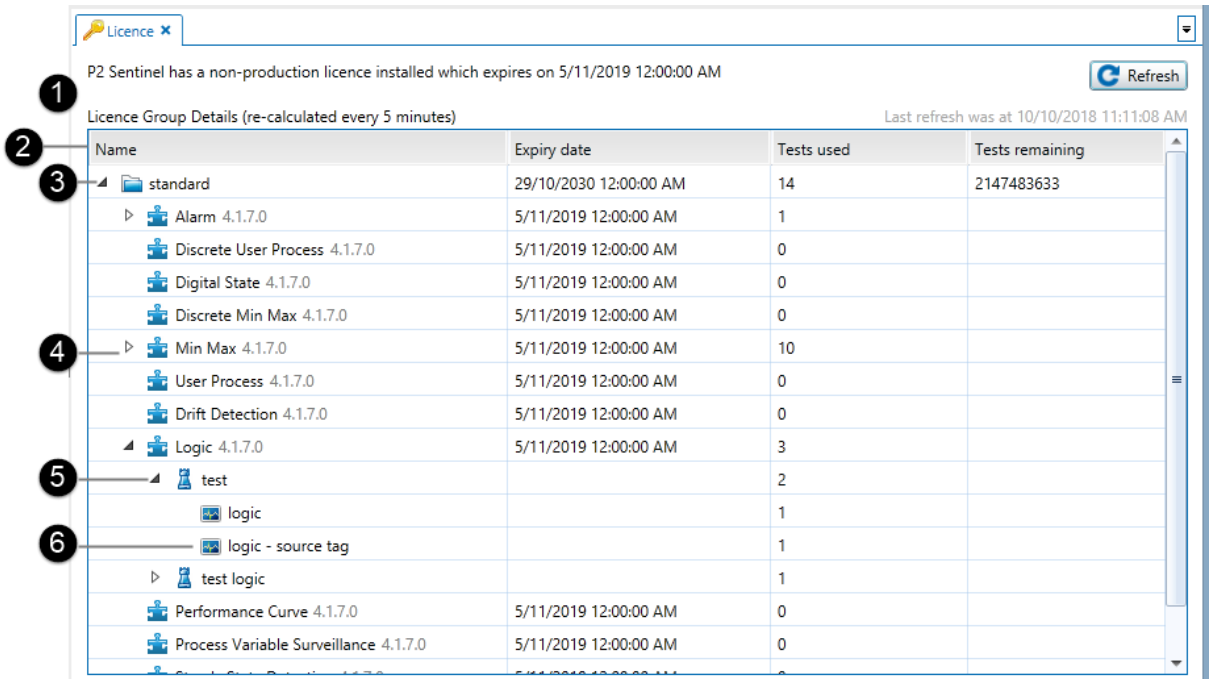
- To view the current state of Sentinel licences, click the Licence icon on the lower right of the Main panel.



The Licence tab opens in the Main panel.



The Licence tab displays information pertaining to the various licences and licence groups that this installation of P2 Sentinel holds, as well as the volume information and expiry dates of those licences and licence groups. Licence details are displayed as at the last refresh time.



1. The **Licence tab header** displays the following information about the licence:
   - The type of licence (production or non-production) and the Sentinel Engine licence expiry date.
   - The licence details recalculation interval.
   - The last time this tab was refreshed. Licence details are displayed as at the *last refresh time*.
   - The **Refresh** button; click this to display the latest licence details.
2. **Grid columns** (Name, Expiry date, Tests used, Tests remaining)
3. A **licence group**
4. **Process** that is part of the licence group (this includes the process name and version)
5. A **monitor** with tests that use the process
6. A **test** that uses the process

Explanation of Grid Columns

Name

The name of the licence group/process/monitor/test.

Expiry date

The date and time that the licence group expires; there is also a separate expiry date for each of the processes that form part of the licence group. The expiry date is marked in red font if it has already been reached.

Tests used

This relates to volume licensing; it shows the number of tests that are using the licence. There are separate *Tests used* figures for licence group, process, monitor and test. To show/hide details within the licence group, click the expand or collapse button. In the same way, you can also show/hide details for processes and monitors.

Licence group

The total number of tests that use the process within this licence group.

Process

The total number of tests that use this process.

Monitor
For this monitor, the number of monitor tests that use this process.

Tests
The number of tests using this process.

Tests remaining
The number of tests that may still use processes belonging to this process group; this figure is for total allocation for the process group (according to the Volume Licensing agreements), less the total tests already using the group.

Recalculating the Licence Group Details

Licence group details change when the number of tests used changes. The number of tests using processes from the group could change for any of the following reasons:

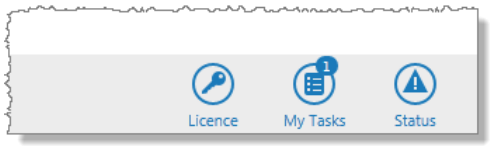
- Changes to monitors or tests
- A monitor may have been disabled
- Changes in the underlying P2 Server Data Dictionary may cause a different number of tests.

Changes to tests remaining could be due to an updated licence agreement.

Licence Group Details are calculated at set intervals (for example, every five minutes), as defined in the Sentinel configuration file.

P2 Sentinel Status

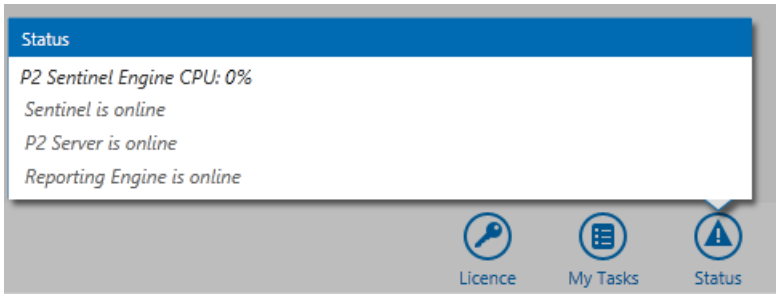
The Sentinel status icon is located on the lower right of the Main panel. If the system currently has any warning messages, the status icon flashes on and off intermittently.



If there are any warnings, the total count is displayed as a number on the icon.

- To see the current status of P2 Sentinel, click **Status**.

P2 Sentinel Engine CPU usage, as well as Sentinel status, Reporting Engine status and P2 Server online status are displayed in the status window.



- To close the Status window, click away from the Status window.

Warning Messages

Warnings are shown on the status panel, as follows:

Warning icon

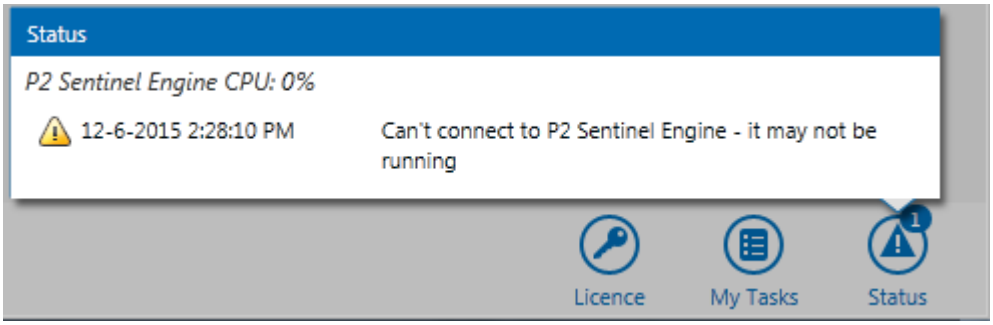
The warning icon shown for warning messages

Date and time

The date and time the message was created

Message

The message content



P2 Sentinel Concepts

There are three main aspects to working with P2 Sentinel:

Setting up P2 Sentinel Monitors

Monitors are added to workspaces and folders. Monitors use various test processes, triggers, and actions.

The following sections describe the concepts around monitors, triggers, test processes, test inputs, and actions, as well as assets, events, case management, and change management.

Viewing P2 Sentinel Outcomes

After the P2 Sentinel monitors have been configured and are active, you are able to view reports, create custom reports, and receive notifications. This is described in later sections.

Creating User Processes

Sentinel Studio allows those users with appropriate licensing and privileges to create processes (collectively called ***user processes***) and define the conditions that trigger an event. For detailed information on creating user processes, refer to the *P2 Sentinel Studio User's Guide*.

Monitors

All of the work in P2 Sentinel revolves around *monitors*. Monitors watch over P2 Server entities for compliance with specified limits or conditions. When limits are exceeded, or conditions change, P2 Sentinel raises an event and performs actions.

A monitor consists of a collection of tests, each having its own process. The tests all belong to the same category, which is defined in the monitor. They share a trigger, and run concurrently.

Monitors also have actions, which are assigned to tests. These are invoked by the tests that use them, when certain specified events occur.

A monitor has the following parts:

Monitor Details
: The name, category, description, and status of the monitor.

Trigger
: The trigger defines when the tests are started.

Tests
: Tests are the activity hub of the monitor. Each monitor uses at least one test. Each test evaluates one or more entities against predefined limits (states or values), by using one of the P2 Sentinel processes. The test results can cause events of particular states (each state being configured to a severity level), which in turn cause predefined actions to trigger.

Actions
: The activity that occurs as a result of a Sentinel event. A standard P2 Sentinel action is an email or SMS notification, or a web service action. Sentinel can also be configured to allow A-Plus actions. Actions may be added to the monitor, and assigned to the various tests.

Post Process
: When the monitor finishes running, P2 Sentinel calls a web service, if this has been selected in the **Post Process** section of the monitor.

Note: The web service needs to be specified in the **Sentinel Configuration** file. Refer to the *P2 Sentinel Installation and Administration Guide*.

Versions

Every time the monitor is updated and saved, a history of the changes is retained.

For more details on the monitor components, see the following sections:

- Monitor Details
- Triggers
- Monitor Status

Monitor Details

A monitor name and description define the monitor. The monitor name is a label for the monitor in the hierarchy of the Workspace panel.

Any open tabs in the Main panel that relate to the monitor have the monitor name as a header. For example, the monitor status tab and the monitor event tab both use the monitor name as a header.

The monitor category is used in reporting.

You can disable or enable a monitor in the monitor details section. The monitor is enabled by default, unless it is a copied monitor.

If you don't want to store events relating to the monitor, select the **Disable Event Storage** check box.

Monitor Category

The monitor category is used in reporting and does not affect the functionality of the monitor. Some examples of available categories are:

- Financial
- Operational
- Environmental
- Occupational Health and Safety
- Maintenance

There may be additional or different categories, depending on your installation.

When Case Management is enabled, a monitor's category is saved to a case when it is raised from a test in that monitor.

Triggers

Every monitor has a trigger. The trigger defines when the initial and subsequent monitor tests are processed. All tests within a single monitor share a single trigger.

There are four different types of trigger, as follows:

- Periodic trigger
- Date trigger
- Monitor Chaining trigger
- Application trigger

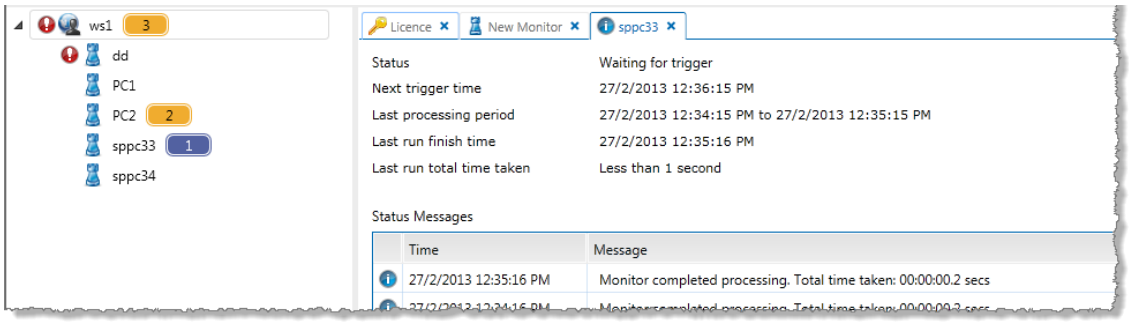
For all trigger types, the sample data is collected at the current trigger time, for the whole processing period. The processing period is the time between the last trigger time (last run finish time), and the current trigger time.

For the first trigger time, the processing period is the time between the monitor start date and time, and the first trigger date and time.

The status page for a monitor displays the following information:

- Status
- Next trigger time
- Last processing period
- Last run finish time
- Last run total time taken
- Current processing period

Note: The current processing period only appears when a monitor is currently processing data.



The Periodic Trigger

For periodic triggers, the tests are processed at set intervals. You define a start time (immediately or sometime in the future), and a repeat interval (for example, every minute, every two minutes, every hour, every week or every two hours, every two days, and so on). The periodic trigger can also be quantised.

Explanation of a Quantised Periodic Trigger

The quantise option is only available for the periodic trigger type. The quantised periodic trigger can affect the outcome of events for normal processing and also for catch-up processing.

CATCH-UPS

A process catch-up occurs when the Sentinel engine has stopped for a period of time, and is then restarted. After the engine is restarted, processes need to catch up processing data for the period that the engine was stopped. A process catch-up also occurs when a monitor is re-run. Catch-up processing for a monitor that uses a periodic trigger is performed in chunks determined by trigger intervals, the processing parameters (*MinCatchUpMonitorRunMinutes* and *MaxCatchUpMonitorRunMinutes)*, and the total run period.

USING THE QUANTISE OPTION

If the quantise option is selected for a periodic trigger, this ensures that the monitor is triggered at exact intervals from the *start time*.

For example, if the start time is on Monday at 12:38 pm, and the quantised period trigger is set to run every day, then the monitor runs on Monday at **12:38 pm** (trigger start time), Tuesday at **12:38 pm** (trigger start time plus trigger interval), Wednesday at **12:38 pm** (last trigger time plus trigger interval), Thursday at **12:38 pm** (last trigger time plus trigger interval), Friday at **12:38 pm** (last trigger time plus trigger interval), and so on.

In the same example, if the quantise check box is *not* selected, the monitor will *still attempt to run at set intervals*; that is, on Monday at **12:38 pm**(trigger start time), Tuesday at **12:38 pm** (trigger start time plus trigger interval), Wednesday at **12:38 pm** (last trigger time plus trigger interval), Thursday at **12:38 pm** (last trigger time plus trigger interval), Friday at **12:38 pm** (last trigger time plus trigger interval), and so on.

However, if there is any lag at all, the trigger intervals might not be exact; this is a factor of Sentinel's optimisation functions.

So, for example, there may be trigger times of: Monday at **12.38 pm**, Tuesday at **12:38 pm**, Wednesday at **12:38 pm**, Thursday at **12:38 pm**, Friday at **12:39 pm** (**slipped by a minute**), Thursday at **12:40 pm** (**slipped by another minute**), and so on.

When a monitor is re-run, or when the Sentinel engine is restarted (prompting catch-up processing), further problems may occur if quantised is not selected. The catch-ups may be conducted in smaller intervals (for example, half-hour intervals to catch up one day), possibly causing more events than what a one-day trigger interval would normally produce.

For example, a Sentinel process using 24-hour periodic trigger produces a single event. During a catch-up, the un-quantised periodic trigger causes the process to produce an event every hour, as it is catching up in one hour chunks.

For quantised triggers, this sort of variance in behaviour is also affected by the *MinCatchUpMonitorRunMinutes* and *MaxCatchUpMonitorRunPeriodMinutes* parameters.

To manage how catch-ups are performed, you need to understand the different rules defined in the following section.

Quantised Triggers and Catch-Up Parameters

Sentinel has different process catch-up behaviours, depending on the values in the Sentinel configuration parameters *MinCatchUpMonitorRunMinutes* and *MaxCatchUpMonitorRunMinutes*.

Catch-up behaviour is further determined by the value of the quantised periodic trigger (where applicable), as well as the total run period (the period that needs to be caught up).

Note: We recommend that the quantised trigger interval is an exact multiple of the *MaxCatchUpMonitorRunMinutes*.

Rule 1: Catch Up with MaxCatchUpMonitorRunMinutes Overriding Quantised Trigger Interval

If the quantised trigger interval is greater than *MaxCatchUpMonitorRunMinutes*, then *MaxCatchUpMonitorRunMinutes* overrides the quantised trigger interval (that is, processing will occur in time chunks the size of *MaxCatchUpMonitorRunMinutes*, rather than the quantised trigger interval).

Example 1:

MaxCatchUpMonitorRunMinutes is 24 hours. Quantised trigger interval is 48 hours. The catch-up is processed in 24-hour chunks.

Note: The default value for MaxCatchUpMonitorRunMinutes is 1440 (24 hours).

Rule 2: Catch Up with MinCatchUpMonitorRunMinutes Overriding Quantised Trigger Interval

If the quantised trigger interval is less than *MinCatchUpMonitorRunMinutes* **and** the total run period is greater than *MaxCatchUpMonitorRunMinutes*, then *MinCatchUpMonitorRunMinutes* overrides the quantised trigger interval (that is, processing will occur in time chunks the size of *MinCatchUpMonitorRunMinutes*, rather than the quantised trigger interval).

Example:
MaxCatchUpMonitorRunMinutes is 24 hours. Quantised trigger interval is five minutes. *MinCatchUpMonitorRunMinutes* is one hour. Total run period is 26 hours. The catch-up is processed in one-hour chunks.

Note: The default value for MinCatchUpMonitorRunMinutes is 60 (One hour).

Rule 3: Catch Up with Quantised Trigger Interval

If the quantised trigger is not overridden due to conditions described in Rule 1 and Rule 2, above, the catch-up occurs in data chunks the same size as the quantised trigger interval.

Example 1:
MaxCatchUpMonitorRunMinutes is 24 hours. Quantised trigger interval is five minutes. *MinCatchUpMonitorRunMinutes* is one hour. Total run period is 12 hours. The catch-up is processed in five-minute chunks.

Example 2:
MinCatchUpMonitorRunMinutes is one hour. Quantised trigger interval is two hours. The catch-up is processed in two-hour chunks.

How Does the Quantised Periodic Trigger Affect Events?

Because the quantised periodic trigger processes data at exact intervals, events (if these occur) can also be expected to relate to these exact intervals (occurring between the start and end of an interval).

So, if you have set up a **daily** trigger to go off at 1:00pm, for example, all events viewed from after 1:00pm onwards on any day will have occurred **up until 1:00pm on that day**, and not after. That is, if you view a day's worth of events at 1:15pm on Tuesday, those events will be from 1:00pm on Monday until 1:00pm on Tuesday, and no later.

If your periodic trigger is not quantised, the trigger period may not be as accurate. Here, if you view a day's worth events from 1:00pm on Monday, these may include events from 1:10pm on Tuesday, or even later.

Example Showing Quantised Versus Un-Quantised Periodic Triggers

In the following example, events from the five trigger periods leading up to 2.30pm are used for reporting. Using a quantised hourly trigger period, set to run on the hour every hour, the last five trigger periods are at exactly 10:00am, 11:00am, 12:00pm, 1:00pm and 2:00pm (see Figure 1).The events that take place during this time are events **1, 2, 3, 4 and 5.**

Using the exact same data, but running off an un-quantised periodic trigger (see Figure 2), the actual events are the same, yet those that occurred over the last five trigger periods form a slightly different group. This is because the trigger has shifted forward by half an hour (in this example, for the purpose of illustrating the potential behaviour of non-quantised period triggers).

The last five trigger periods are thus 10.30am, 11:30am, 12:30pm, 1:30pm and 2:30pm. The events that take place during this time are events **2, 3, 4, 5 and 6**. Note that event **1** falls outside of the range of the last five trigger intervals, and that event **6** has taken place (whereas for the quantised trigger period this has not been processed yet).

- Quantised Periodic Trigger used for the monitor
- Looking at the *last five intervals*
- The trigger interval is 1 hour

Current time (2.30pm) | Events (1 through 6) | Trigger interval

Data item | The periods between intervals (looking at the last four from 10:00am)

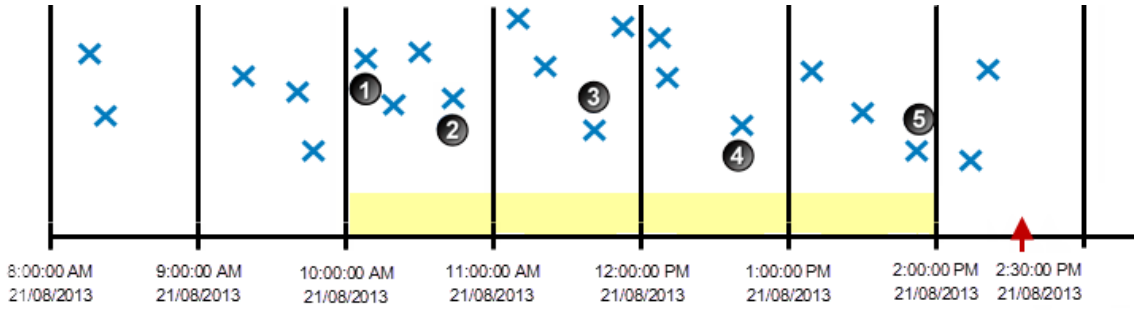


Figure 1: Using a quantised periodic trigger, on the hour

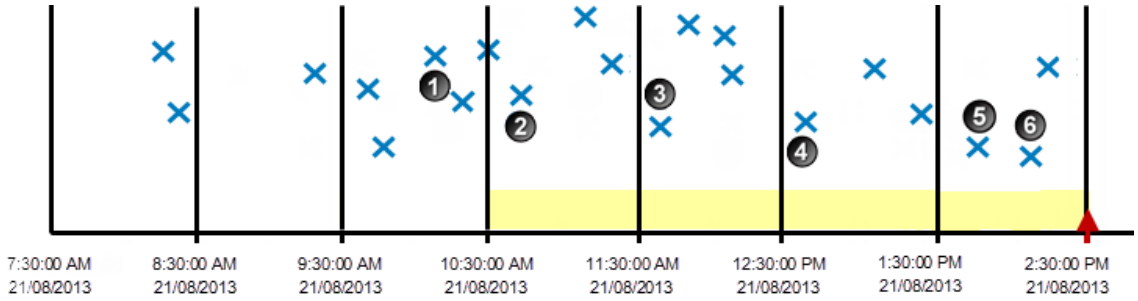


Figure 2: Using an un-quantised periodic trigger

Note how the trigger times have shifted, yet the data and the events remain the same.

The Date Trigger

For date triggers, the test processes can be set to run at daily, monthly, or yearly intervals at a set time. As with the periodic trigger, you can set a date trigger to start immediately, or at a specified time in the future.

Note: Monitors that use a periodic trigger or a date trigger are started as soon as they have been saved and approved (if enabled).

The Monitor Chaining Trigger

States raised by a test within a monitor can be set to trigger a different monitor. To achieve this outcome, the triggered monitor needs a **monitor chaining trigger**; any test within the triggered monitor should use the **Monitor Chaining Source** as its source, in order to be triggered by states.

The monitor chaining trigger can be activated by various selected states, from a selected test within another monitor.

The monitor that is triggered by monitor chaining can also be linked to another monitor for monitor chaining, and this one can be linked too, and so on, resulting in several linked monitors.

The Application Trigger

The application trigger causes the monitor to be started by an external application. There is no next start time. The next trigger time (if any) is dependent on the external application.

In order to activate the trigger, you need to make a call from an external application to the Monitor Triggering Service using the SOAP, the HTTP GET or the HTTP POST request method, using the applicable URL, as shown below.

SOAP Request Method

- Make a SOAP request to the following URL:

https://Sentinel/Server Name]:[Sentinel Server Port]/Sentinel/MonitorTriggeringService

HTTP GET Request Method

- Make an HTTP GET request to the following URL:

https://[Sentinel Server Name]:[Sentinel Server Port]/Sentinel/Trigger/MonitorName=[Monitor Name]

HTTP POST Request Method

1. Make an HTTP POST request to the following URL:

   https://[Sentinel Server Name]:[Sentinel Server Port]/Sentinel/Trigger/TriggerMonitorNameWithPostData

2. Type the name of the triggering monitor in the body of the HTTP POST request.

The application trigger activates every time a call is made from an external application.

Monitor Status

The monitor always has a current status. The monitor starts as soon as you have created and saved it, with a **started** status.

The monitor status can include any of the following:

- Started
- Stopped
- Waiting for trigger
- No approved version
- Disabled
- Running
- Re-running
- Deleting events

Note: Where an application trigger is used, the monitor only starts when an external application makes a call to the service.

You can view current monitor status information, as well as a history of monitor status messages, on the **View Status** page. This is explained in the section **Viewing Monitor Status**.

Note: If a monitor is running, this is indicated by a rotating processing icon in the workspace panel.

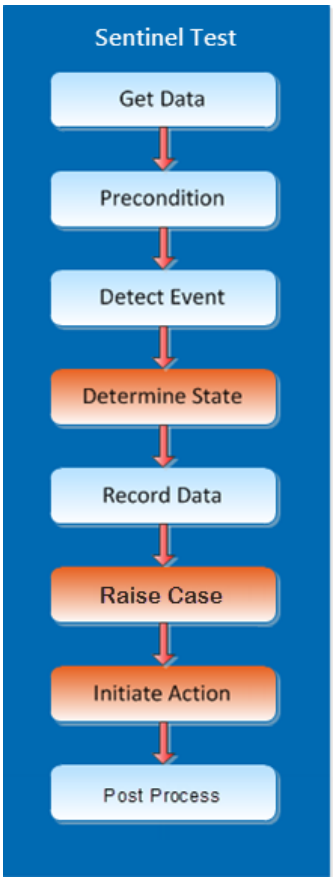
Monitor Behaviour

Once a monitor has been set up, each of its tests will behave in the following manner.

Data moves through the P2 Sentinel **test** flow, following these steps:

Get Data: P2 Sentinel fetches time-series data directly from P2 Server.

Precondition: If a precondition is defined, each portion of data must pass the precondition rules before it is tested any further.



Detect Event: An event is defined according to conditional logic. The event depends on the process used, and on the data values.

If there is no data
Sometimes there is no data at all. For tests using a *discrete data* process, such as the *Discrete Min Max* process, this causes a *No Data* event. For tests using a *continuous data* process, this may cause three different possible outcomes, depending on what has been configured in the Sentinel configuration file (parameter *NoDataBehaviour*):

- **Error**: This causes a monitor error. A monitor may stop after a certain number of monitor errors have occurred (as defined in the configuration file).
- **Ignore**: This has no effect on the processing. There will be a gap in the event data.
- **Suppress**: A Suppressed event is raised with the following message: *Processing was suppressed because no data was returned for <entity-name>.*

Determine State: The P2 Sentinel Engine determines the state based on the event. If the state changes, a new event is raised. States can be renamed if preferred, and can be mapped to different severity levels.

Record Data: P2 Sentinel maintains a database with the history of events across the lifetime of the system. Information is used in P2 Sentinel reporting and is displayed in the P2 Sentinel Event Log; it can also be published into P2 Server for analysis. Note that you have the option to disable event storage, in the configuration tab of a monitor.

Note: Comments can be added to event data. These are also saved to the database.

Raise Case: If Sentinel is configured to use Case Management and if the state for this test is configured to raise a case then, depending on the case options for the test, a case is raised. Actions may be deferred, depending on the state's configuration.

Initiate Action: P2 Sentinel will notify specified personnel (using email or SMS actions), or call a web service (using a web service action), when a particular state has been reached. This is all configured when the monitor is created. Other actions that trigger further processing can also be added to the P2 Sentinel installation.

Note: If Case Management is enabled, actions may be deferred until the case is confirmed. This depends on the state's configuration.

Post Process: When the monitor finishes running, P2 Sentinel calls a web service, if this has been selected in the monitor configuration tab.

Tests

A P2 Sentinel test evaluates source data using a defined process, and raises events when the state changes. The states resulting from a test can trigger specified actions.

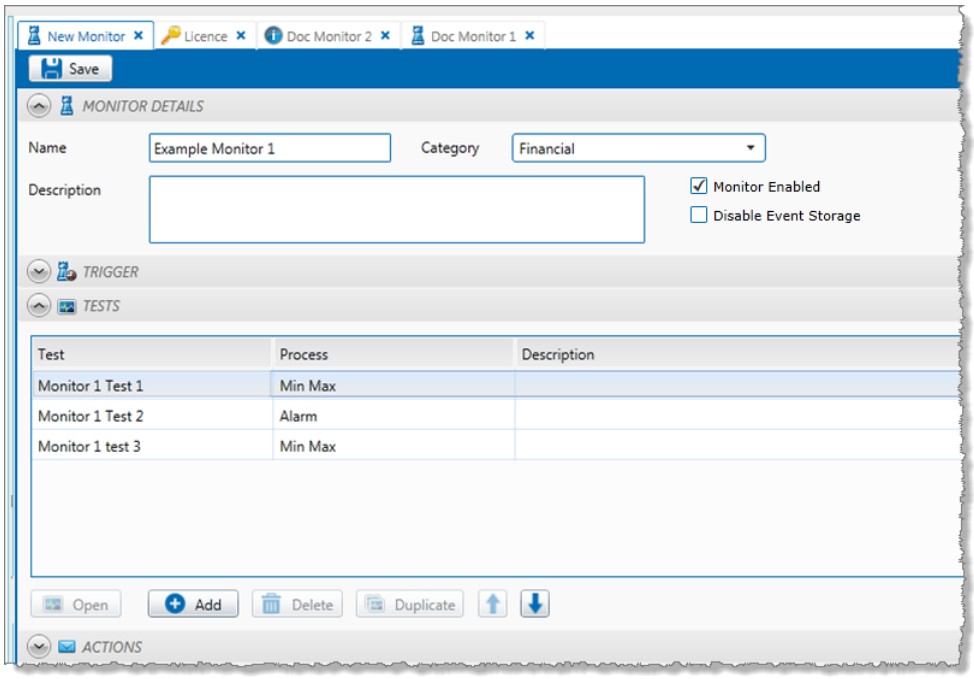
Every monitor has a collection of one or more tests. All tests run concurrently, as defined by the monitor trigger, and each test uses its own process.

The tests all belong to the same category, which is defined in the monitor.

A test may also have actions assigned to it. These are actions that are defined in the monitor, and may be assigned to any of the monitor tests.

You may also duplicate a P2 Sentinel test, within the same monitor, giving the new test a unique name.

The following screen image shows a monitor with three separate tests:



The test details, as well as the process that each test uses, are listed in the **Tests** panel of the monitor.

A test has the following components:

Test Details

The name and description of the test.

Test Suppression

An optional test suppression is specified here. For *time suppression*, the test is suppressed for the period between the selected suppression start time and suppression end time.

Source

The source data for the test is defined in this panel.

Precondition

While a test is running, any input values are evaluated for the periods when the precondition is true. This precondition may be the state or value of one or more entities. For the periods

that the precondition fails (and optionally for a stated period thereafter), the test monitor item goes into a **suppressed** state.

Process

The process that is used by a test.

State Configuration

Exceeded limits, as defined in the process, raise various states. In this panel you can configure the possible state outcomes with a severity level, and you can override the standard state description. You can also add notes giving a reason for the state, the potential impact, and the recommended action to take.

If Case Management is enabled, this is where you can configure Sentinel to raise a case for a state, and whether to defer actions until the case is confirmed.

Auxiliary Data

The values of any auxiliary data defined in the test are saved with the event details. Auxiliary data is displayed in the Events History table, and also in the Associated Event Data in an email action. Auxiliary data can be displayed in the content of an email or SMS action.

Actions

In this panel you assign various monitor actions to the test.

These components are described in more detail in the following sections:

- Test Details
- Test Suppression
- Source
- Precondition
- Processes
- Event State
- Auxiliary Data
- Actions

Test Details

The test is identified and described in this panel. The test details are added when the test is set up, and may be edited.

The test details are displayed in a grid in the **Tests** panel of a monitor, and should clearly identify the test.

Test Suppression

This is where a planned suppression of the test is defined.

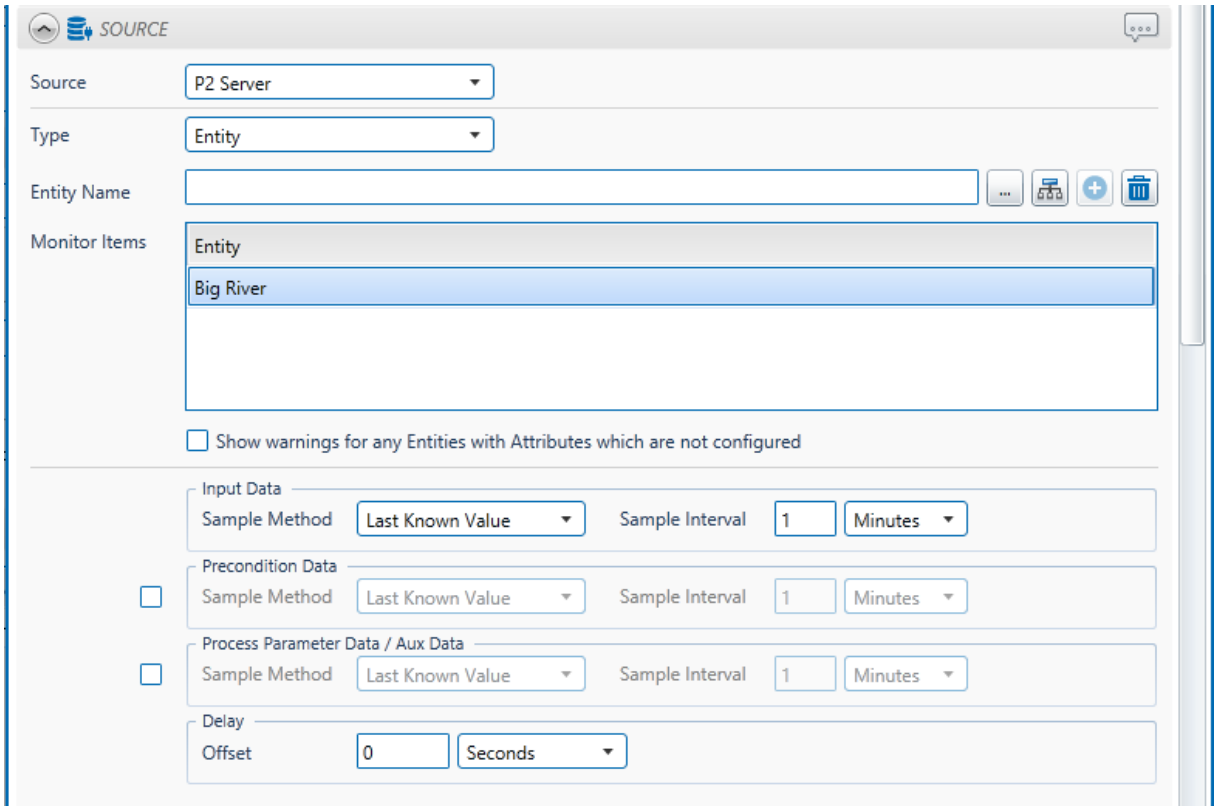
If you select *Time Suppression*, the test is suppressed between the specified start and end times; a notification email can be sent to specified recipients, at a predefined interval before the time suppression ends.

Source

This is where the test source data is defined, and where the sampling details are specified.

The most common source for a test is P2 Server. The source may be an entity or a hierarchy. If it is an entity type, then you can look up various entities in the P2 Server Data Dictionary, and add these as separate monitor items. These can be tags or general entities.

If you are using a hierarchy source type, then you will select a hierarchy from the P2 Server Data Dictionary. The hierarchy will have a starting point, and you will be able to select which template to use.



When defining a source you need to specify the following:

Source

The most common source for a test is P2 Server.

Type

There are three source types to choose from:

Entity

With an entity type, you are able to select individual entities to monitor.

Tag

With a tag type, you are able to select individual tags to monitor.

Hierarchy

With a hierarchy type you can monitor all the entities from a starting point from a hierarchy that exists in the P2 Server Data Dictionary.

Note: There is an option to only include entities for which the selected template is set as the primary template.

Sample Methods for Data

A sample method must be defined for the input data. Separate sample methods can be defined for preconditions (where applicable), as well as for the process parameter data, and auxiliary data.

Sample Method
The sample method you choose to fetch the data. Choose from Raw, Average, Linear Interpolate, or Last Known Value. The default and the available sample methods depend on the process that is used.

Sample Interval
The regular interval between trigger periods to collect sample data. At every sample interval, the collected data is prepared according to the sample method used, and then evaluated in the process. You can specify the sample interval in seconds, minutes, hours, days, or weeks. The default sample interval is 30 seconds.

Delay
By setting this option, you cause a delay before the sample data is collected. This option is useful in cases such as when a historian is writing data at a similar time to when P2 Sentinel is reading data.

Precondition

You can specify a precondition for a test. For each entity during the processing period, P2 Sentinel will evaluate the precondition rules to determine the periods when the data will be processed. The precondition data may be an attribute of the source entity, either as it is, or as part of a calculation, or it may be the attribute of another entity. If the source type is **Tag**, the precondition data can be the source tag or a calculation using the source tag.

For the periods that the precondition fails, the test monitor item goes into a **suppressed** state. During the suppression periods, no data is processed.

The standard precondition is made up of a single condition, *Condition 1*, with two optional extra conditions, *Condition 2* and *Condition 3*. In addition to the conditions that make up the precondition, you may set an *Out of Suppression Delay*. After a test monitor item emerges from the suppressed state caused by the precondition, it will enter a new suppressed state for the duration of the out of suppression delay. For more information, see Add a Precondition.

Event State

The event state is the state that is reached to raise an event for a test. The event state is displayed in the event grid on an event page.

The various states in a particular test process can be assigned a severity.

During processing, an event is raised when the monitor item value exceeds defined limits, or when the monitor item moves to a particular, defined state. Every new event causes a state to be reached.

State Configuration

Each state, for a test, has a severity assigned to it; this is defined when the test is added to the monitor. The default severity for all states is *None*.

STATE SEVERITY

The severity for a particular state outcome should be configured in accordance with what is being monitored.

For example, if a process has a *High* value that is exceeded during the test, then this raises a *High Exceeded* event. If this is considered to be a severe outcome for this particular test, then a severity of *High* should be assigned to the state.

However, if the *High Exceeded* state for this test is considered to be of a medium or low severity, then a *Medium* or *Low* severity configuration is more appropriate for this outcome.

State Override

There is also a *State Override* option, for each state outcome of a test. This can be used when a more specific description of the state is required. Where a state override is used, the standard label for a state is replaced by the state override text. The new label displays in all the reports.

The different states for a test outcome can be configured.

Case Management

This is only available if Case Management is enabled in Sentinel.

Each state can be configured for case management.

Manage Case

If this is selected, a case is raised for this state outcome of a test (this also depends on Sentinel's configuration for cases and the test's Case Options). See details in 3.6 Configure States.

Note: If Aggregate Cases is enabled for the monitor's category, and there are open cases for the category, then Sentinel will not raise this case; instead, a comment is added to the most recent open case of the category.

Defer Actions

Any actions linked to this state are deferred until the related case is confirmed. A case is confirmed by a user in P2 Explorer, in the case details. If the case is rejected, the actions do not happen at all.

State Comments

Each state has three comment panels:

Reason for State

Used for stating the most likely reason for this state outcome, for the particular test.

Potential Impact

Used for outlining the potential impact of the test reaching this state.

Recommended Action

Used for elaborating on what actions to take following this state outcome.

These comments are all added when the test is set up, and can be included as tokens in email, SMS or web service actions, making it easier and quicker for notification recipients to understand possible causes and take remedial action.

If Case Management is enabled in Sentinel, there is a fourth comment panel:

Override Case Comment

This optional comment can be used to override the test's Case Comment for a specific state.

State Severity

The available severity levels are displayed as colours:

None	Grey
Suppressed	Blue
Low	Yellow
Medium	Orange
High	Red

In the P2 Sentinel charts, and in the event notification in the workspace, the colours used are based on the *highest severity* encountered in the grouping.

Note: There could be more than one event notification label, if you have cleared the option **Combine severities into a single count** in the **Event Display Options**.

Examples:

- If the highest severity reached for all events for tests running under a workspace is of *Medium* severity, then the event notification label for the workspace is coloured in orange, the colour for *Medium* severity.
- If the highest severity is *Low*, then the event notification label for the workspace is coloured in yellow, the colour for *Low* severity.

This is explained in the section on Viewing Events. The same principle applies to the colours shown in the asset reports.

Case Options

If Case Management is enabled in Sentinel, there is a Case Options panel for configuring how a case is managed for a test.

Case Title

A default title can be set up in the Sentinel Configuration file, and can be edited for a test. This is the title that Sentinel generates when a case is raised with an event, and appears in the case details in P2 Explorer. The case title can contain tokens.

Case Description

A default description can be set up in the Sentinel Configuration file, and can be edited for a test. This is the description that Sentinel generates when a case is raised with an event, and appears in the case details in P2 Explorer. The case description can contain tokens.

Case Comment

A default comment is set up in the Sentinel Configuration file, and can be edited for a test. The case comment can contain tokens.

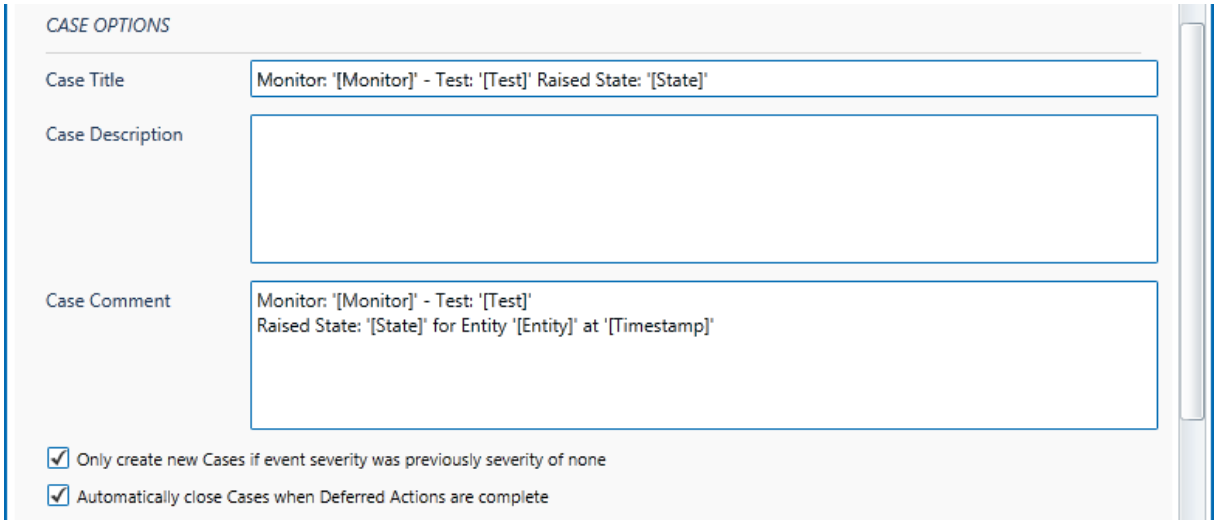
Only create new Cases if event state was previously severity of none

If this option is selected, cases are only raised if there has been a severity of *None* since the last case was raised for the test.
If the *OnlyCreateCasesDefaultOption* setting is set to *True* in the Sentinel configuration file, the check box is selected by default.

Automatically close Cases when Deferred Actions are complete

This relates to cases by state where the Defer Actions check box is selected. Deferred actions are carried out by the system as soon as a case is confirmed. With this option selected, the case is automatically closed after the actions are complete.

If the *AutoCloseCasesAfterConfirmation* setting is set to *True* in the Sentinel configuration file, the check box is selected by default.



Auxiliary Data

You can add auxiliary data to a Sentinel test. Auxiliary data is not monitored, but is saved with other event details when one of the test's monitored assets raises an event. For example, your test may be monitoring pressure; if you have temperature selected as auxiliary data this is recorded when pressure raises an event.

Actions

In P2 Sentinel, you can add actions to monitors.

When an event is raised, P2 Sentinel triggers the configured action (or actions) which can be an event notification, or a call to a web service URL.

P2 Sentinel provides the following standard action types: email, SMS, SMS via Web Service, and Web Service. Sentinel can also be configured to allow for A-Plus action types. The notification actions (email and SMS) can be sent to specified personnel alerting them to events; Web Service actions can make GET or POST calls to a specified web service URL when an event occurs; these can be used for a variety of purposes, such as raising work orders, for example.

Standard Action Contents

Each standard action defined in a monitor consists of the following:

Name

A descriptive name that you assign to an action.

Type

The standard action types are email, SMS, SMS via Web Service, and Web Service.

To

You can add recipients of an email or SMS action from a contacts list, if the Active Directory is set up in the configuration file, or you can type in the contact details.

Entity Source
For email actions only, you can add recipients using an entity source, instead of, or as well as, adding recipients in the **To** edit box. Select the checkbox, then type the full definition for the attribute that stores the list of recipients' email address, in the format: [template]:attribute!attribute value.

Format
Choose a format of *Text* or *HTML* for email actions.

Subject
A subject line, for email actions only; this may contain tokens.

Message
For Email and SMS actions only. The message is made up of text and tokens. Some of the tokens are standard to all messages (as defined in the P2 Sentinel configuration file); you can add other available tokens to the message content.

URL
For Web Service actions; type in the web service URL for a GET or POST request method.

Body
For Web Service actions; for a POST request type, you can type additional text into the Body section.

Replacement Tokens
System-generated variables. You may include these in the subject line, and in the message. In the case of Web Service actions, you may include tokens in the URL and/or in the Body.

STANDARD ACTION LISTS

After actions are added to a monitor, they are listed in the **Actions** panel of the monitor.

Action
The action name.

Type
The type of action: email, SMS, A-Plus, SMS via Web Service, and Web Service.

Filter
The action may have a Group Suppression filter.

Tests Used By
A list of all tests that use the action.

ACTIONS IN A TEST

Monitor actions are assigned to tests. Select the state that causes the action when you assign the action to the test.

Deferred Actions

If Case Management is enabled, there is a configuration option for each state within a test for that state's actions to be deferred until the related case has been confirmed. If the related case is rejected, the deferred actions won't happen at all.

Group Suppression

In P2 Sentinel you may choose to suppress certain actions within a monitor, or even within a test.

Actions that are Part of Group Suppression

Within a monitor, all actions that have been defined as *Group Suppression* actions are treated as one group.

Whenever there is more than one action within that group, all actions of a lower severity are suppressed, with the result that P2 Sentinel only initiates a single action. This is the action with the highest severity in the group.

P2 Sentinel continues to monitor all ensuing events within the group. As soon as there is a change in severity within the group, P2 Sentinel causes a new action to raise a notification. Again, this is the action for the event with the highest severity within the group.

Actions that are not part of Group Suppression

These are any actions that are defined within the test, or within the other monitor tests, that are *not* part of group suppression.

These actions behave independently of any other actions in the monitor. If a state is reached for the action, then the action raises its specified notification.

Group Suppression in Monitors and Tests

A single grouping is available in a monitor.

If all group suppressed actions are defined within one test only, then the group suppression applies to the test only.

If there is group suppression in more than one test, then group suppression applies to the monitor.

Tokens

Tokens are system-generated variables that can be added to the message content, or to the subject line of an email or SMS action. Tokens can also be used in the URL or Body portion of a Web Service action. The token variable name forms part of the text of an action message, once it has been added. In the action content, once the action message has been delivered, the token variable name is substituted with the token value.

An example of a token is the *monitor name*, which can be used to form part of the message content, or maybe part of a URL in the case of a Web Service action. If the monitor name is changed at any point, then the latest monitor name will show in the message content of an action, when it is delivered.

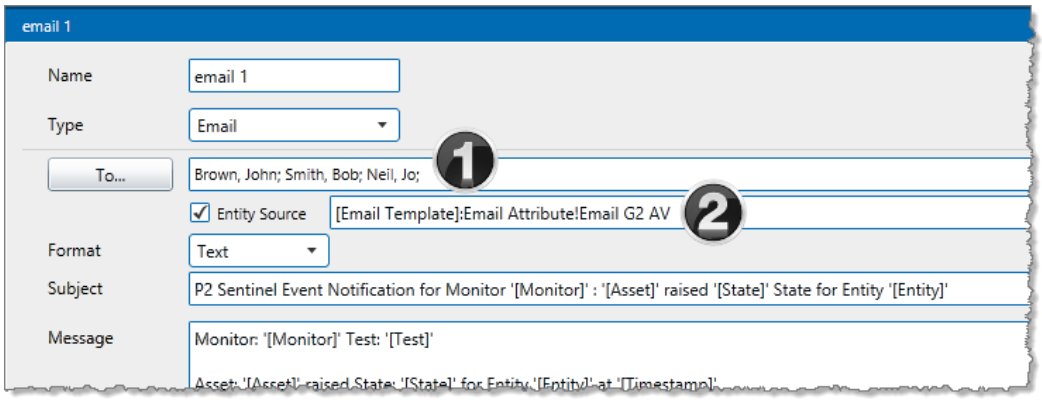
Another example of a token is the web address for the asset report of the test event that has caused the action. The received message will contain the correct hyperlink, which can then be used to access the relevant web page directly from the email or SMS.

For instructions on how to insert tokens in an action message, see Using Tokens.

Action Recipients

For the SMS and the SMS via Web Service actions, you need to specify the recipients. The SMS action sends alerts to the list of recipients, regardless of the data that caused the event behind the action.

Email actions can also be configured to send notifications to the fixed list of recipients in this way; there is another way of setting up email recipients: the **Entity Source** method. This can be used in conjunction with the standard list of recipients.



Email Recipients	
1	Set list of email recipients; these are always notified as part of the action
2	**Entity Source** attribute definition. The email recipients can be stored as attribute value for entities that are defined as the test's source.

Entity Source Recipients

Entity Source recipients need to be configured in Enterprise Manager. If you are a Server Administrator, you can configure entity source recipients as follows:

Note: the instructions below need to be carried out in **P2 Server Management**, and require knowledge of that system, as well as the appropriate privileges.

Create a New Template in P2 Server

1. Create a new template that will be used especially for this purpose. Give it a name, for example: 'Email Template', and assign it to a suitable template group; you can create a new template group especially for this purpose, and call it 'Email Template Group', or similar.
2. Add an attribute to the template, with a data type of TimeSeries, and give it a name, for example: 'Email Attribute'.
3. Add an attribute value to the attribute and give it a name, for example, 'Email List 1'.

   The template is ready to be used for storing email recipients.

Assign the Template to Entities in P2 Server and Configure the Attribute Values

For entities that will be using the Entity Source feature in a Sentinel email action, assign the new email template.

Note: Because the email template is only for assigning email attributes, we recommend that it is assigned as a non-primary template.

For each entity that you are assigning the new email template to:

1. Locate the entity.
2. Assign the new template.

3. Edit the attribute value, by adding a list of email recipients for the entity. The attribute value must be of type **String**, and email recipients are separate by a semi-colon (;). Type in either the full email address (for example, jo.smythe900@gmail.com) or type in the email display address, as it appears in the active directory, enclosed in double quotations (for example, "Smythe, Jo").

   Example of the attribute value showing several recipients
   "James, Logan"; "Cook, Simon"; "Jones, Bob"

Note: If the asset that raised the state for the action is an entity that does **not** have the email template defined, or the attribute value has not been configured to hold an email address, the monitor will stop due to the fact that the email recipients could not be found for the entity.
The following error message, or similar, is displayed:
'Email was not sent because an error occurred getting the email recipients from 'WIW 2[Sentinel Email Recipients]:Email List!List One': The following data object was not found: 'WIW 2[Sentinel Email Recipients]:Email List!List One',
where **WIW 2** is the **entity, [Sentinel Email Recipients]** is the **template, Email List** is the **attribute** and **List One** is the **attribute value**.

Setting up the *Entity Source* option for email actions in Sentinel is detailed in the section under adding actions, Define Entity Source.

Processes

Every test in a monitor has a single process. The process is the component that does the "work" specified by the monitor to analyse the data required to raise events.

The process determines the method of testing inputs to a test. In a process, the test inputs are specified, as well as the test evaluators. Where there are multiple test inputs, or monitor items, a test for each input will run concurrently at the triggered start time.

Standard Sentinel Processes

The following processes are included in the default P2 Sentinel installation and do not require further licensing:

- Alarm Process
- Min Max Process
- Digital State Process
- Discrete Min Max Process

The following processes are also included in the default installation, but you must have the appropriate licences to run them:

- Process Variable Surveillance
- Drift Detection
- Stuck Value
- Steady State Detection
- Logic
- Performance Curve

For more information, refer to the appropriate appendix for each process (for example, Appendix A. Alarm Process).

Sentinel User Processes

P2 Sentinel provides the capability to construct your own processes using Sentinel Studio. This requires additional licensing and privileges. For further information on creating user processes, refer to the *P2 Sentinel Studio User's Guide*.

Privileges: To add or edit user processes, you need a security role that has the **User Processes Edit** privilege. To delete user processes, you need a security role that has the **User Processes Delete** privilege.

Process Entity Volumes and Licence Groups

Each process belongs to a licence group, which has an *Entity Volume* assigned to it. The Entity Volume defines the maximum number of entities that may be used, collectively, for all processes that belong to the applicable licence group. Entities using the various processes from a particular licence group are counted throughout every monitor in the P2 Sentinel installation, excluding those for disabled monitors.

The Entity Volume value may vary between the various licence groups. The Entity Volume value for each licence group is agreed upon as part of the licensing procedure.

Note: If a particular test has caused the group Entity Volume limit to be exceeded, that test will stop running until the volume limit is no longer exceeded.

Process Inputs

The following inputs are available, for many of the test processes:

Attribute

This is available where the **Source Type** is either **Entity** or **Hierarchy**.

Click the ellipsis button to open the **P2 Server Attribute Picker**. This shows templates of the source entities. To view primary templates of the source entities, select the **Primary Template** check box. Select an attribute.

Source Tag

This is available where the **Source Type** is a **Tag**.

Calculation

Click the ellipsis button to open the *Edit Calculation* window.

Where the source type is **Entity** or **Hierarchy**, enter '*this*' for the source entity token, followed by an attribute or attribute value definition. For example: **{this:THP} + 34**. Another example: **{this:Choke!Current Position}*1.2** The expression is resolved in the P2 Server calculation engine.

Where the source type is **Tag**, enter '*this*' for the tag token. For example: **{this} * 1.2**. The expression is resolved in the P2 Server calculation engine.

Process Limits

The process input value is compared against the various process limits, at every sample interval during monitoring.

Depending on which process is used, there are different process limits to define. You can also configure the various states for a process.

To find out more about the various P2 Sentinel processes, refer to the separate Appendix that is supplied with each of the processes (for example, Appendix A. Alarm Process).

Events

P2 Sentinel raises an event when a monitor item exceeds a predefined outcome (as defined in the process for a test), or when a monitor item reaches a digital state (as defined in the process for a test), during processing.

Depending on the process used by a test, different limit evaluators need to be set up.

For example:

Events for a Digital State Process

- A *Primary* limit is defined. When the monitor item is in the *Primary Limit* state of the selected state pair, a **Primary** event is raised, and a **Primary** state is reached.
- An optional *Secondary* alarm is defined. If the Primary state extends beyond the *duration* specified for the secondary limit, a **Secondary** event is raised, and a **Secondary** state is reached.

- An optional *Tertiary* alarm is defined. If the Secondary state extends beyond the *duration* specified for the tertiary limit, a **Tertiary** event is raised, and a **Tertiary** state is reached.

Events for a Min Max Process

- A *Max* value is defined. When the *Max* (maximum) is exceeded, a **Max Exceeded** event is raised, and a **Max Exceeded** state is reached.
- A *Min* value is defined. When the input value is lower than the *Min* (minimum) value, a **Min Exceeded** event is raised, and a **Min Exceeded** state is reached.

Events for an Alarm Process

- A *High High* value is defined. When the *High High* value is exceeded, then a **High High Exceeded** event is raised, and a **High High Exceeded** state is reached.
- A *High* value is defined. When the *High* value is exceeded, a **High Exceeded** event is raised.
- A *Low* value is defined. When the *Low* value is exceeded (where the input value is lower than *Low* value), a **Low Exceeded** event is raised.
- A *Low Low* value is defined. When the *Low Low* value is exceeded (where the input value is lower than *Low Low* value), a **Low Low Exceeded** event is raised.
- If there is no sample data available as an input to the test, a **Suppressed** event is raised.

Events for a Discrete Min Max Process

- A *High* value is defined. When the *High* value is exceeded, a **High Exceeded** event is raised.
- A *Low* value is defined. When the *Low* value is exceeded (where the input value is lower than *Low* value), a **Low Exceeded** event is raised.
- Sometimes there is no data at all during a trigger interval. This causes a **No Data** event.

Events for other Sentinel Processes

P2 Sentinel has a number of plug-in processes available. The events depend on the process used, and are described in the separate Appendix section for that process (for example: Appendix B. Min Max Process contains a section that describes states and events for the Min Max process).

Event Comments

Wherever an event has been raised, it is possible to add an event comment.

Multiple comments can be added to a single event, with the latest one displayed in the main event grid, along with a tally of comments.

Each comment is saved with a time stamp, and the logon identity of the person who added the comment. You can view all of these comments.

Note: In P2 Sentinel, you cannot delete or edit comments.

Editing an Event

Privileges: To edit events, you need a security role that has the **Sentinel Events Edit** privilege.

Sentinel events can be partially edited. Users with privileges to edit an event can update the state and severity of any Sentinel event. These updates require a comment.

Event Status

An event becomes **Invalid** if the related case is investigated and then rejected, as part of Case Management. The event status is **Valid** if the related case is confirmed. For all other case statuses, the event status is **Unknown**.

Note: An event is only given a *status* (Unknown, Valid, and Invalid) if Case Management is enabled in Sentinel.

Assets

P2 Sentinel uses the concept of an *Asset* to help to identify the events that are raised.

When you select a monitor item, while defining a P2 Sentinel test, you identify which asset that item belongs to. Assets are mapped from the P2 Server template, where the entity is configured with attributes and attribute values.

For example: Monitor the flow rate on a pump named Pump100. Pump100 has a template with a flow rate attribute which points to a tag called 01FCEAA. Any events raised have a reference to the entity (01FCEAA) and will also refer to the asset (Pump100).

In this example, the reporting shows that Pump100 raised the event.

P2 Sentinel Reports

The standard P2 Sentinel reports show all events against a selected asset. When a test is set up, the asset is defined in the **source** panel. You may view all the events for any particular asset.

To limit the report data, several filtering options are available, such as which monitor events to view, and over which period. You may access reports through an asset, which is selected from a list of events.

States

Every item that is monitored in P2 Sentinel is in a certain state, at any point whilst the monitor is running.

As new input is evaluated, its state can change.

For each input in a test, the initial state depends on the process used. After the test is triggered, new sample data is collected at every sample interval. The sample data is evaluated against predefined limits. If a sample value exceeds a limit, then a new state is reached.

State Duration

State duration lasts until a new state is reached.
State duration is measured to the nearest second.

Start Time

The start time of an event for an entity is the time that the current state was reached. When the state changes, there is a new start time for the event.

Note: Where a delay is used, the start time is the time that the data exceeded a limit to cause an event, rather than the time that the data was fetched.

State Severity

The state severity is specified in the state configuration of a test.

There are five severities that can be used to classify the different states:

- None
- Suppressed
- Low
- Medium
- High

The default severity for all of the states is **None**.

Suppressed State

When a test runs, any input values are evaluated for the periods when the precondition is true. For the periods that the precondition fails, the test monitor item goes into a **suppressed** state.

If there is low confidence data for an entity that is being tested, then the resulting state for that entity will be **suppressed**.

A third circumstance which may cause a suppressed state is Test Suppression, whereby testing is deliberately suppressed for a specific reason.

The following states can be reached, depending on which process is being used by the test:

- Default
- High High Exceeded
- High Exceeded
- Low Exceeded
- Low Low Exceeded
- Suppressed
- Min
- Max
- Primary
- Secondary
- Tertiary
- No Data

For more information about which states apply to the various processes, refer to the appendices below, for more about the different processes.

Case Management

Case Management, in P2 Explorer, is all about actions and changing the status of events raised in source applications such as P2 Sentinel, along with related case commentary. You can also manually raise a case in P2 Explorer.

Sentinel has configuration options for raising cases for certain events, under specific conditions.

In P2 Explorer, cases can be automatically prioritised daily, according to a set of configurable rules.

In P2 Explorer, cases can be pushed through various statuses (New, Investigating, Rejected/Confirmed, Closed, Deprecated), with each case assigned to a single user at a time. Cases can be re-assigned at any stage, and comments can be added to a cases. Editing cases is covered in the online help, the Help Center, at https://e4helpcenter.petroleumplace.com/help/cases/.

Case Management Configurations

Case Management in P2 Sentinel can be configured at various levels, and can also be overridden in places.

Case Management Enabled or Disabled

Case Management is optional in P2 Sentinel, and is enabled in the P2 Sentinel configuration file. Refer to the "**Update the Configuration Files**" section in the *P2 Sentinel Installation and Administration Guide*.

This affects what is shown in the User Interface.

Aggregate Cases

The second level of configuration is at a **Category** level.

This option is configured and updated separately (refer to the *P2 Sentinel Installation and Administration Guide,* in the section: **Case Management**), and cannot be changed from within the Sentinel application.

If Aggregate Cases is enabled for a category, and there are open cases for the category, then no new cases are raised by Sentinel for that category; instead, a comment is added to the most recent open case of that category. The comment includes the following details:

```
Event Raised:
[Comment from the originating test's case options]
```

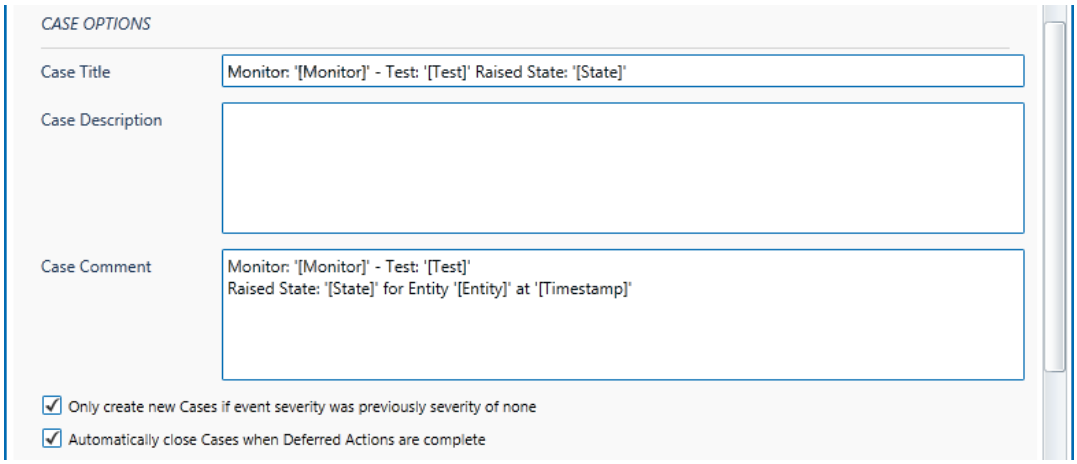
When there are no open cases for the category, a single case for that category can be raised.

Note: Every monitor belongs to a category. When a case is raised, it gets its monitor's category.

Case Options

Case options have default values that are defined in the Sentinel Configuration file. These values can be overridden in Sentinel, per Test. Refer to the "**Update the Configuration Files**" section in the *P2 Sentinel Installation and Administration Guide* for the Case Management defaults.

Case Options can be updated in a Test, and will affect all cases that are raised when the test runs.



Case Options in a Test

Case Title

This is the default title that Sentinel generates when a case is raised with an event, and appears in the case details in P2 Explorer. This is defined in the Sentinel configuration file, but can be updated for a Test.
Setting in the Sentinel Configuration file: **DefaultCaseTitle**

Case Description

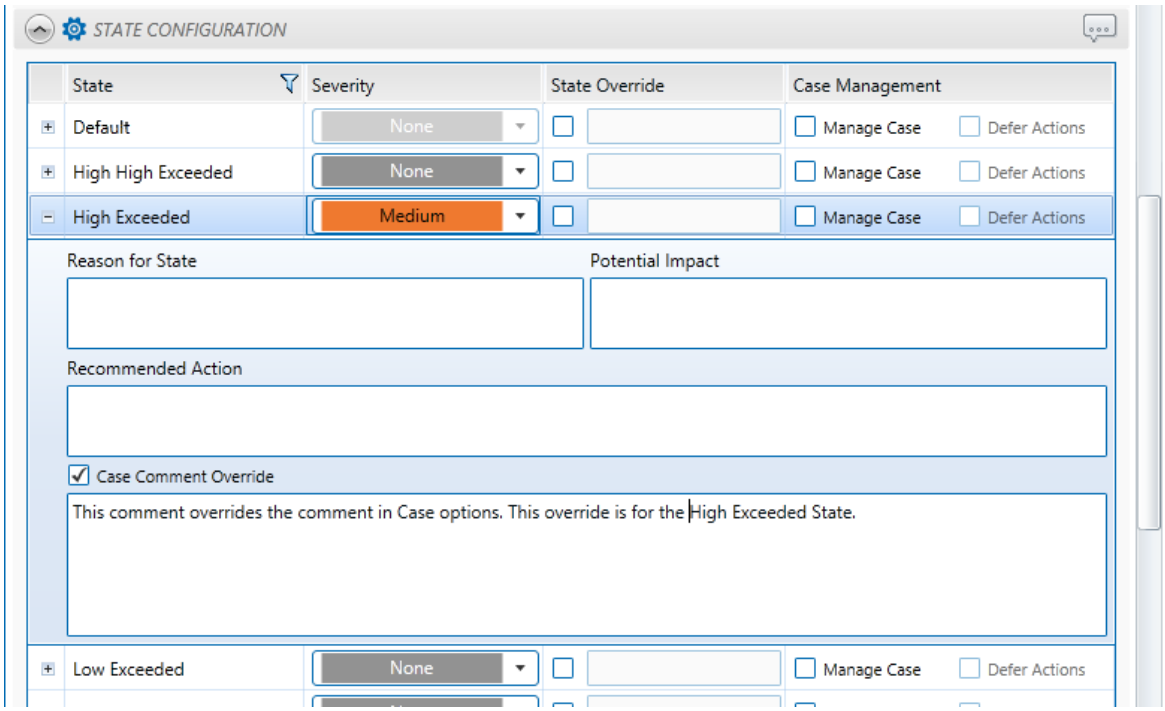
This is the default description that Sentinel generates when a case is raised with an event, and appears in the case details in P2 Explorer. This is defined in the Sentinel configuration file, but can be updated for a Test.
Setting in the Sentinel Configuration file: **DefaultCaseDescription**

Case Comment

This is the default comment that Sentinel generates when a case is raised with an event, and appears in the case details in P2 Explorer. This is defined in the Sentinel configuration file, but can be updated for a Test.
Setting in the Sentinel Configuration file: **DefaultCaseComment**

Case Comment Override

When you set up the state configuration for a test, you can override the test's Case Comment, for a specific state.



Case Comment Override for the High Exceeded State in a Test

Only Create New Cases if Event State was Previously Severity of None

If this option is selected, a case is only raised if the event state has had a severity of **None** since the last case was raised.

Setting in the Sentinel Configuration file: **OnlyCreateCasesDefaultOption**. This is selected by default if specified as **True** in the Sentinel Configuration file.

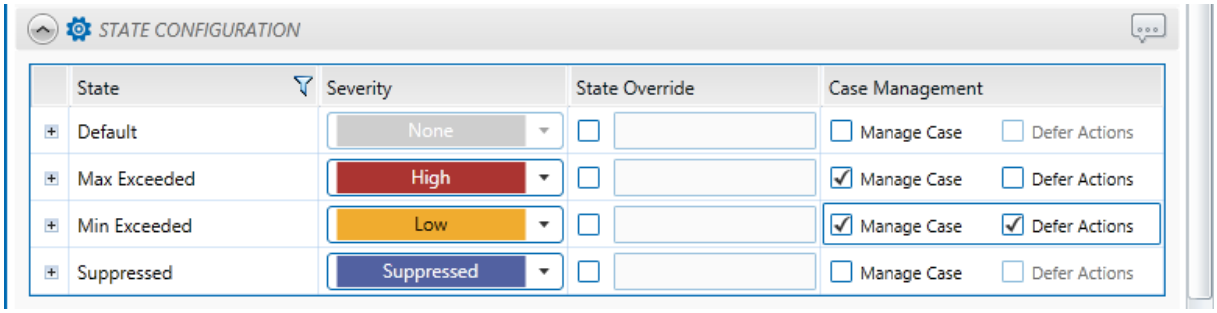
Automatically Close Cases When Deferred Actions are Complete

If this option is selected, Sentinel automatically closes a case after it is confirmed (a user sets a case to confirmed in P2 Explorer). If there are deferred actions set for the event, Sentinel closes the case after it carries out the actions.

Setting in the Sentinel Configuration file: **AutoCloseCasesAfterConfirmation**. This is selected by default if specified as **True** in the Sentinel Configuration file.

Manage Case for a State

At this level, you can configure Sentinel to raise a case with the event. If you select this option, then Deferred Actions is also an option. Sentinel will defer all actions for the state until the case is confirmed. If the case is rejected, the actions will not happen at all.



The State Configuration for a Test. Manage Case selected here for Max Exceeded and Min Exceeded, with Defer Actions for Min Exceeded.

Case Priorities

Priority rules can be set at a Category level, by a System Administrator. If a case belongs to a category that has prioritisation rules defined, its priority may be updated by the system during the daily Server service run. Every case is evaluated against a defined set of conditions particular to a category, and given a priority based on this evaluation.

Each new case is immediately prioritised according to the rules. If there are no rules that apply to the case, it is given a priority value of 10, which is the lowest priority. Thereafter, the case is re-prioritised every day along with all the other cases, during the Server service run.

For more information, refer to the *P2 Explorer Installation Guide*, section '**Appendix 1. Case Management**'.

Viewing and Updating Cases in Explorer

Explorer provides an interface to all of the cases raised in Sentinel or other source applications. Cases can also be manually added from within Explorer. Users with **Case** privileges can update cases and add commentary, in the case details and case commentary, in P2 Explorer.

For more on Cases and case privileges in Explorer, refer to the online help: **Explorer Help Center:** https://e4helpcenter.petroleumplace.com/help/cases/

Case Management URLs

The URL command for the opening a case in Explorer is:

Error! Hyperlink reference not valid. where [server name] is the name of the Explorer Server and [CaseId] is the case's ID.

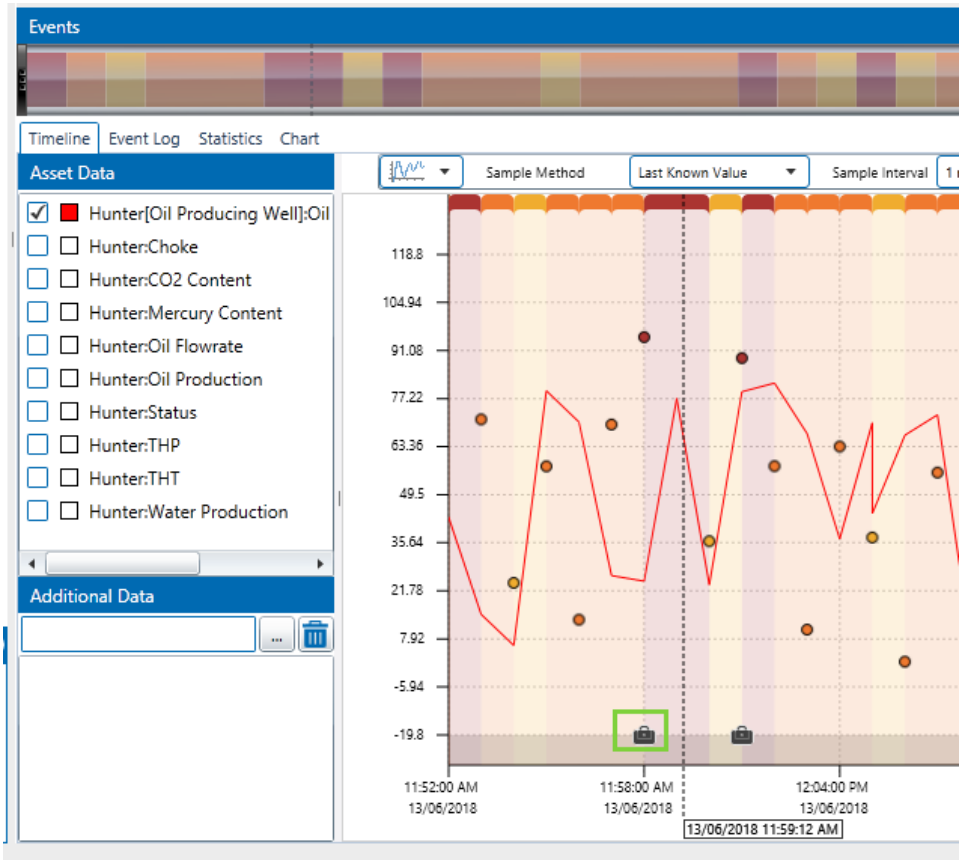
Managing Cases in a Test

If Case Management is enabled in Sentinel, you can configure the various states in a test to use it. This is detailed in section 3.6 Configure States.

Cases and Events

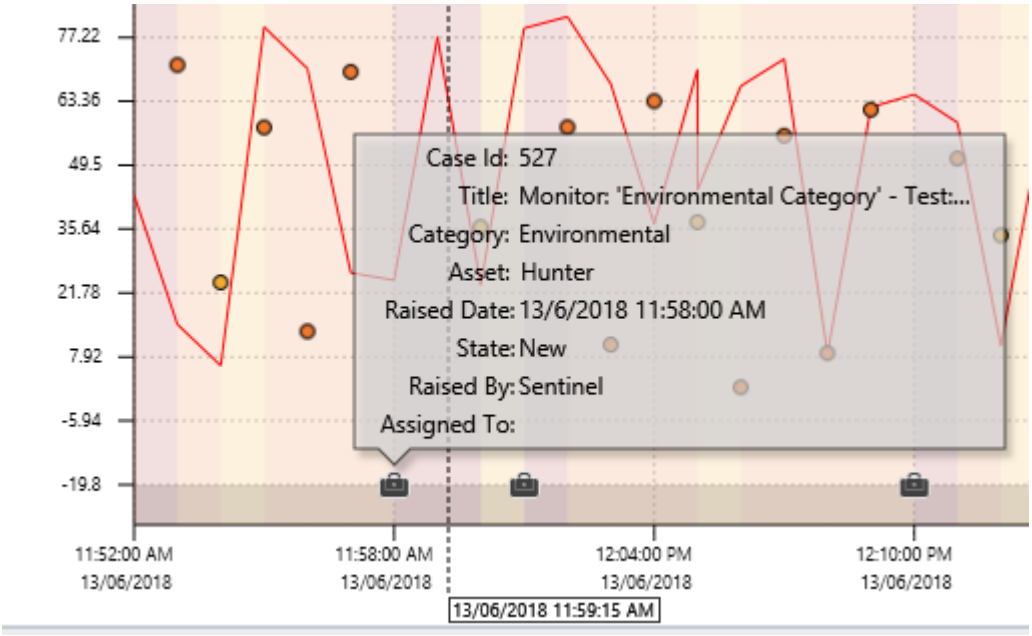
When an event is raised in Sentinel, a case will also be raised if the test's states have been configured for Case Management, and if the configured conditions are met.

The Events Grid shows a status for each event, based on the related case (or an *Unknown* status if there is no related case). If an event has a related case, the event status is **Unknown** until the case has been investigated. If the case is rejected (case status Rejected) the status becomes **Invalid**; if the case is confirmed (case status Confirmed), the event status is **Valid**. Cases are also displayed on the Event Timeline, in the Asset Reports. Cases details can be located using the Case Icon along the bottom of the timeline chart.



A Case Icon along the X Axis

- Click the case icon to open the case details.



A Case Icon along the X Axis

Change Management

Privileges: To submit a monitor for approval (or to unsubmit it) you need a security role that has the **Sentinel Workspaces Edit** privilege.

Change management is optional in P2 Sentinel, and is enabled in the P2 Sentinel configuration file. Refer to "**Update the P2 Sentinel Configuration Files**" section in the *P2 Sentinel Installation and Administration Guide*.

Note: Change management is disabled, by default.

The change management process ensures that new monitor versions are approved before they can run.

Note: The current approved version of the monitor continues to run, until the new approved version is ready.

SCENARIOS OF CHANGES TO MONITORS UNDER CHANGE MANAGEMENT

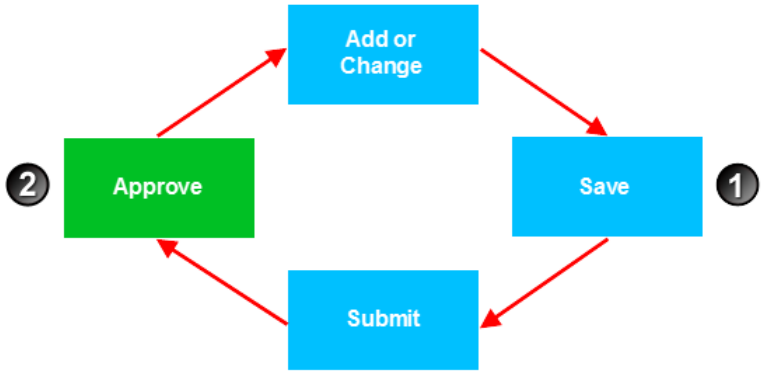


***Figure 3: Approve changes. Run on** new major version*

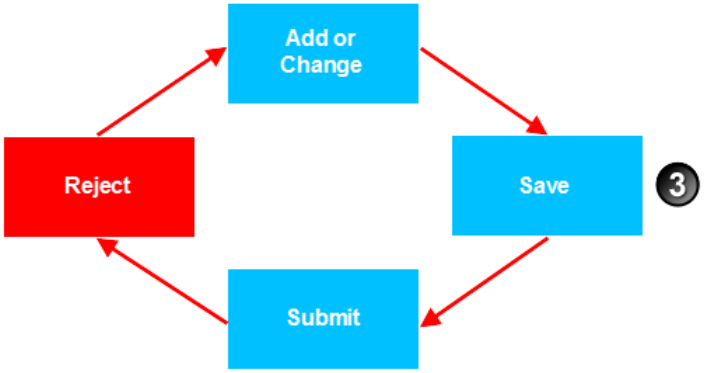


***Figure 4: Reject changes. Run on** previous major version.*

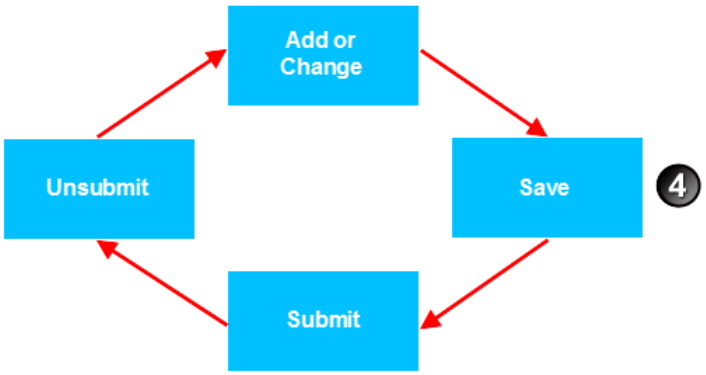


Figure 5: Unsubmit changes. Run on** previous major version**.

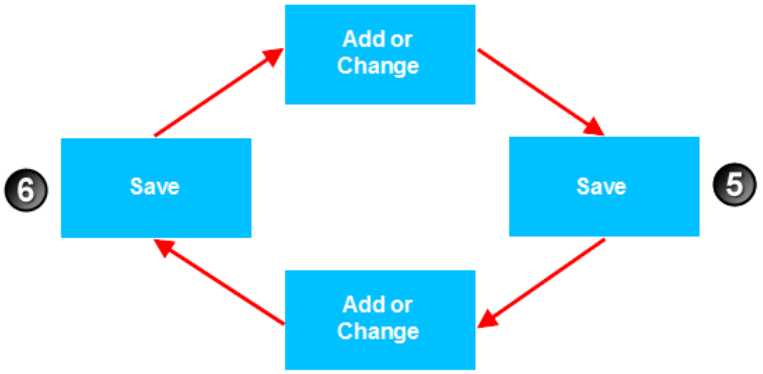


Figure 6: No submission. Run on** previous major version**.

Figure	What has happened	Version Outcome	
Figure 3	Changes are saved, submitted for approval, and **approved**.	1	New **Minor** version created.
		2	New Major Version created.
Figure 4	Changes are saved, submitted for approval, and **rejected**.	3	New **Minor** version created.
Figure 5	Changes are saved, submitted for approval, and **unsubmitted**.	4	New **Minor** version created.
Figure 6	Changes are saved, changed, and then **saved** again.	5	New **Minor** version created.
		6	New **Minor** version created.

MONITOR CHANGE MANAGEMENT PROCESS

If change management is in place, the following steps need to be taken before the monitor runs at the new version:

Submit monitor for approval

The person making the changes to the monitor submits the monitor for approval after saving changes. The monitor is assigned with the next *minor* version number. If it is an existing monitor, it continues running at the previous major version.

Awaiting approval

After submission, the monitor awaits approval. The monitor details appear in the *My Tasks* panel task list of personnel who have approver privileges for the workspace in which the monitor is stored.

Note: You cannot edit the monitor while it is awaiting approval. To edit, first unsubmit the monitor.

Approve or reject monitor

A person with approver privileges for a particular workspace can view pending approvals for that workspace, and can approve or reject the relevant monitors.

Note: Personnel with approver privileges have a list of monitors requiring approval in their *My Tasks* queue.

New version

As soon as the monitor is approved, it acquires a new major version number, and continues running at the new major version. Rejected monitor changes must be revised before the change management process is repeated.

Refresh

When you try to edit or view a monitor that has had a major version change, you need to refresh the latest version changes before you can save any further changes.

Major and Minor Versions

Minor versions are only used if the installation is configured to use change management.

Versions with change management

When change management is in place, monitors are saved with a new **minor** version number, whereby the digit after the decimal point is incremented by 1 (for example version 3.1 moves to version 3.2 after a save, and then to version 3.3, and so on).

After the new monitor version is approved, the next version number is a **major** version number, replacing the last *minor* version number (for example, minor version number 3.5 becomes major version number 4.0). The major version number is incremented by 1 (for example, if the last major version number was 3.0, the next major version number is 4.0).

Versions without change management

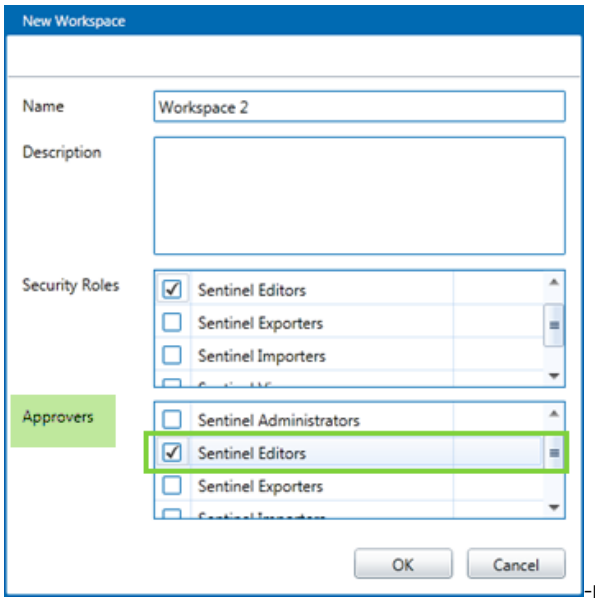
When there is no change management, the version numbers are whole integers that increment by one with every new save.

Approvers

The *Approvers* role only applies if change management is in place.

Privileges: To approve submitted monitors, you either need a security role that has the **Workspaces Approve** privilege (allowing you to approve any submitted monitor), **or** you need privileges to approve monitors within a specified workspace.

Approvers for a workspace are personnel belonging to any of the selected roles, for example, Sentinel Administrators, that have been assigned to the **Approvers** list for that workspace.



-run

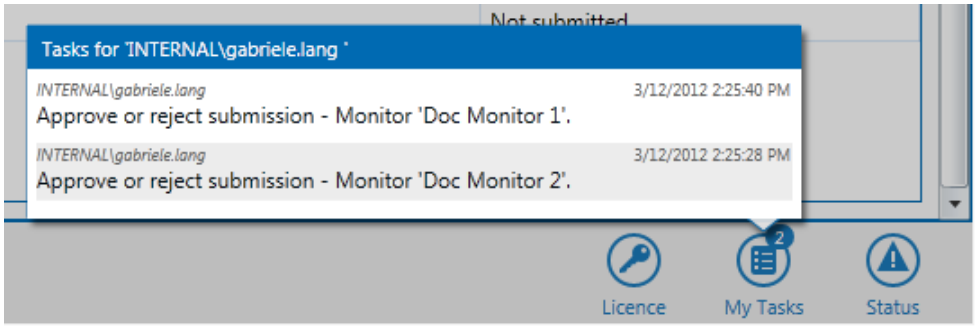
In the example above, Workspace 2 has the **Sentinel Editors** role selected as approvers. Users that have this role can approve any submitted monitors in this workspace.

When a monitor has been changed and is awaiting approval, approvers can view the monitor and approve or reject the new minor version.

My Tasks

My Tasks is a panel containing a list of various tasks. Every user has their own list of tasks; this list depends on which tasks have been assigned to the user, and can be empty.

Note: Users may share tasks, for example where several users have approver privileges for a particular workspace which contains monitors awaiting approval.



The **Tasks** panel consists the following:

Heading
Tasks for [user.name].

List of tasks
A list of tasks that the user can address.

CHANGE MANAGEMENT TASKS

A change management task contains details of *monitors awaiting approval*. Every user has their own list of change management tasks, and this list depends on their approver privileges for the various workspaces, as well as on the monitors that are awaiting approval. The list can be empty.

Note: A change management task may appear in the task list of more than one user.

A change management task appears as follows:

User name
The name of the user who submitted the monitor for approval.

Time
The date and time that the monitor was submitted for approval.

Description
A description of the task, including the monitor name, for example, *Approve or reject submission - Monitor 'Doc Monitor 5'*.

Licensing

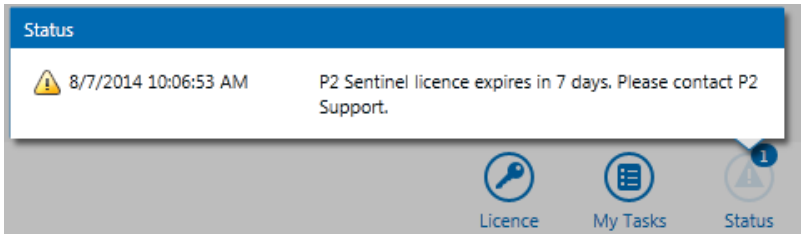
In P2 Sentinel, there is a licence expiry date for the P2 Sentinel engine and for each P2 Sentinel process. In addition, each process licence has a link to a licence group, which has its own volume limit. See Process Entity Volumes and Licence Groups in Processes.

Licence Usage

The Licence tab shows Licence group allocations, and licence usage, from Process group level down to Test level. To view the current state of P2 Sentinel licences, click on the Licence icon on the lower right of the Main panel.

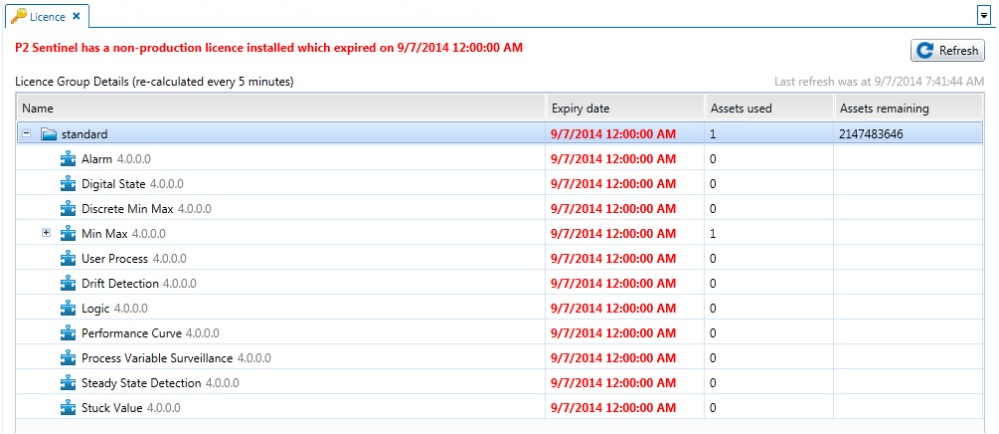
Licence Expiry

When the engine licence is within 21 days of expiry, a warning message appears in the **P2 Sentinel Status** panel and the **About** box.



The following behaviour can be expected when a licence expires:

- When a process licence expires, monitors that use that process display a licence error status message.
- On the Licence Tab, the expiry date font, for the affected licence, is **red**.



When the engine licence expires, the engine continues to run. However if it stops for any other reason it cannot be restarted until the licence is renewed.

Note: Please see your System Administrator regarding licence renewal.

Volume Limit

P2 Sentinel uses one or more licence groups to define volume licensing for the various available processes. Each licence group has a defined volume limit.

Each process in P2 Sentinel belongs to a single licence group. This is arranged as part of the licence agreement procedure. Collectively, all processes within a licence group share the volume limit of that group. The limit is specified as the **count** for the licence group.

Points to note:

- If a particular test has caused the group volume limit to be exceeded, the test will stop running until the volume limit is no longer exceeded.

  Possible causes are:

  - A change in the number of assets using the test.
  - If this is a new test that uses a process.

- Monitors display a licence error status message, if they use a process belonging to a licence group of which the volume count is exceeded.

Note: Entities are not counted (as part of volume limit calculations) where they are used by tests in disabled monitors.

LICENCE WARNING

When the engine licence approaches its expiry date, a message appears in the monitor status panel, stating the licence name and how many days remain on the licence. This message appears when there are less than 21 days before expiry.

NOTIFICATION EMAILS

Licence notifications can be sent to an administrator email account (as specified in the P2 Sentinel configuration file). Emails are sent at specified intervals (also set in the configuration file) after a Licence Group volume limit has been exceeded.

Managing Workspaces

Privileges: To add or edit a workspace you need a security role that has the **Sentinel Workspaces Edit** privilege. To delete a workspace, you need a security role that has the **Sentinel Admin** privilege.

Workspaces are provided as a way for you to logically group monitors into a hierarchy that makes sense for your site. Workspaces are described only by a *name* and *description*, and you can create as many as you need for your site.

Next to each workspace in the Workspace panel is an event notification label, showing the total number of current non-default events for all monitors in that workspace. The number is colour-coded to display the highest severity of event occurring within the workspace.

Note: There could be more than one event notification label, if you have de-selected the option **Combine severities into a single count** in the **Event Display Options**.

If a workspace contains a monitor with a status message, this is displayed next to the workspace.

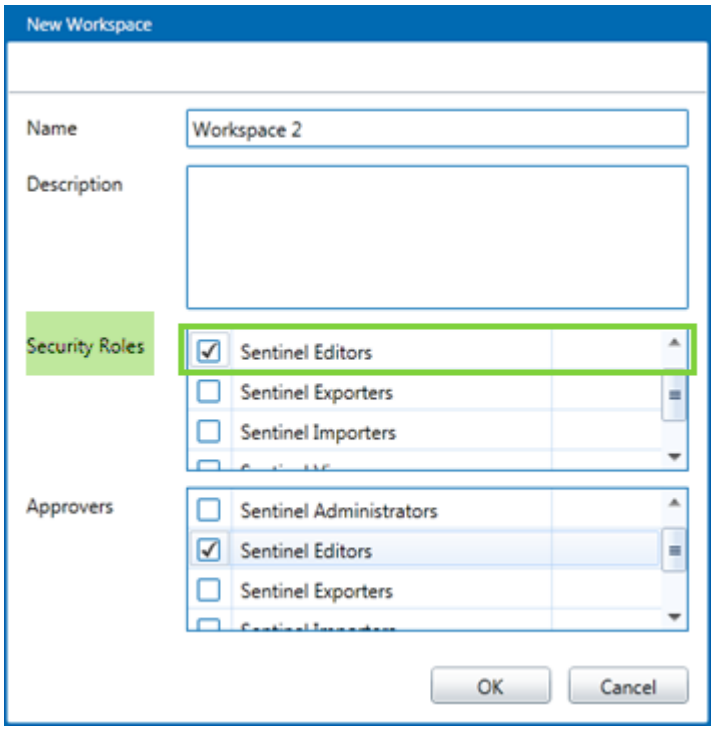
You can perform the following actions on a workspace:

- Add a new workspace.
- Edit the workspace name and description.
- Remove the workspace from P2 Sentinel. You can only delete a workspace that has no folders or monitors.

Workspace Security Roles

To see a workspace in the Workspace panel, you either need a security role that has the **Workspaces View** privilege (allowing you to view all public workspaces), **or** you need privileges to view a specific workspace.

Workspace viewers are personnel belonging to any of the selected roles, for example, Sentinel Editors, that have been assigned to the **Security Roles** list for that workspace.



In the example above, Workspace 2 has the **Sentinel Editors** role selected as Security Roles. Users that have this role can view all folders and monitors in this workspace.

Note: All roles in Security are listed under both the **Security Roles** and **Approvers** panels in the workspace.

These are the levels of workspace access:

- Users who have a role selected in **Security Roles** for a workspace, have access to that particular workspace.
- Users who have a role with the **Sentinel Workspaces View** privilege have access to all workspaces, excluding private workspaces.
- Users who have a role with the **Sentinel Workspaces Edit** privilege have access to all workspaces, excluding private workspaces. They can also:
  - Add and edit workspaces
  - Add and edit folders
  - Submit monitors for approval (and unsubmit)
  - Add and edit event views
- Users who have a role with the **Sentinel Admin** privilege have access to all workspaces, including private workspaces. They can also:
  - Set Security Roles in workspaces
  - Set Approvers in workspaces (where Change Management is enabled)
  - Delete workspaces, folders, monitors

  Note: the Sentinel Admin privilege cascades into all of the Sentinel module privileges.

Workspace Approvers

The Workspace Approvers function is only applicable when Change Management is enabled.

When a new workspace is added or edited, approvers for that workspace can be selected in the **Approvers** panel. Note that users with a security role that has the **Workspaces Approve** privilege can approve any submitted monitor.

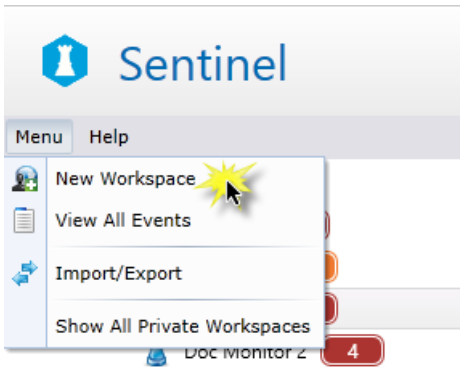
Note: The **Approvers** list is only available if Change Management has been implemented.

For more about Approver privileges, see Approvers.

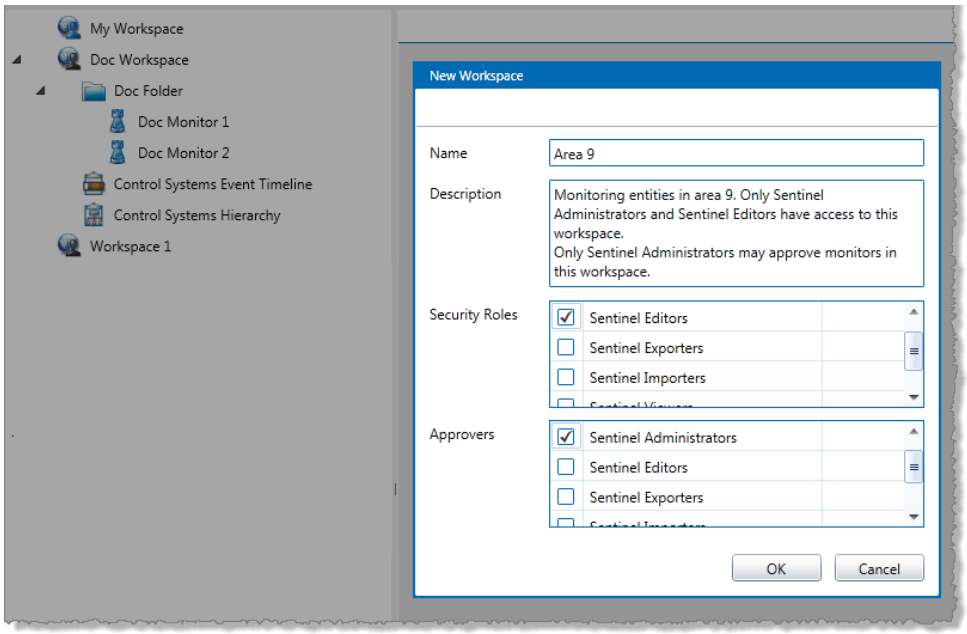
Add a Workspace

To add a new workspace:

1. Click the Menu button below the Sentinel header.
2. Click **New Workspace**.



A **New Workspace** dialog box opens in the Main panel:



3. In the **New Workspace** dialog box:
   a. In the **Name** text box, type a name for the new workspace.

b. In the **Description** text box, type a description for the new workspace.

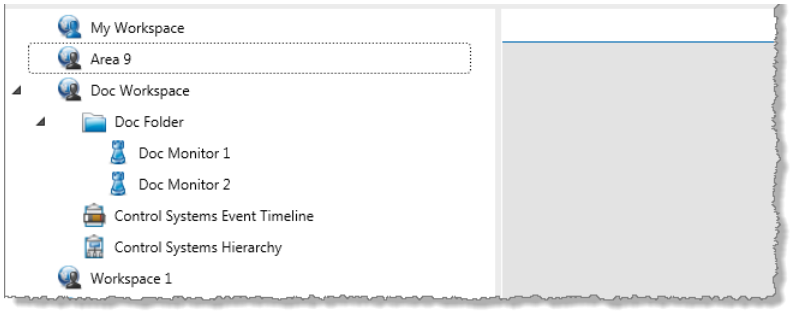
c. Assign workspace security roles in the Security Roles group.

d. Assign approvers, in the Approvers group.

> **Note:** The *Approvers* section is only applicable where P2 Sentinel has been configured to use Change Management. Refer to "**Update the P2 Sentinel Configuration File**" in the *P2 Sentinel Installation and Administration Guide*.

e. Click **OK** to save the new workspace.

The new workspace appears in the Workspace panel.



Notes: Workspaces are alphabetically ordered in the workspace panel, with the exception of My Workspace, which appears at the top of the list. **My Workspace** is automatically created by the system.

Edit a Workspace

Editing a workspace is similar to adding a new one.

> **Note:** You cannot edit any of the private workspaces, for example *My Workspace*.

1. In the Workspace panel, right-click on the **workspace** that you want to edit.
2. Select **Edit** from the list.

   The workspace page opens in the Main panel.
3. Update the **Edit Workspace** page as required:
   - Change the name in the **Name** box.
   - Change the description in the **Description** box.
   - Change security roles by selecting the relevant **Security Roles** check boxes.
   - If Change Management is in use, you can change approvers by selecting the relevant **Approvers** check boxes.
4. Click **OK** to save.

   Your changes to the workspace are saved.

Delete a Workspace

> **Privileges:** To delete a workspace you need a security role that has the **Sentinel Admin** privilege.

You will only be able to delete a workspace that contains no folders, monitors, or event views.

Note: You cannot delete private workspaces, for example *My Workspace*.

1. In the Workspace panel, right-click on the **workspace** that you want to delete.
2. Select **Delete** from the list.
3. Click **Yes** at the prompt.

   The workspace is removed.

Clear Messages for a Workspace

Privileges: To clear messages for a workspace, you need a security role that has the **Sentinel Workspaces Clear Messages** privilege.

To clear all status messages from the monitor status log, for every monitor within a particular workspace:

1. In the Workspace panel, right-click on the **workspace**.
2. Select **Clear Messages** from the menu.

   The status messages are deleted, for the workspace.

Note: Only user with appropriate privileges can perform this function.

Adjust the Event Display Options

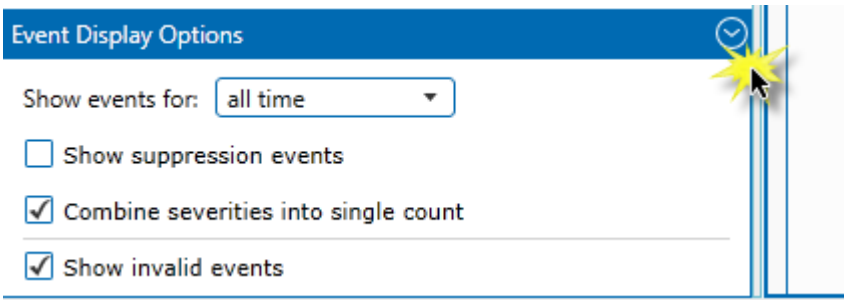
The event display options determine which current events are counted and then displayed in the event notification labels.

Based on the time selection (in the **Show events for** drop-down list), events are counted or not counted depending on when they occurred. For example, if a current event started two hours ago, and the *last 48 hours* option is selected, this event is **not** included in the count.

Suppression events are only included in the count if the *Show suppression events* option is selected.

Depending on the selection of *Combine severities into a single count*, the event count is either a single total for that workspace / folder / monitor, displayed in a single event notification label, or it is grouped into separate counts for the different severities. When severities are not combined, each severity has its own event notification label (if the count is greater than zero).

- To close the Event Display Options panel, in the Workspace panel, click the *collapse arrow*.



- To open the Event Display Options panel, in the Workspace panel, click the *expand* arrow on the Sentinel footer.

CHOOSE EVENTS PERIOD

- Select a period from the **Show events for** drop-down list. The options are:

all time
Shows the count for all current events regardless of when they started.

today
Shows the count for current events that started today.

this week
Shows the count for current events that started within the last week.

this shift
Shows the count for current events that started during the current shift.

last 12 hours
Shows the count for current events that started during the last 12 hours.

last 24 hours
Shows the count for current events that started during the last 24 hours.

last 48 hours
Shows the count for current events that started during the last 48 hours.

Note: *today*, *this shift* and *this week* are all based on the P2 Server that define the "start of day offset" (**StartOfDayOffsetMin**), as well as "first day of week" (**FirstDayOfWeek**)and "shift length" (**ShiftHrs**). Please see your P2 Server Administrator if you are unsure of these settings.

SHOW SUPPRESSION EVENTS

- To include suppression events in the event count, select the **Show suppression events** check box. Note that suppression events are displayed in the Events Grid regardless of this selection.

COMBINE SEVERITIES

- To combine severities into a single count, displayed in a single event notification label, select the **Combine severities into single count** check box.

Figure 7: Example of severities combined in a single count

Figure 8: Example of severities shown in separate counts

SHOW INVALID EVENTS

An invalid event is one that raised a case which was subsequently investigated and rejected. The event status is *Invalid*. Other event statuses are *Unknown* and *Valid*.

- To include invalid events in the event count and in the Events Grid, select the **Include Invalid Events** check box.

Note: Event Status is only applicable where Case Management is enabled. The **Show Invalid Events** option is greyed out if Case Management is disabled.

View Pending Approvals

Approval or rejection of monitors is part of Change Management, and only applies if P2 Sentinel has been configured to use change management. See Approvers to see who can approve or reject monitors.

To approve or reject monitors that require approval within a workspace, follow these instructions.

1. In the Workspace panel, right-click on the relevant **workspace** .
2. Select **View Pending Approvals** from the list. (This menu option is only available if you have approver privileges for the workspace.)

   The **Pending approvals page** opens for the workspace. The page contains a list (if any) of all *pending approval* monitors in this workspace.
3. Approve or reject the various monitors, as shown in the following section.

Note: You can also approve or reject monitors awaiting approval from My Tasks.

Approve or Reject a Monitor

The **Pending approvals** list contains the following information for monitors awaiting approval:

Action

This column contains an **Approve** button, and a **Reject** button.

Item
The monitor name.

Version
The minor version number of the monitor; this is the version that requires approval.

User
The username of the person who added or changed the monitor to create this minor version.

Time
The date and time that the version was saved.

Comment
The approval / rejection comment.

Approval Comment
This is the comment that is added when the pending monitor changes are approved. This comment is mandatory if the approval comments setting, *ApprovalCommentsRequired*, is set to *True* in the Sentinel configuration file.

Rejection Comment
This is the mandatory comment that is added when the pending monitor changes are rejected.

APPROVING OR REJECTING THE MONITOR VERSION

1. Locate the monitor whose latest version you want to approve or reject.

   Tip: To open the monitor page from here, hover the mouse over the monitor name, and click on the *View Version*  icon that appears.

   To approve the new version:

   a. Click **Approve**.

      If the approval comment is mandatory (as defined in the Sentinel configuration file), the **Approval reason** screen appears.

   b. In the **Reason** edit box, type an approval reason. Then click **OK**.

   The monitor version is approved, and the version number changes to a *major* version number.

   The monitor is removed from the list of pending approvals.

   To reject the new version:

   a. Click **Reject**.

      The **Rejection reason** screen appears.

   b. In the **Reason** edit box, type a rejection reason. Then click **OK**.

      The monitor version is rejected, and the minor version number is retained.

      The monitor is removed from the list of pending approvals.

2. Continue approving or rejecting the remaining monitors on the list, as described in the previous step.

APPROVE ALL

If there is more than one monitor pending approval within a single workspace, you can approve all monitors in a single batch. This is particularly useful for when you have imported several monitors that all require approval. All approvals done in this way have the same approval comment.

To approve all pending approval monitors within a workspace:

1. Click **Approve All**, located above the approvals grid, in the pending approvals tab for that workspace.

   If the approval comment is mandatory (as defined in the Sentinel configuration file), the **Approval reason** screen appears.

2. In the **Reason** edit box, type an approval reason. Then click **OK**.

   The monitor version for each of the pending monitors in this workspace is approved, and the version number for each of these monitors changes to a *major* version number. If a reason was supplied, this applies to all of the approved monitors.

The pending approvals tab closes.

Show All Private Workspaces

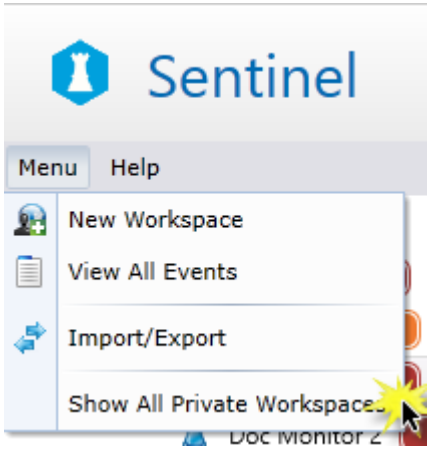
Privileges: To view all private workspaces, you need a security role that has the **Sentinel Admin** privilege.

Whereas most users are only able to see their own private workspace, only users with appropriate privileges to see **all** private workspaces within the P2 Sentinel system, to view, edit and move the monitors, folders and event views in these private workspaces, and also to view the events raised within these private workspaces.

A possible reason for moving a monitor to another workspace is when the owner of the originating private workspace is unable to work on the monitor for a while. The monitor can be worked on by another user within their own private workspace, if it has been moved there by a Sentinel Administrator. A Sentinel Administrator may also choose to disable or edit a monitor within a private workspace if it causing performance issues.

To gain access to all private workspaces:

1. Click the **Menu** button below the Sentinel header.
2. Click **Show All Private Workspaces**



Note: This menu option is only visible to Sentinel Administrators.

The menu closes, and all private workspaces appear in the Workspace panel. The private workspaces are ordered alphabetically under "My Workspace", and before public workspaces. Private workspaces are named as: "[UserName]'s Private Workspace". For example "Jo Smith's Private Workspace".

- To remove your access to all private workspaces, repeat the steps above.

Note: When you have access to all private workspaces, the item **Show All Private Workspaces** in the menu is preceded by a *tick* symbol.

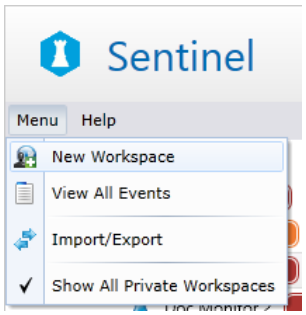


Figure 9: A tick symbol precedes *Show All Private Workspaces*

Managing Folders

Privileges: To add or edit a folder you need a security role that has the **Sentinel Workspaces Edit** privilege. To delete a folder, you need a security role that has the **Sentinel Admin** privilege.

Folders provide further organisation in the Workspace panel.

You can perform the following actions on a folder:

- Add a new folder.
- Edit the folder name and description.
- Delete the folder from P2 Sentinel. You can only delete a folder that has no sub-folders or monitors.
- Move a folder to a different workspace, or to a different folder.
- Clear all status messages for a folder.

- To view the folders in a workspace, or in another folder, click the expander arrow next to the workspace or the folder.

Add a Folder

You can add a folder to a workspace, or to another folder.

1. In the Workspace panel, right-click on the **workspace** or **folder** where you want to add a new folder.
2. Select **New Folder** from the list.
3. In the **New Folder** dialog box:
   a. Type a name in the **Name** box.
   b. Type a description in the **Description** box.
   c. Click **OK**.

The new folder is saved under the selected workspace or folder.

Edit a Folder

1. In the Workspace panel, right-click on the **folder** that you want to edit.
2. Select **Edit** from the list.

   The **Edit Folde**r dialog box appears.
3. Change the details as required:
   – Change the name in the **Name** box.
   – Change the description in the **Description** box.
4. Click **OK**.

   Your changes to the folder are saved.

Delete a Folder

You can only delete a folder that contains no sub-folders, monitors, or event views.

1. In the Workspace panel, right-click on the **folder** that you want to delete.
2. Select **Delete** from the list.
3. Click **Yes** at the **Delete Folder** prompt.

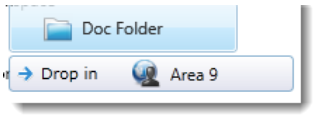
   The folder is deleted.

Move a Folder

You can move a folder to a different workspace, or to another folder.

1. In the Workspace panel, click on the **folder** that you want to move.
2. Drag the folder to the destination workspace or folder.

   Tip: 'Drop in' and the destination workspace or folder is displayed when the folder you are moving is correctly positioned.

3. Release the mouse button.

   The folder is moved to the destination workspace or folder.

Note: The configuration of sub-folders and monitors beneath this folder remains the same. All sub-folders and monitors for this folder are moved with the folder.

Clear Messages for a Folder

Privileges: To clear messages for a folder, you need a security role that has the **Sentinel Workspaces Clear Messages** privilege.

To clear all status messages from the monitor status log, for every monitor within a particular folder:

1. In the Workspace panel, right-click on the **folder**.
2. Select **Clear Messages** from the menu.

   The status messages are deleted, for all monitors within the folder.

Note: Only users with appropriate privileges can perform this function.

Working with Monitors

Privileges: To add or edit a monitor you need a security role that has the **Sentinel Workspaces Edit** privilege. To delete a monitor, you need a security role that has the **Sentinel Admin** privilege.

Monitors contain tests, each of which runs through a specified process which raises events when pre-defined limits are exceeded, or when pre-defined states are reached.

Setting up the monitor

You can perform the following actions on a monitor:

- Add a new monitor.
- Edit a monitor.
- Remove the monitor from P2 Sentinel.
- Move a monitor to a different folder, or to a different workspace.
- Approve or reject a monitor version.
- Delete a monitors events and cases, and reset the states.

Note: *Approval and rejections* functionality is part of Change Management, and is only applicable if P2 Sentinel has been configured to use Change Management.

Viewing Monitor Results

You can view the following for a monitor:

View Events 
View the latest events for the monitor.

View Asset Reports
View asset report for assets that are used by the monitor.

View Status 
View the monitor status.

Copying a Monitor

You can copy a monitor.

Re-Run a Monitor

You can re-run a monitor for any period. If you create a new monitor, you can re-run it for a period before it was created.

Delete Events and Reset

You can delete all the events associated with the monitor, as well as any cases that were raised. This resets all states.

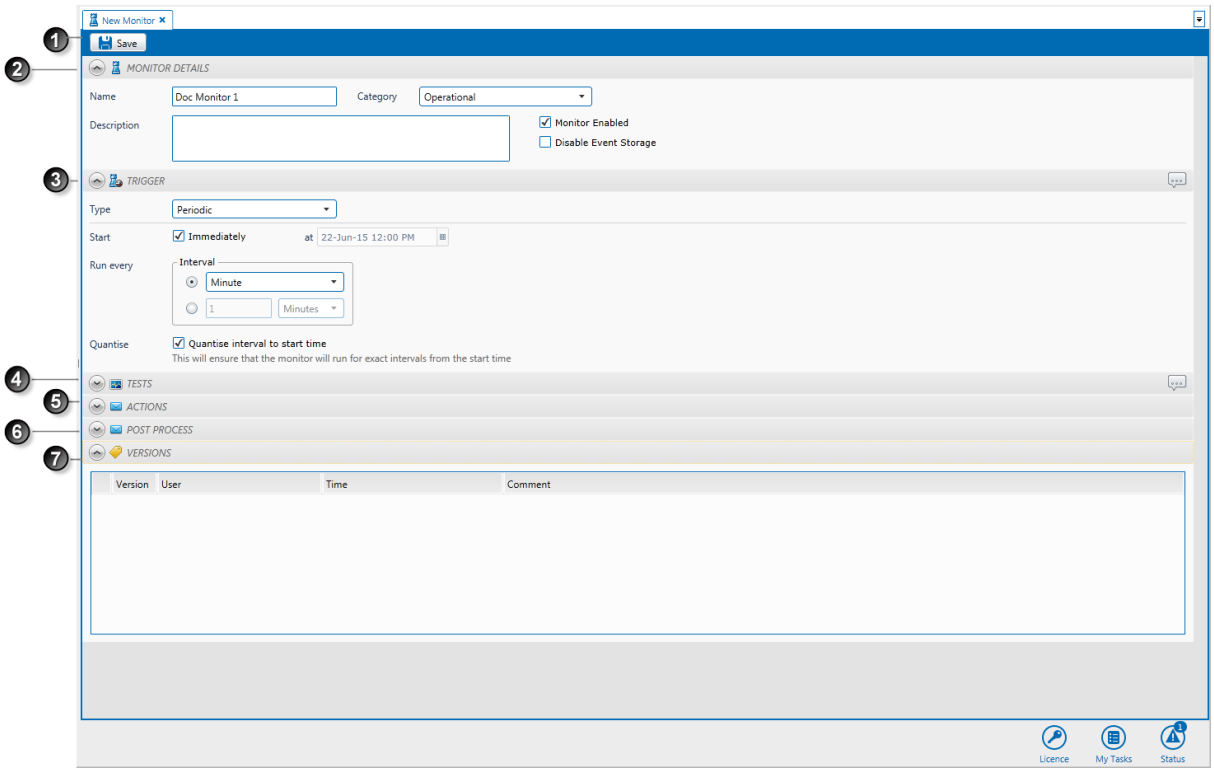
Add a Monitor

You can create a new monitor in a workspace or in a folder. The following steps summarise how to add a monitor.

1. In the Workspace Panel, right-click on the **workspace**  or **folder**  where you want to add a new monitor.

2. Select **New Monitor** from the list.

The **New Monitor** page opens on the Main Panel.



1. Monitor Header
2. Monitor Details panel (expanded)
3. Trigger panel (expanded)
4. Tests panel (collapsed)
5. Actions panel (collapsed)
6. Post Process panel (collapsed)
7. Versions panel (expanded)

Note: The monitor page contains a lot of information. Expand or collapse panels as needed.

3. Define the following (these are further explained in the following sections):

Monitor Details
The name, category, and description of the monitor. You can also enable or disable the monitor from here.

Trigger
This is set up to start the tests in the monitor. The trigger can be time based or condition based, or driven by an external application.

Tests
Define what you want to monitor, how you want to monitor it, which sample intervals to use, and which actions to take under certain conditions.

- Add test details.
- Add a source.
- Add a precondition.

- Add a process.
- Configure states.
- Assign actions.
- Save the test.

Actions
Define monitor actions. Assign actions to various tests.

Post Process
Add a web service, which P2 Sentinel calls when the monitor finishes running.

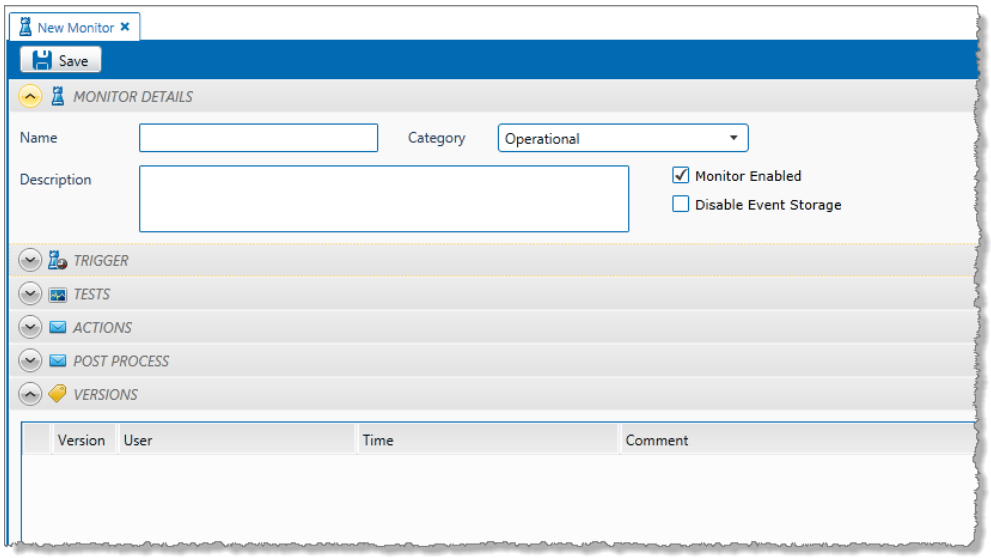
4. Save the monitor.

Note: Alternatively, you can copy an existing monitor as the base for your new monitor.

Step 1. Add Monitor Details

In the **New Monitor** page:

1. Expand the **Monitor Details** panel.



2. Type a name in the **Name** box.

   This is a unique, descriptive name for the monitor. This field is required.

3. Select a category from the **Category** drop-down list.

   The monitor category is used as a filter in reporting. The **Operational** category is the default.

4. Type a description in the **Description** box.

   This is a meaningful description of what the monitor is intended for. The monitor description appears as a tooltip when you hover the mouse over the monitor in the Workspace panel. The description is optional.

5. To ensure that the monitor will process, select the **Monitor Enabled** check box is selected.

   Note: The monitor is enabled by default, unless it is a copied monitor, in which case it is disabled.

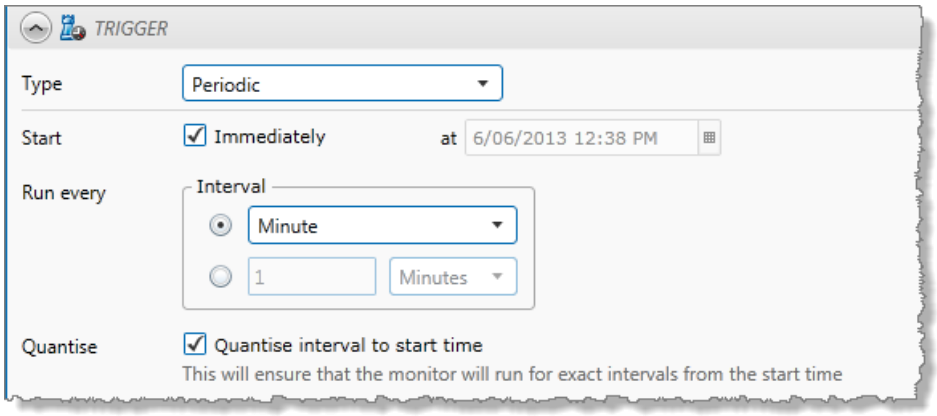
6. If you don't want to store events relating to the monitor, select the **Disable Event Storage** check box.

Step 2. Set a Trigger

You need to define a trigger to ensure that the monitor processing occurs at a specified time, or under specified conditions.

In the **New Monitor** page:

1. Expand the **Trigger** panel.



2. Set the trigger details, following the specific instructions for the trigger that you want to use.

   There are four types of triggers to choose from:

   - Periodic Trigger
   - Date Trigger
   - Monitor Chaining Trigger
   - Application Trigger

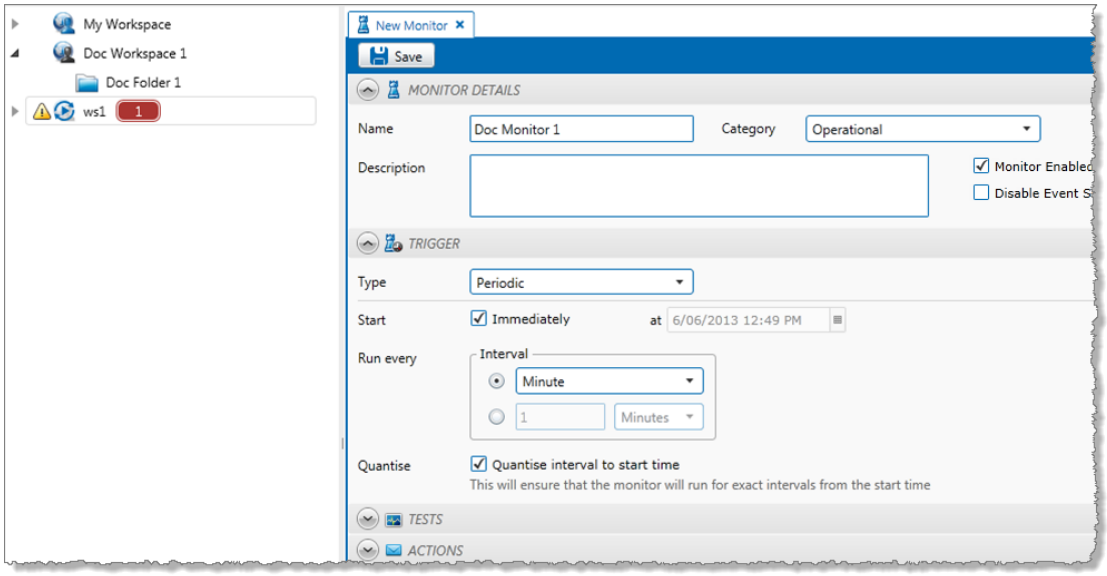
3. Click the comment button on the top right corner of the *Trigger* panel, to add an optional comment, describing the reasons you have chosen to use this trigger.

Setting a Periodic Trigger

Use a periodic trigger to initiate monitor processing at **periodic intervals**.

1. From the **Type** drop-down list, select **Periodic**.

   The **Trigger** panel appearance changes, as shown in the screen image below:



2. Select a start time.

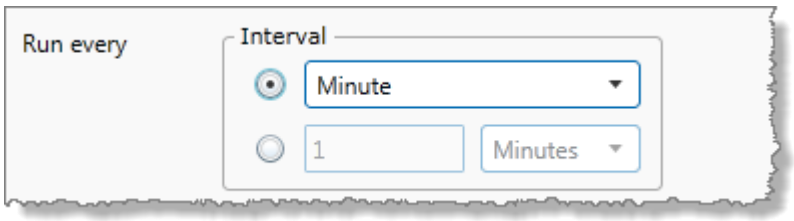
   You can set a periodic trigger to start immediately, or at a specified time in the future.

   – Select the **Immediately** check box to start the trigger immediately.

     Or

   – Click the calendar ▦ icon to select a *Start* date and time for the monitor.

3. Select a time interval in the **Interval** box.



   a. Select the first option button in the **Interval** box, and then select an interval from the corresponding **Interval** drop-down list. This could be a minute, 5 minutes, an hour, a week, and so on, and indicates that the trigger should run every single minute, 5 minute interval, hourly interval, and so on.

      Or

   b. Select the second option button in the **Interval** box. Then type in a number, for example 2, and select *Minutes* or *Hours* from the accompanying drop-down list.

4. To ensure that the monitor is triggered at exact intervals from the *start time*, select the **Quantise** check box.

Tip: To set trigger times that start on the hour or on the minute, set the start time to be exactly on the hour and minute (for example, 19/06/2013 **1:00pm**). With the *quantise* check box selected, the monitor will trigger at exactly every minute, hour, day, etc. (depending on the selected interval) from that time so that your trigger times are, for example, 20/06/2013 **1:00pm**, 21/06/2013 **1:00pm**, 22/06/2013 **1:00pm**, 23/06/2013 1:**00pm**.

The periodic trigger causes the monitor to start at each set interval. The interval period can be a minute, 5 minutes, an hour, a week, or every two hours, every three minutes and so on, depending on the interval settings selected.

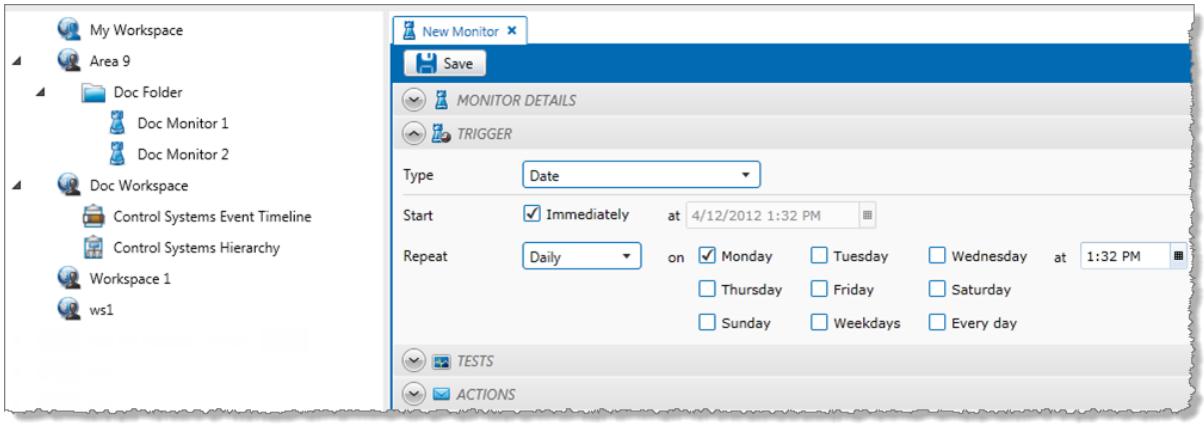
Note: The first trigger time for the monitor is the start time plus the trigger interval. Subsequent trigger start times are the last trigger time plus the trigger interval.

Setting a Date Trigger

Use a date trigger to initiate monitor processing at selected **date intervals**, at a set time.

1. From the **Type** drop-down list, select **Date**.

   The **Trigger** panel appearance changes, as shown in the screen image below:



2. Select a start time.

   You can set a date trigger to start immediately, or at a specified time in the future.

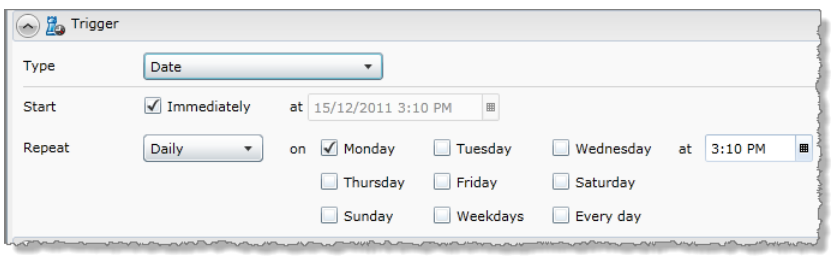
   – Select the **Immediately** check box, to start the trigger immediately.

   – Click the calendar ▦ icon to select a start date and time for the monitor.

3. Select an interval (Daily, Monthly, or Yearly) from the **Repeat** drop-down list.

4. Select the trigger days of the week, days of the month, or days of the year, as appropriate:

   – For a **Daily** repeat interval, every day of the week has a check box, as shown:

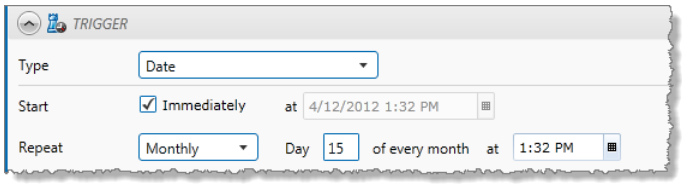


   - Select the **Weekdays** check box to select all days from Monday to Friday.

- Select the **Every day** check box to select every day of the week, from Monday to Sunday.
- Select individual days, for example select the **Monday** check box and the **Wednesday** check box.

The trigger runs the monitor tests on all of the selected days, at the specified run time.

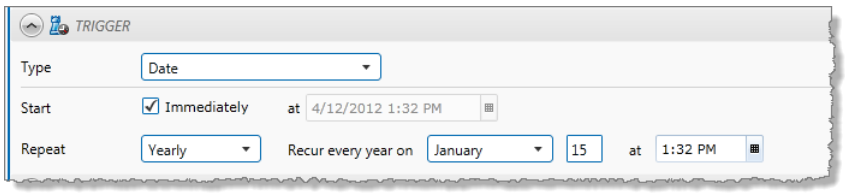
– For a **Monthly** repeat interval, type a valid day (1 to 31) of the month in the **Days** box, to select which days of every month to trigger the monitor tests.



The trigger runs the tests on the specified day of every month, at the specified run time.

Note: If the day in the **Days** box is greater than the number of days in a month, then the trigger runs for the last day of that month. For example, if the day is set to 31 and the month is April (which only has 30 days), the trigger runs for day 30.

– For a **Yearly** repeat interval:



i. Select a month from the **Months** drop-down list.

ii. Type a valid day (1 to 31) of the month in the **Days** box.

The trigger runs the monitor tests every year, on the specified day of the specified month, at the specified run time.

5. Click the calendar ▦ icon to select a run time.

Note: The first trigger time for the monitor is the next date and time selected, *after the start date*. Subsequent trigger times will be at the next repeat period, *after the last trigger time*.

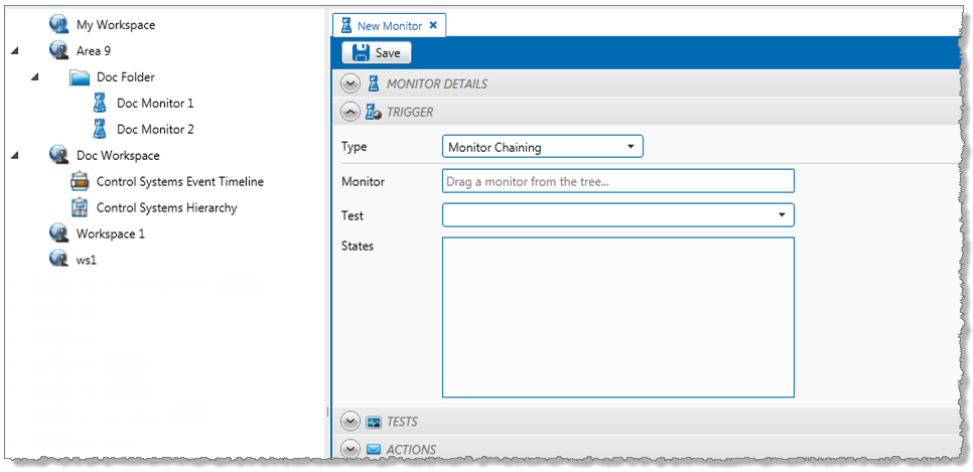
Setting a Monitor Chaining Trigger

You may want to trigger a monitor when various states are reached by a test within another monitor. To achieve this outcome, the triggered monitor needs a **monitor chaining trigger**.

To set up a monitor chaining trigger:

1. Select **Monitor Chaining** from the **Type** drop-down list.

The **Trigger** panel appearance changes, as shown in the screen image below:



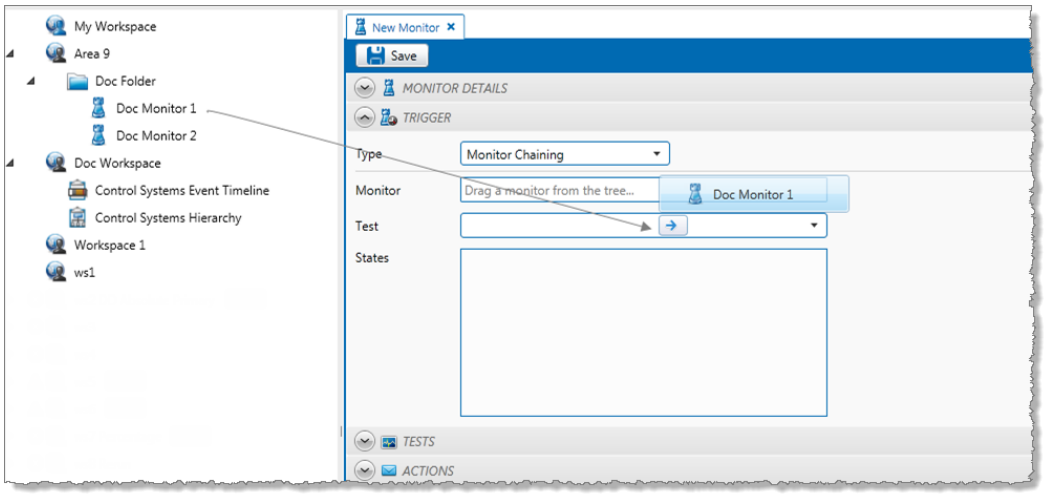
2. Add a Triggering Monitor.

   This is the monitor which causes the trigger to activate.

   a. In the Workspace panel, find the monitor that you want to use.

   b. Click and drag the monitor to the **Monitor** box in the trigger panel.

      When the monitor is positioned directly over the **Monitor** box, an arrow icon appears.



      When the arrow icon appears, release the mouse button.

      The triggering monitor name appears in the **Monitor** box.

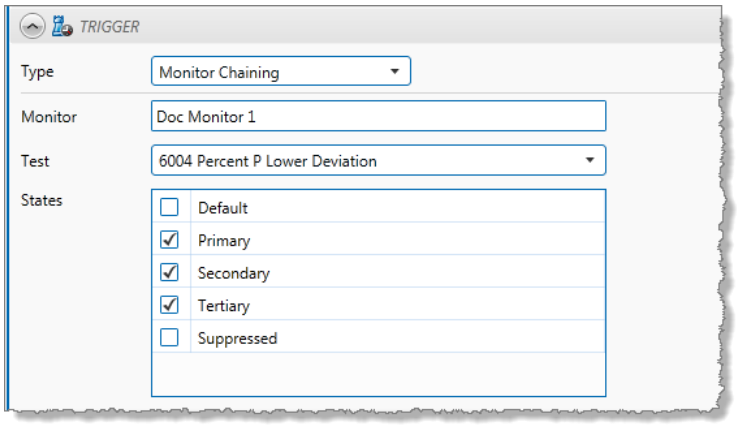
3. Select a test from the **Test** drop-down list.

   This is the particular test within the triggering monitor which will cause the new chained monitor trigger to activate.

   Note: The drop-down list includes all of the triggering monitor tests.

   The selected test is the triggering test, and appears in the **Test** box of the trigger panel.

4. From the **States** check list, select **Triggering States**. You may select one or more of the listed states.



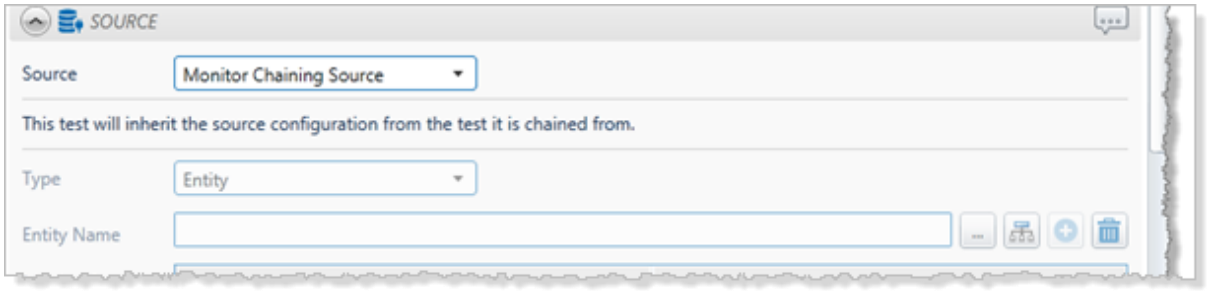
These are the selected states within the test that cause the trigger to activate (for tests that use **Monitor Chaining Source** as their source).

Note: The available states depend on the process used by the test.

The monitor chaining trigger is ready. Every time the Triggering Test of the Triggering Monitor reaches any of the Triggering States, the monitor is triggered.

Setting the Source for a Chained Monitor

The source for any test using a chained monitor defaults to **Monitor Chaining Source**.



The test inherits the source configuration from the chaining test. If you change the source configuration for the chaining monitor, the change carries through to the chained monitor.

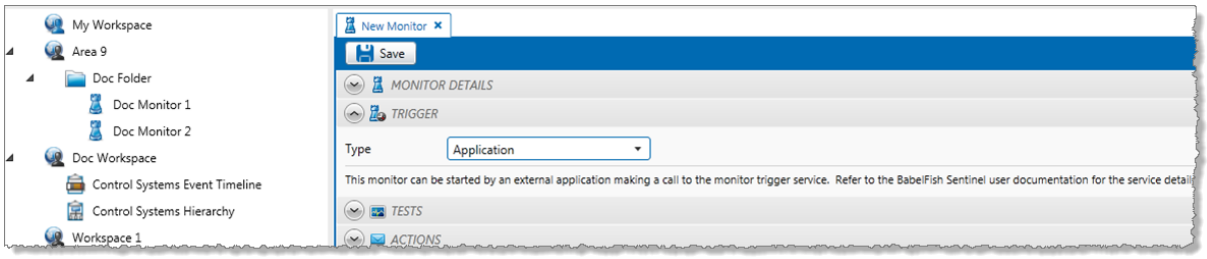
If any test of a chained monitor uses a source other than "Monitor Chaining Source" (for example, "P2 Server"), the chained monitor uses the parent trigger setting, and is *not* triggered by events of the parent monitor.

Setting an Application Trigger

This trigger is activated whenever a call is made from an external application.

- Select **Application** from the **Type** drop-down list.

The **Trigger** panel appearance changes, as shown in the screen image below:



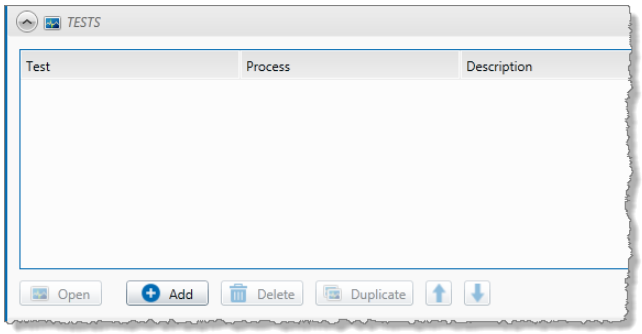
The application trigger is set for the monitor.

Step 3. Add Tests

You need to add at least one test to the monitor.

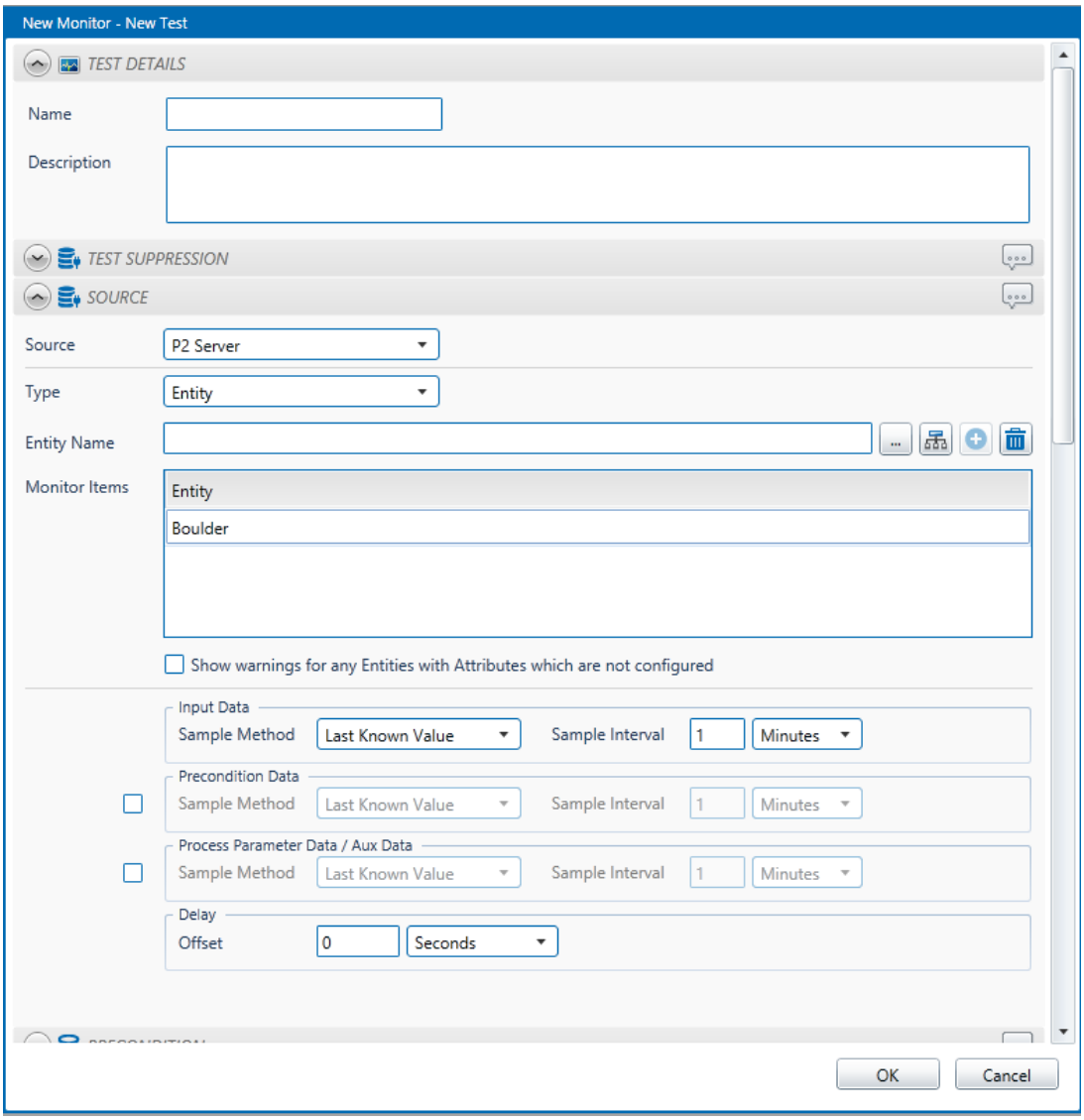
In the **New Monitor** page:

1. Expand the **Tests** panel.



2. Click **Add**.

   The new test page appears.



3. Set up the following components of the test; each panel is described in detail in the following sections.

Test Details
Add a test **name** and **description** here.

Test Suppression
Set a suppression for the test. For example, suppress the test if your test monitor items are due for maintenance. This is optional.

Source
Choose a test source. The process uses this source.

Precondition
Set a precondition. Test data is only evaluated when the precondition is met. This is optional.

Process
Select a process to run the test. Define the input, and the relevant test condition parameters.

State Configuration
Configure severity levels for the different possible state outcomes, and configure Case Management and Case Options (if Case Management is enabled). Optionally apply a state override. Add state configuration comments.

Auxiliary Data
Define auxiliary data for the test. Auxiliary data values are saved with event details.

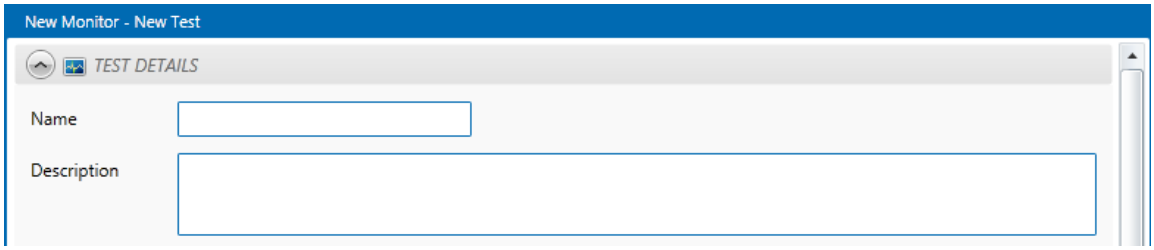
Actions
You will only be able to select actions for the test when actions have been added to the monitor.

4. When you have finished adding the test, click **OK** to close the test panel, and optionally add a comment to the test panel, describing the reasons you have chosen to use this test.

Note: The test page contains a lot of information. Expand or collapse panels as needed.

3.1 Add Test Details

1. Expand the **Test Details** panel.



2. Type a name in the **Name** box. This must be a unique name for the test.
3. Type a description in the **Description** box. This is an optional description of what the test is used for.

3.2 Add a Test Suppression

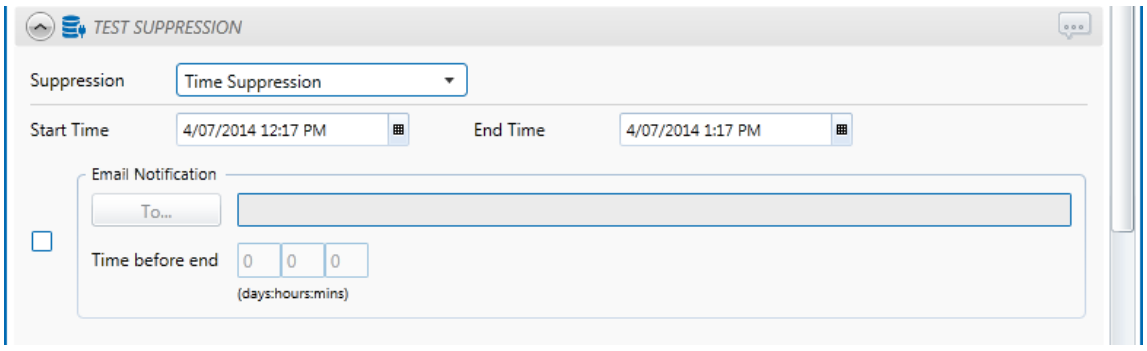
This is an optional step for when you want to suppress the test for a specific reason, for example when a piece of machinery is going down for planned maintenance.

ADDING A TIME SUPPRESSION

1. Expand the **Test Suppression** panel.

2. From the **Suppression** drop-down list, select *Time Suppression*.

   The panel changes, as shown below:



   a. In the **Start Time** edit box, click the calendar ▦ icon to select a start date and time.

b. In the **End Time** edit box, click the calendar ▦ icon to select an end date and time.

c. If required, specify email notification details:

i. Select the check box to the left of the Email Notification panel.

ii. Add a list of email addresses by typing one or more valid email addresses in the text box (separated by semicolons).

Alternatively:

a) Click **To**.

The **Choose Contacts** page opens, displaying all contacts on the mail server database that have an email address.

b) In the **Filter** box, type part of a contact name, or part of an email address to filter the contact list.

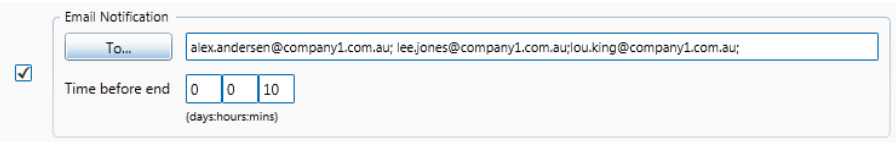
c) To add a contact from the list, double-click a user or a group. The User or Group is added to the **To** edit box.

d) Keep adding contacts following the instructions, above.

e) Click **Add.**

The **Choose Contacts** page closes, and the list of contacts is added to the **Email Notification** edit box.

iii. In the **Time before end** edit box, capture the email notification time in days, hours, and minutes. This specifies the interval before the end of the suppression period, at which time the email notification is sent to the email notification contacts.



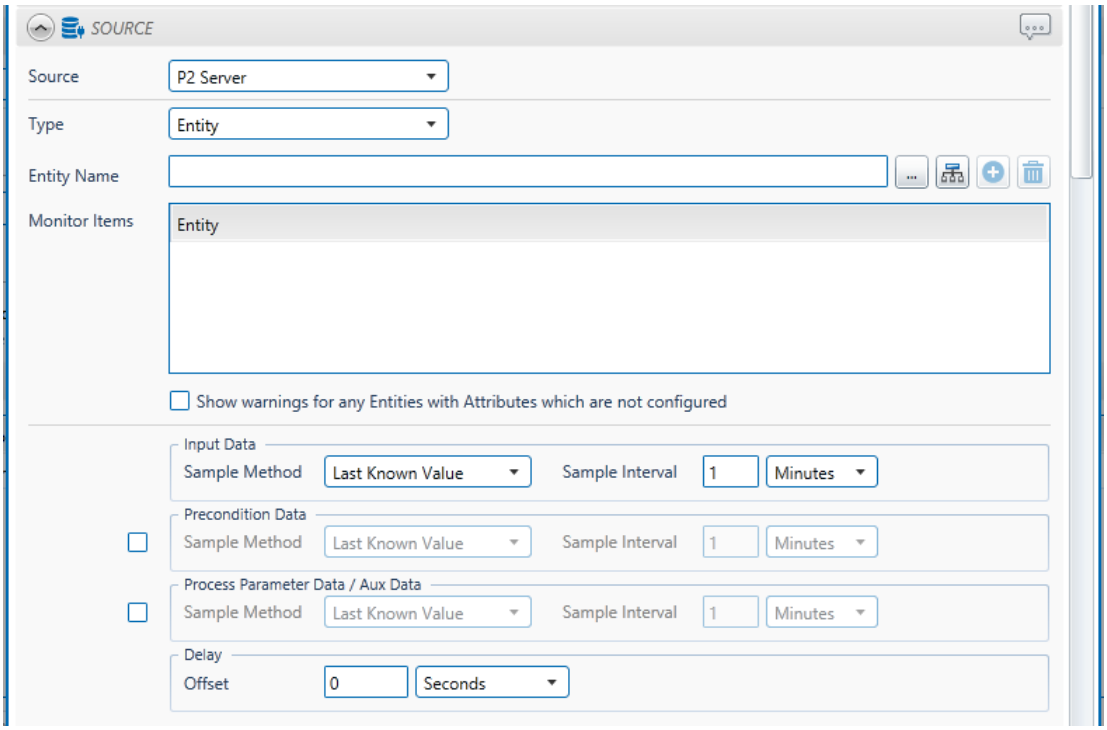
3. Click the comment button on the top right corner of the *Test Suppression* panel, to add an optional comment, describing the reasons you have chosen the test suppression.

Note: You can set a new test suppression at any time by editing the monitor.

3.3 Add a Source

There are three types of data source to use: **Entity**, **Tag** and **Hierarchy**.

1. Expand the **Source** panel.



2. In the **Source** drop-down list, select a source.

3. In the **Type** drop-down list, select a source type:

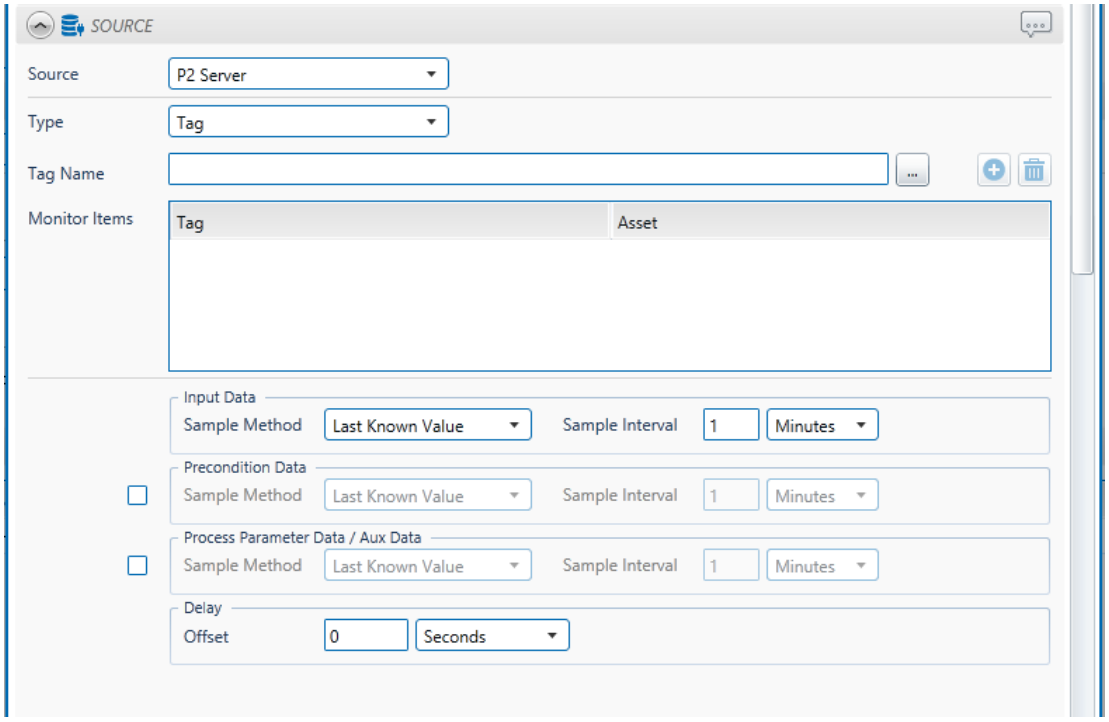
Entity
This is the default source type. With an entity type, you are able to select individual entities to monitor; these are listed as monitor items.

Monitor Items
The selected entities are listed. The Entity is the source of the process input. (In Sentinel, this is known as the *Asset*. All P2 Sentinel reporting is based on assets.)

Show warnings for any Entities with Attributes which are not configured
If you unselect this check box, Sentinel will ignore the entities that have missing attributes. If you select it, Sentinel will send a warning message for any of these. It can be useful to know about any un-configured attributes when you are first working with the monitor.

Tag

If you select **Tag**, different fields are displayed on the screen:



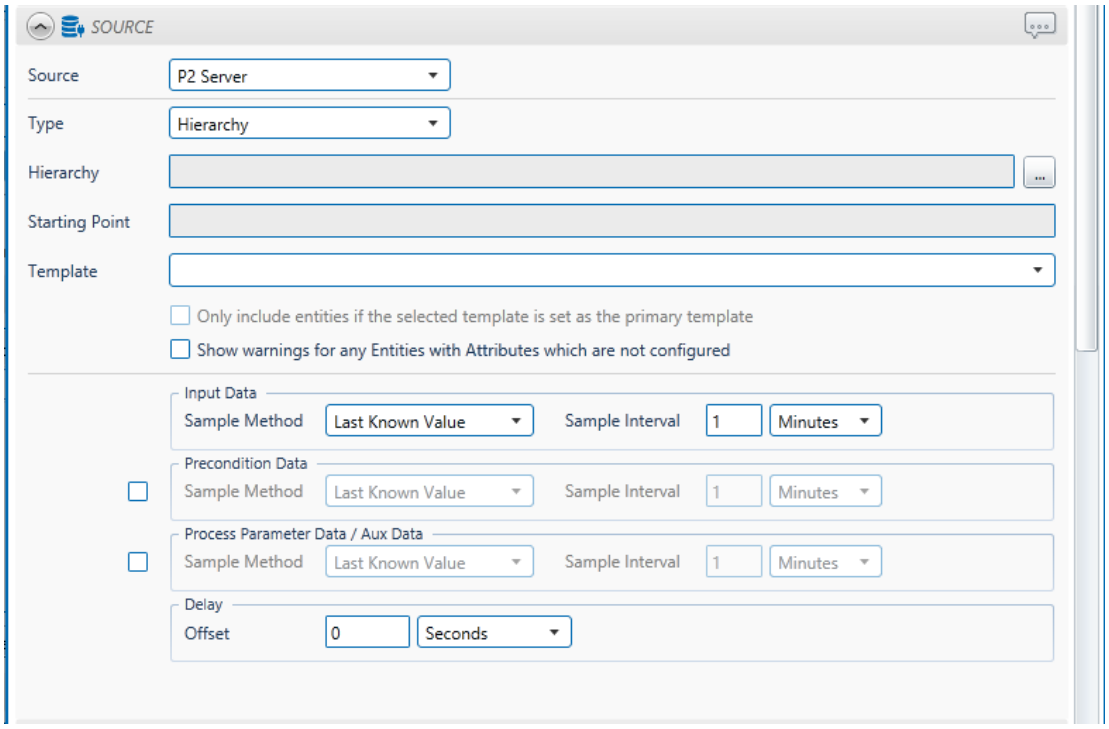
With the **tag** type, you are able to select individual entities to monitor; these are listed as monitor items.

Monitor Items

The selected tags are listed. The tag is the source of the process input. Because tags can be related to more than one entity (in P2 Explorer), you need to define the entity, by selecting it from the *Asset* drop-down list under this is (*Entities* are referred to as called *Assets* in P2 Sentinel).

Hierarchy

If you select **Hierarchy**, different fields are displayed on the screen:



You can monitor all the entities from a specified point in the Data Dictionary hierarchy.

Hierarchy
A P2 Server entity hierarchy.

Starting Point
This is the starting point in the hierarchy, used in the test. All entities from this point in the hierarchy are available as source entities.

Template
Only entities that exist in the selected template structure are source entities.

Only include entities if the selected template is set as the primary template
Select this check box if you only want to include entities where the selected template is set as the primary template.

Note: By default, this option is **not** selected.

Show warnings for any Entities with Attributes which are not configured
If you unselect this check box, Sentinel will ignore the entities that have missing attributes. If you select it, Sentinel will send a warning message for any of these. It can be useful to know about any un-configured attributes when you are first working with the monitor.

4. For the **Input Data**, define the sample method and sample interval.

   a. In the **Input Data** box, select a sample method from the **Sample Method** drop-down list.

   Last Known Value
   The last known value of the data is used, even if this data point is in the past. This sample method is only available for processes using continuous data.

Linear Interpolate
Requests a linear interpolation of the data for the time specified by the *Sample Interval* period. This sample method is only available for processes using continuous data.

Average
Requests an average of the data between the times determined by the *Sample Interval* period. This sample method is only available for processes using continuous data.

Raw
Displays the most recent data for tags for the time specified by the *Sample Interval* period. This is only available for processes using discrete data.

Note: Depending on which Sentinel process is being used, the available options could be *Raw, Last Known Value*, *Average*, or *Linear Interpolate*. For example, if the *Discrete Min Max* process is used in this test, then the **Raw** sample method is the only available method.

b. Define a sample interval.

This is the regular interval between trigger periods, to collect sample data. At every sample interval, the collected data is prepared according to the sample method used, and then evaluated in the process. You can specify the sample interval in seconds, minutes, hours, days, or weeks. The default sample interval is 1 minute.

Note: For accurate results and predictable behaviour, choose a sample interval that correlates well with the trigger interval that this monitor is using. For example, if the monitor's trigger interval is hourly, select a sample interval that divides evenly into that interval, such as one minute, five minutes, six minutes, ten minutes, fifteen minutes, twenty minutes, and so on. In this example, a sample interval of 35 minutes does not divide evenly into the one hour trigger interval, in which case the second 35 minutes fall beyond the trigger's end time and will not be processed for that trigger interval.

i. In the **Sample Interval** box, type an integer value. The default value is **1** (minute).

ii. In the **Interval Type** drop-down list for **Sample Interval**, select an interval type. The default type is **Minutes**.

5. If you have defined a precondition and you want to define a different sample method and interval for the collection of this data, then select the check box to the left of the *Precondition Data* box, and define the sample method and interval in the same way as for the *Input Data*.

You may want to do this if, for example, your monitor is using a *Discrete Min Max* process, fetching *Raw* data, but your precondition is dependent on the evaluation of continuous data.

Note: If you do not define this, then precondition data (if you have defined a precondition) is fetched using the same sample method and interval as the input data.

6. If you want to define a different sample method and interval for the collection of process parameter or auxiliary data, then select the check box to the left of the **Process Parameter / Aux Data** box, and define the sample method and interval in the same way as for the *Input Data*.

Note: If you do not define this, then process parameter data and auxiliary data is fetched using the same sample method and interval as the input data. For this reason, you **need to**

select the check if your process is a Discrete Min Max Process, as that process type can only use the *Raw* sample method, whereas the auxiliary data needs to be defined (as *Last Known Value*, *Average*, or *Linear Interpolate*).

7. Define an optional delay period. (This applies to input data, precondition data and process parameter data.)

   By setting this option, P2 Sentinel delays collecting the sample data by the specified interval of time. This option is useful in cases such as when a historian is writing data at a similar time to when P2 Sentinel is reading data.

   a. In the **Delay** box, type an integer value. The default value is **0**.

   b. In the **Interval Type** drop-down list for **Delay**, select an interval type. The default type is **Seconds**. Options are: seconds, minutes, hours, days and weeks.

8. Specify the source of data.

   – For an **Entity** source type, add monitor items.

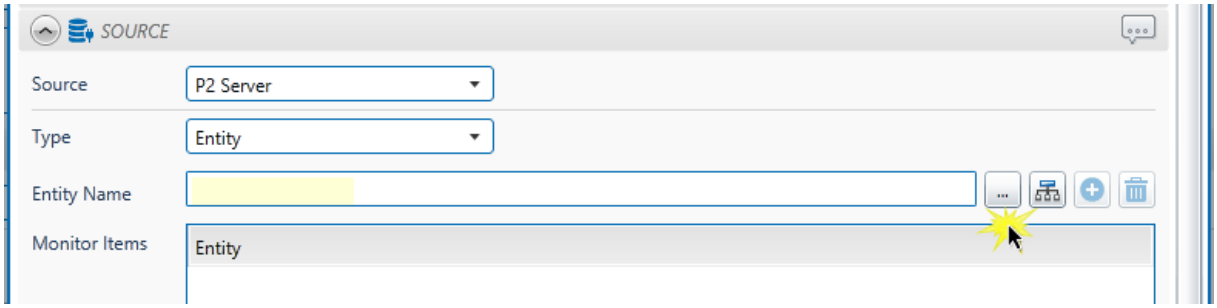
   – For a **Hierarchy** source type, add hierarchy specifications.

9. Click the comment button on the top right corner of the *Source* panel, to add an optional comment, describing the reasons you have chosen this source.

Adding Monitor Items for Entity Source Type

If you select **Entity** as your *source type*, you can add a selection of entities by typing in valid entity names, or by using the **P2 Server Browser** with *Selection Type: Entity* and/or you can choose entities from a hierarchy, using the **P2 Server Browser** with *Selection Type: Hierarchy*.

Adding a Selection of Entities



To add a selection of entities using the entity picker:

1. In the **Entity Name** box:

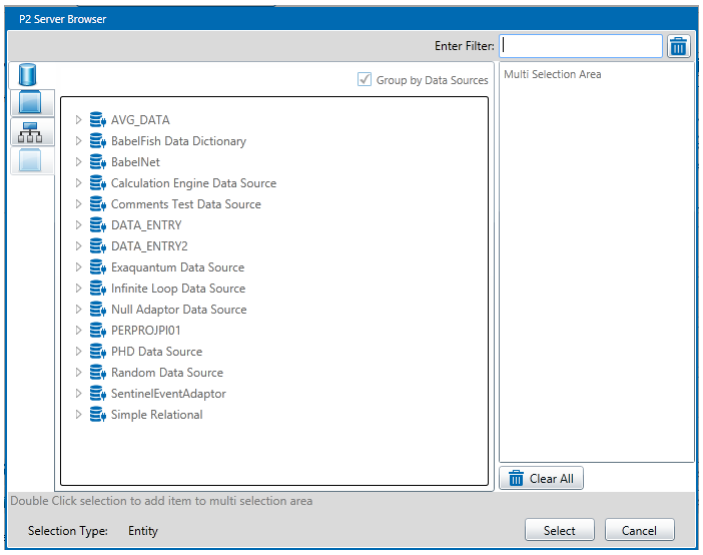
   a. Type a valid P2 Server Entity Name in the **Entity Name** box.

   b. Click the **Add** button next to the Entity Name, or click in the **Entity Name** box and press **Enter**.

   Note: The **Add** button appears dimmed if the entity name is invalid or incomplete.

   and/or

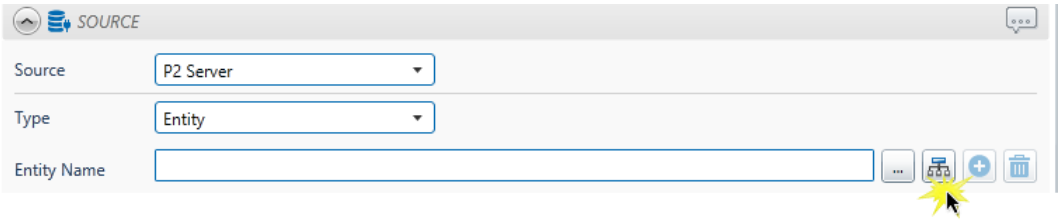
   c. Click the **P2 Server Browser** button next to the Entity Name box, select one or more Entities from the from the P2 Server Browser (see Selecting Entities), and click **Select**.



The new entities appear in the **Monitor Items** grid, below **Entity Name.**

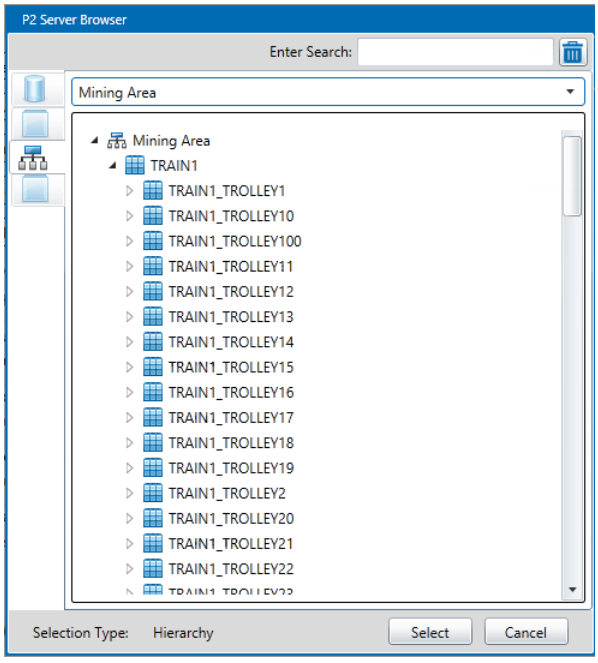
2. You can also add entities using the hierarchy picker, as shown below.

CHOOSING ENTITIES FROM A HIERARCHY



To add entities using the hierarchy picker:

1. Click the **Hierarchy** button next to the **Entity Name** box, and select a hierarchical group of entities by selecting a hierarchy, an optional starting point, and an optional template, using the P2 Server Browser.



The new entities appears in the **Monitor Items** grid, along with any other entities you have already added.

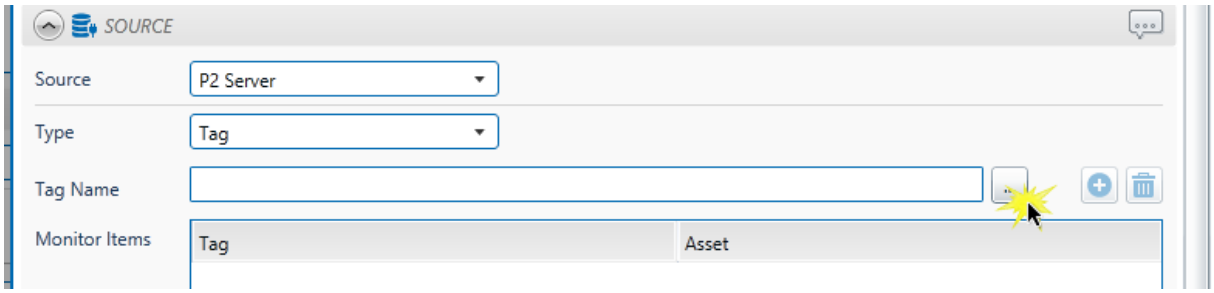
2. You can add more entities in this way, if you choose.
3. Continue to add monitor items for the test until your list is complete.
4. (Optional) Delete unwanted **Monitor Items** from the list.
   a. In the **Monitor Items** grid, select one or more monitor items to delete.
      - Click on a single monitor item in the list to select it.
      - If you want to select the whole list, select any monitor item from the list, and then click **Ctrl** + **A** on the keyboard
      - Click on a monitor item, then click **Shift** on the keyboard, and continue selecting monitor items.
   b. Click the **Delete** button alongside the **Entity Name** box.

      The selected monitor items are deleted.

Adding Monitor Items for Tag Source Type

If you select **Tag** as your *source type*, you can add a selection of tags by typing tag names, or by using the **P2 Server Browser** with *Selection Type: Tag* and/or you can choose tags from a hierarchy, using the **P2 Server Browser** with *Selection Type: Hierarchy*.

ADDING A SELECTION OF TAGS



To add a selection of tags using the tag picker:

1. In the **Tag Name** box:
   a. Type a valid P2 Server Tag Name in the **Tag Name** box.
   b. Click the **Add** button next to the Entity Name, or click in the **Entity Name** box and press **Enter**.

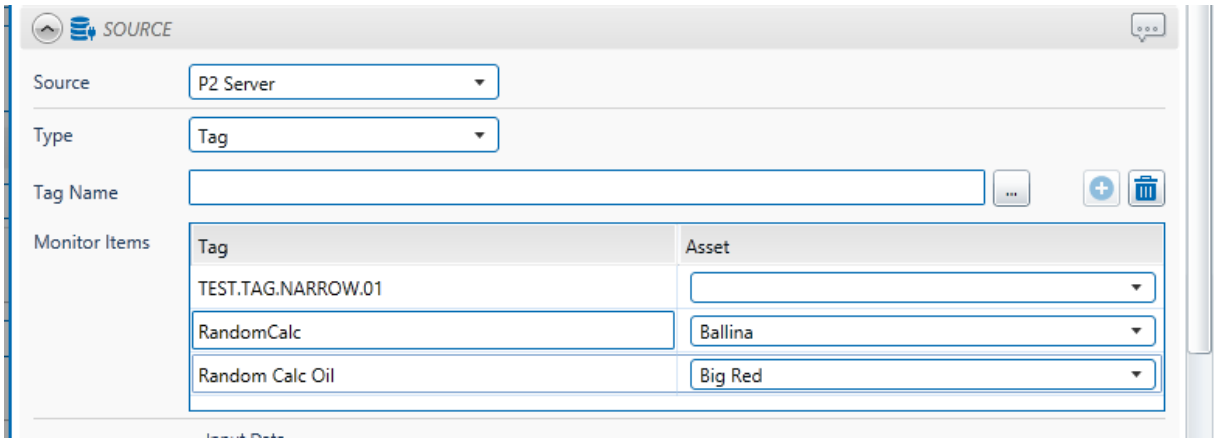
      Note: The **Add** button appears dimmed if the tag name is invalid or incomplete.

      and/or

   c. Click the **P2 Server Browser** button next to the Tag Name box, select one or more Tags from the P2 Server Browser (see Selecting Tags) and click **Select**.

   The new tags appear in the **Monitor Items** grid, below **Tag.**

   d. For each tag, select an asset (entity).



Note: Not all tags have entities. You can leave the asset blank for those tags. Cases cannot be raised against tags that do not have an asset selected.

Adding Hierarchy Specifications for Hierarchy Source Type

Use this method for the **Hierarchy** source type.

1. To select a Hierarchy and a Starting Point:

   a. Click the **P2 Server Browser** button next to the **Hierarchy** box.

   b. To select a starting point, navigate through the hierarchy and click an entity (see Selecting Tags or Entities).

P2 Server Browser can also be used for selecting either an entity or a tag. For example, if you are adding data to a Timeline report, the P2 Server Browser opens for Selection Type Tag, Entity.

To select a tag:

1. Click the **Data Sources** button on the left.
2. Optionally type filter text into the **Enter Search** box, as shown.
3. Expand a data source (if **Group by Data Sources** is selected) and scroll down the list of tags (filtered or unfiltered) listed to locate your tag.

   Or

   Scroll down the ungrouped list of tags (filtered or unfiltered) to locate your tag.
4. Click on a tag.
5. Click **Select**.

To select an entity (by template):

1. Click the **Templates** button on the left.
2. Optionally type filter text into the **Enter Search** box, as shown.
3. Select a template group from the drop-down list.
4. Expand a template and scroll down the list of tags (filtered or unfiltered) listed to locate your entity.
5. Click on the entity.

6. Click **Select**.

To select an entity (by hierarchy):

1. Click the **Hierarchies** button on the left.
2. Select a hierarchy from the drop-down list.
3. Optionally type filter text into the **Enter Search** box, as shown, and select from the drop-down list.

   The entity is auto-selected if there is a search match.

   Or

   a. Navigate through the hierarchies until you locate your entity, then click it.

   b. Click on the entity.
4. Click **Select**.

3.4 Add a Precondition

Add a precondition, in the **Precondition** panel of the test.

You can choose the following combinations for the preconditions, in order for the precondition to succeed:

One condition specified
This condition must be met, in order for the precondition to pass evaluation.

Two conditions specified
If **AND** is selected, then both Condition 1 and Condition 2 must be met, for this portion of the precondition to pass evaluation.
If **OR** is selected, then either Condition 1 or Condition 2 must be met, for this portion of the precondition to pass evaluation.

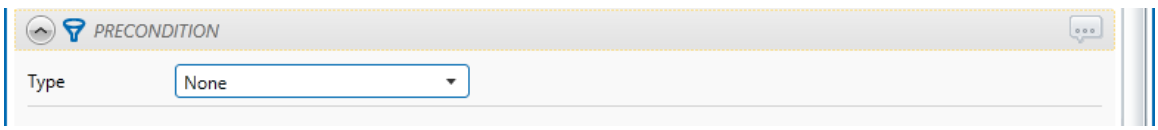
Three conditions specified
If **AND** is selected, then the combined outcome of Condition 1 and Condition 2, as well as the outcome for Condition 3, must be met for the precondition to pass evaluation.
If **OR** is selected, then either the combined outcome of Condition 1 and Condition 2, or the outcome for Condition 3, must be met for the precondition to pass evaluation.

If you have set at least one condition in the Precondition section, you can also add an *Out of Suppression Delay*.

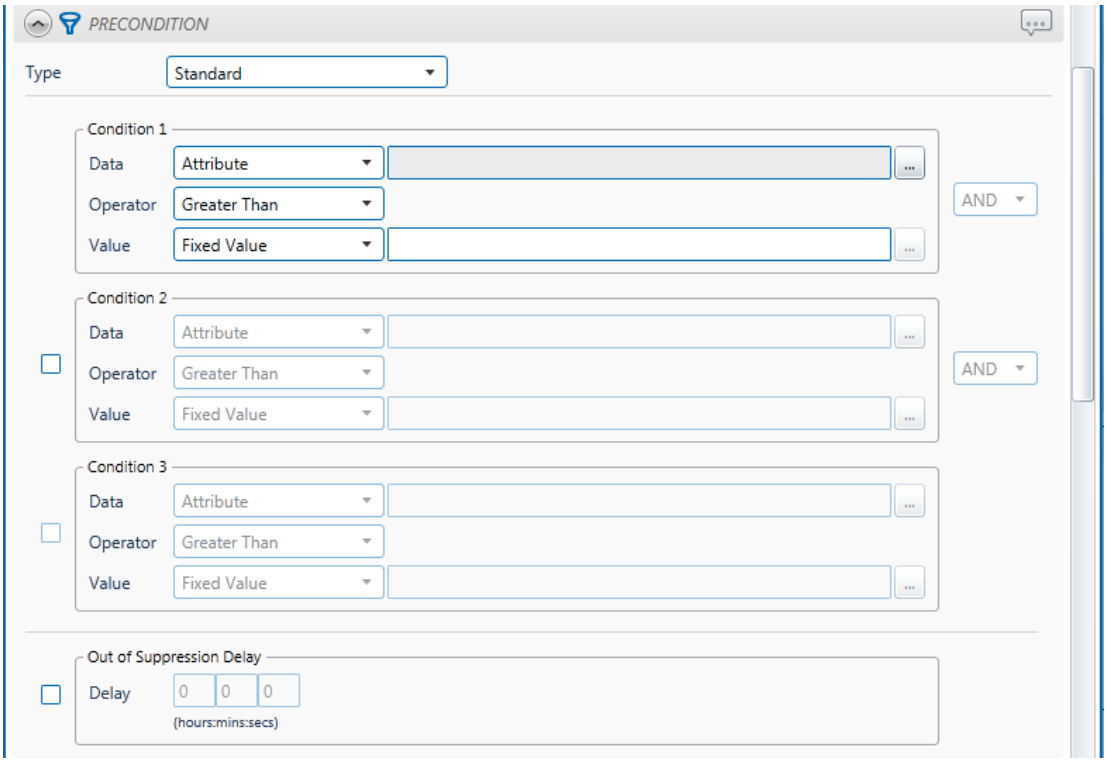
Out of Suppression Delay
As soon as the preconditions have been met, there is a further delay for the duration of the *Out of Suppression Delay*.

ADDING THE PRECONDITION

1. Expand the **Precondition** panel.



2. Select **Standard** from the **Type** drop-down list. The default is **None**.



You may add up to three conditions, as well as an *Out of Suppression Delay*.

3. Fill in the details for **Condition 1**:

   a. From the **Data** drop-down list, select the condition **data**.

   This can be one of the following:

   Attribute
   This is available where the **Source Type** is either **Entity** or **Hierarchy**.

   Click the ellipsis [...] button to open the **P2 Server Attribute Picker**. This shows templates of the source entities. To view primary templates of the source entities, select the **Primary Template** check box. Select an attribute.

   Source Tag
   This is available where the **Source Type** is a **Tag**.

   Calculation
   Click the ellipsis [...] button to open the *Edit Calculation* window.

   - Where the source type is **Entity** or **Hierarchy**, enter '*this*' for the source entity token, followed by an attribute or attribute value definition. For example: **{this:THP} + 34**. Another example: **{this:Choke!Current Position}*1.2** The expression is resolved in the P2 Server calculation engine.
   - Where the source type is **Tag**, enter '*this*' for the tag token. For example: **{this} * 1.2**. The expression is resolved in the P2 Server calculation engine.

   Note: The source entity token (this) used in the calculation expression must be selected in the Source Monitor Items in order for the calculation to run for the precondition.

b. From the **Operator** drop-down list, select an operator (for example: Equals).

c. Type in or select a value in the **Value** box. This is the value that the *Data* will be compared to, when this part of the precondition is evaluated.

The available values are:

Fixed Value
Type in a numerical value.

Attribute
This option is only available if the test's **Source Type** is **Entity** or **Hierarchy**.

Click the ellipsis  button to select an attribute or attribute value from one of the source entities.

Calculation
Click the ellipsis  button to open the *Edit Calculation* window. The expression is resolved in the P2 Server calculation engine.

- **If the Source Type is Entity or Hierarchy**
  Type a calculation, prefixed by 'this' as the **Source Entity** token, for example: **{this:THP} + 34**.
- **If the Source Type is Tag**
  Type a calculation, prefixed by 'this' as the **Source Tag** token, for example: **{this} * 2**.

Entity Attribute
Click the ellipsis  button to select a P2 Server entity, using the P2 Server Browser. From here, select a P2 Server attribute, or attribute value, by using the *P2 Server Attribute Picker* for the selected attribute.

4. (Optional) To add a second condition:

a. Select the check box to the left of Condition 2.

b. Select *AND* or *OR* from the drop-down list to the right of Condition 1.

c. Fill in the details for **Condition 2** (in the same way as for Condition 1).

5. (Optional) To add a third condition:

a. Select the check box to the left of Condition 3.

b. Select *AND* or *OR* from the drop-down list to the right of Condition 2.

c. Fill in the details for **Condition 3**.

6. (Optional) To add an Out of Suppression Delay:

a. Select the check box to the left of the Out of Suppression Delay section.

b. Type integer values for hours, minutes, and seconds in the **Delay** edit boxes, in the Out of Suppression Display section.

Note: You must have at least one condition selected, as the *Out of Suppression Delay* only takes effect after the conditions are met.

7. Click the comment button on the top right corner of the *Precondition* panel, to add an optional comment, describing the reasons you have chosen this precondition.

3.5 Add a Process

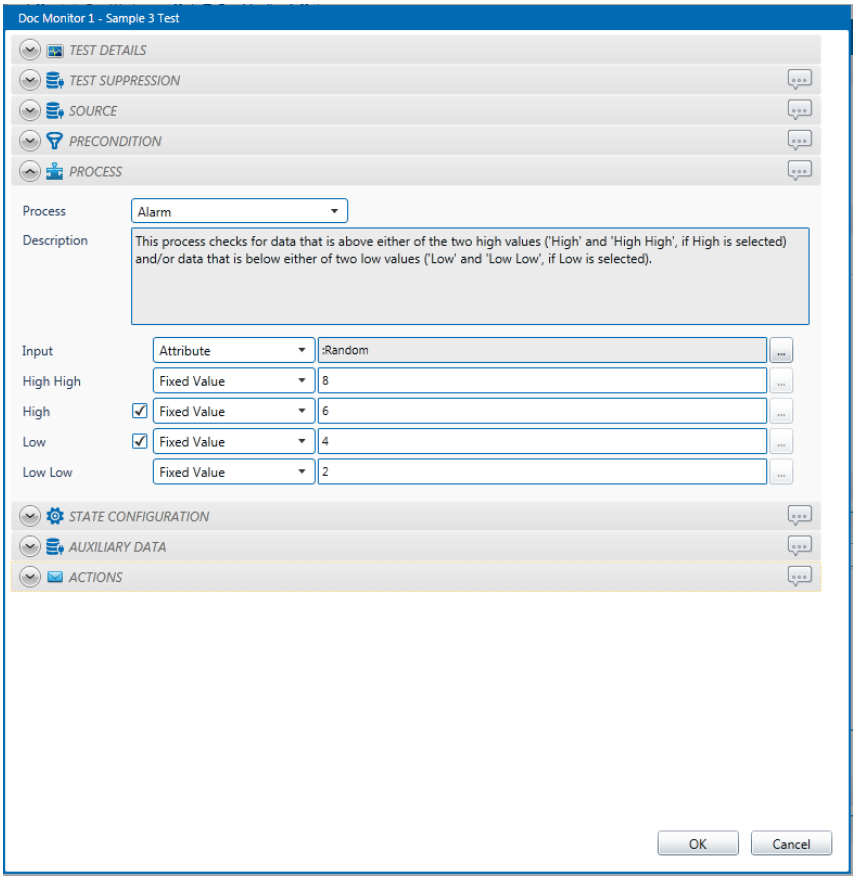
Every test uses a specific type of process. Each process has different limits to define; some of these limits are optional.

P2 Sentinel has several processes to choose from; the available processes will depend on the licence arrangement for this installation of Sentinel.

In the **Test** page:

1. Expand the **Process** panel.

   The **Process** panel appears:



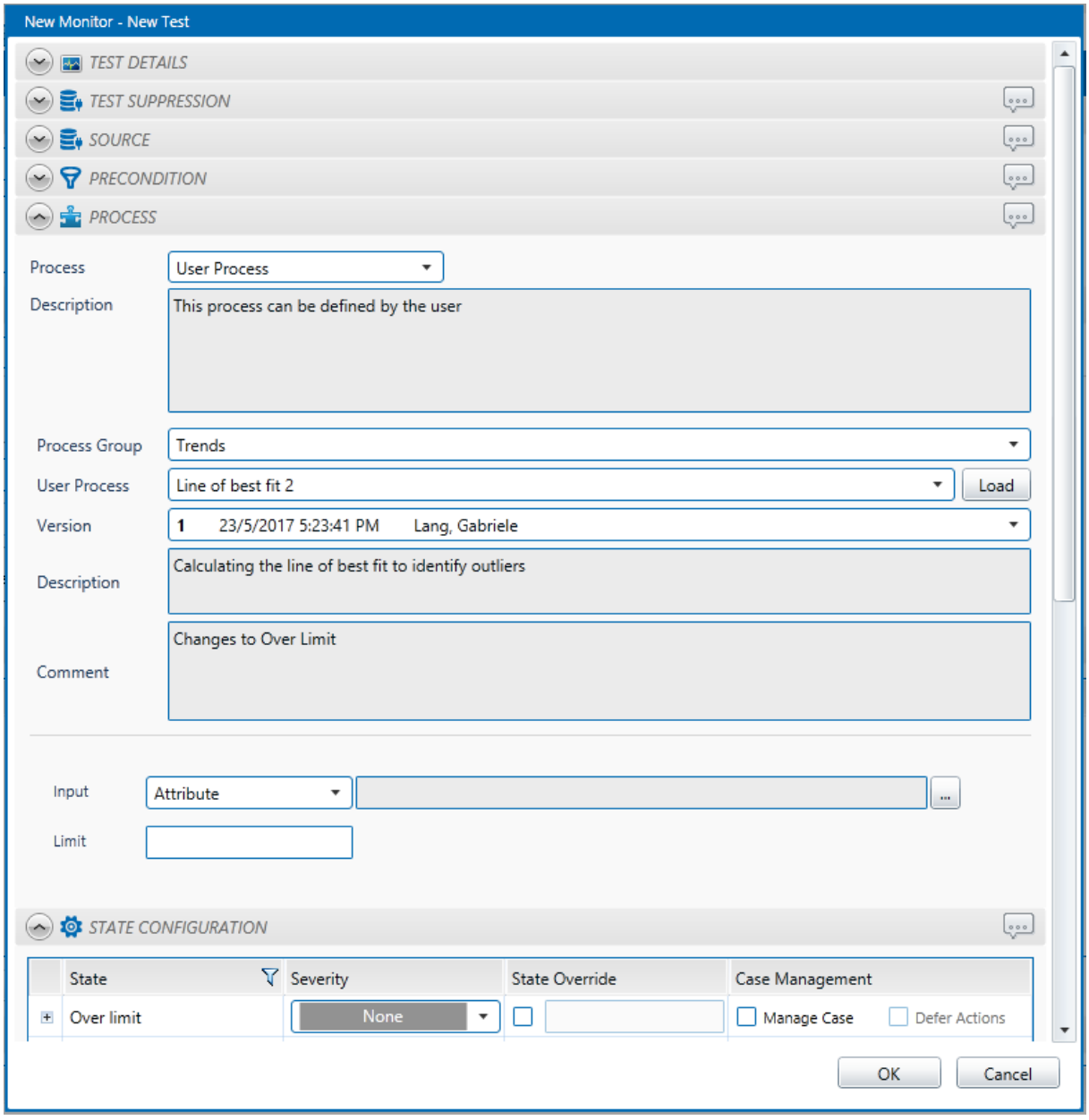
2. Add the process, following the specific instructions for the process that you want to use. Refer to the relevant section in the appendices below (for example, if you are using the Min Max process, refer to Appendix B. Min Max Process).

3. Click the comment button on the top right corner of the *Process* panel, to add an optional comment, describing the reasons you have chosen the various configurations for the process.

Adding a User Process

User processes are defined using Sentinel Studio. Once created, these processes are available for P2 Sentinel monitor tests.

Note: P2 Sentinel Studio is intended to be used by advanced Sentinel users within an organisation, and also requires a licence. Not everyone will have the security privileges required to access P2 Sentinel Studio. If you want to create or modify a user process, contact your System Administrator.



When you select a User Process, you need to select the following:

Process Group: User processes may be saved into groups to make them easier to find at a later date. If you don't select a group, all user processes will be listed.

User Process: Select the process defined in Sentinel Studio that will analyse the data required to raise events.

Version: Every time a user process is modified and saved, a new version is created. Select the version of the process that you want to use.

Description: The process description, summarising what the process is used for.

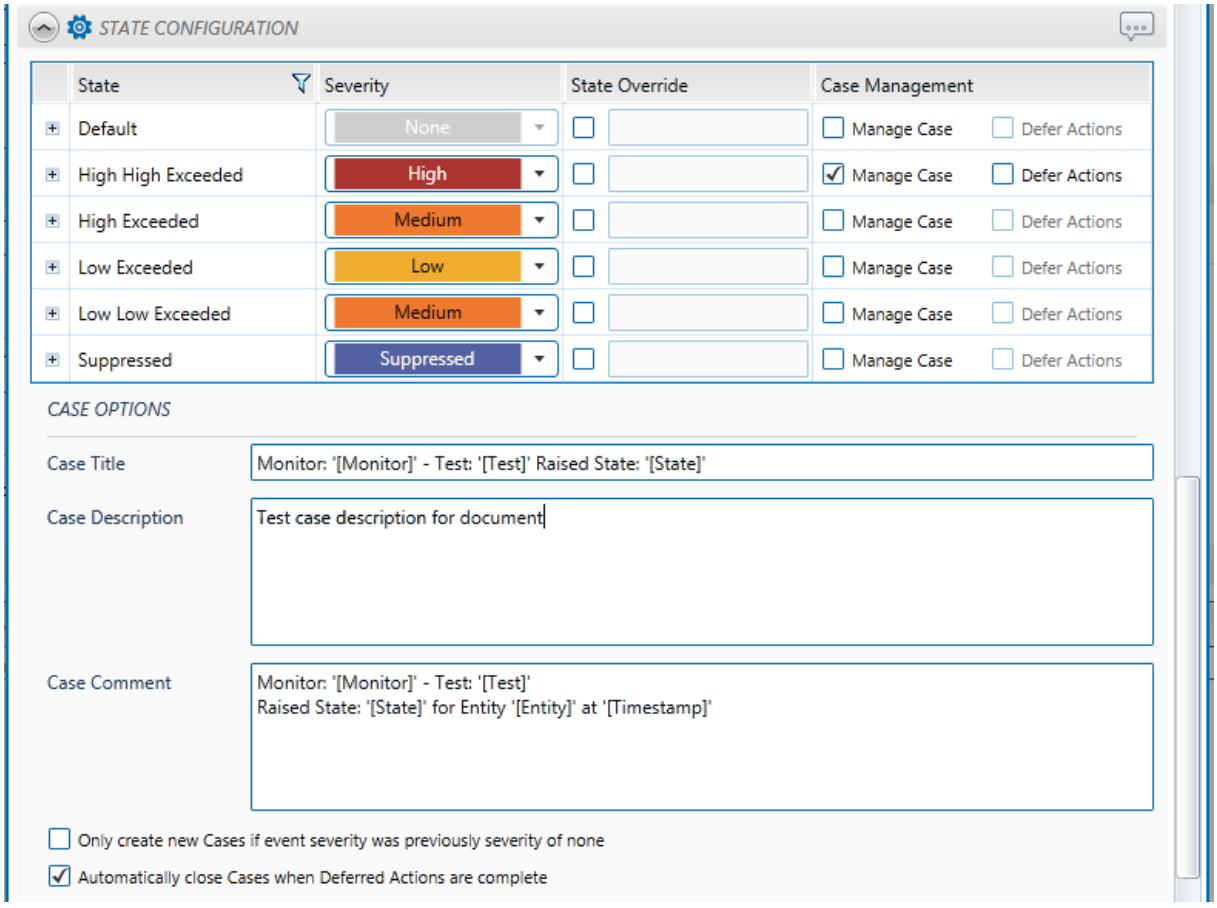
Comment: If Sentinel is configured for User Process comments, the user needs to add a comment every time the user process is saved. The comment relating to the selected version is displayed here.

After the version has been defined, you need to specify the test inputs and test evaluators to be handled by the process. These will only appear after the user process version has been selected and will differ widely, depending on how the user process has been defined. If you are unsure of how a particular user process works, the name of the person who modified the process is listed next to the version number, for you to follow up with.

3.6 Configure States

Every possible state outcome for a test can be configured at a severity level (the possible state outcomes depend on the process you have chosen).

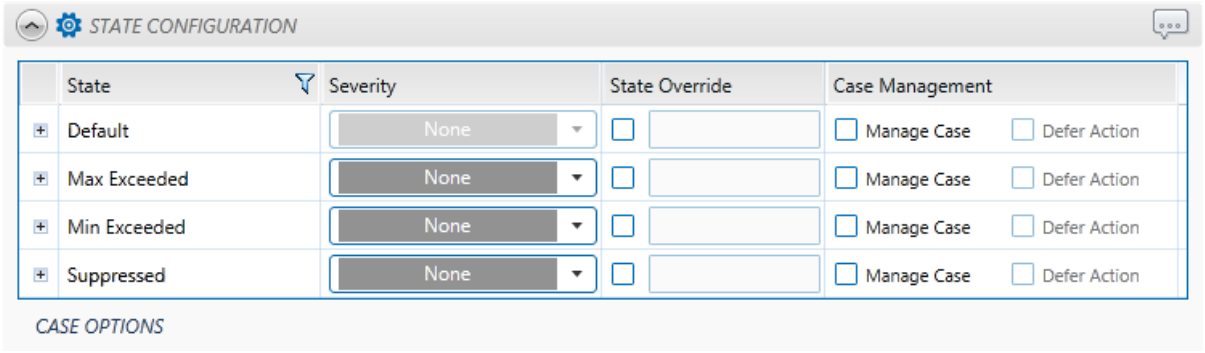
This screenshot below shows an example of a state configuration:



To configure the state outcomes for a test in the **State Configuration** panel of the test:

1. Expand the **State Configuration** panel.

In the state configuration panel, there is a list of possible state outcomes.



2. Configure each state in the list:

   a. Select a severity from the corresponding **Severity** drop-down list.

   Note: The ***Default*** severity state is fixed at **None**.

   b. Optionally add a state override.

      i. Select the corresponding check box for the state.

      ii. Type a valid state override in the corresponding **State Override** box for the state.

   Tip: To clear a state override, deselect the check box.

   c. Optionally configure Case Management for the state.

   Note: This is only available if Sentinel is configured to use Case Management.

      i. Select **Manage Case** so that Sentinel raises a case along with the event, for this state.

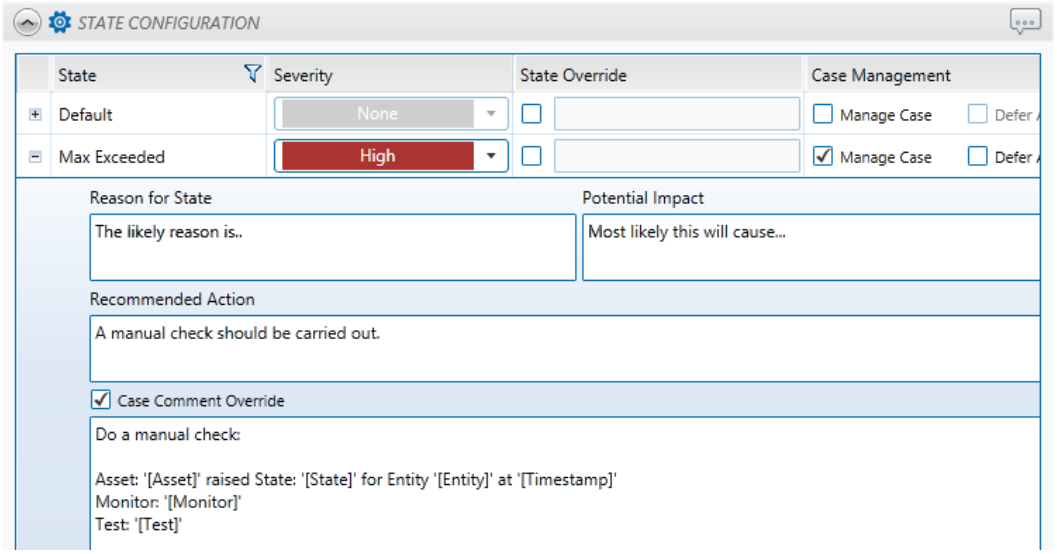
      ii. Optionally select **Defer Action** for Sentinel to defer all actions for the state until the case is closed. If the case is rejected, the actions will not happen at all.

   d. Optionally add comments for the state.

   Note: These comments can be included as tokens in email or SMS, SMS via Web Service, and Web Service actions, making it easier for notification to understand possible causes before taking remedial action. The comments also appear in the case details, in P2 Explorer.

      i. Click the expand ⊞ button in the left-most column of the state configuration grid.

The state comments panel opens:



In the **Reason for State** box, type a comment stating the most likely reason for this state outcome, for this test.

ii. In the **Potential Impact** box, type a comment outlining the potential impact of the test reaching this state.

iii. In the **Recommended Action** box, type a comment recommending what action to take, following this state outcome.

iv. To override the Case Comment for this test's *Case Options*, selected the **Case Comment Override** check box, then type in a comment. This is saved in the case commentary when a case is raised for this state, in this test. We recommend you include tokens for the asset, monitor, test, state and timestamp: '[Asset]', '[Monitor]', '[Test]', '[State]' and '[Timestamp]' to give the case some context, and also to make it easier to find the case on the event timeline.

Note: This is only available if Sentinel is configured to use Case Management.

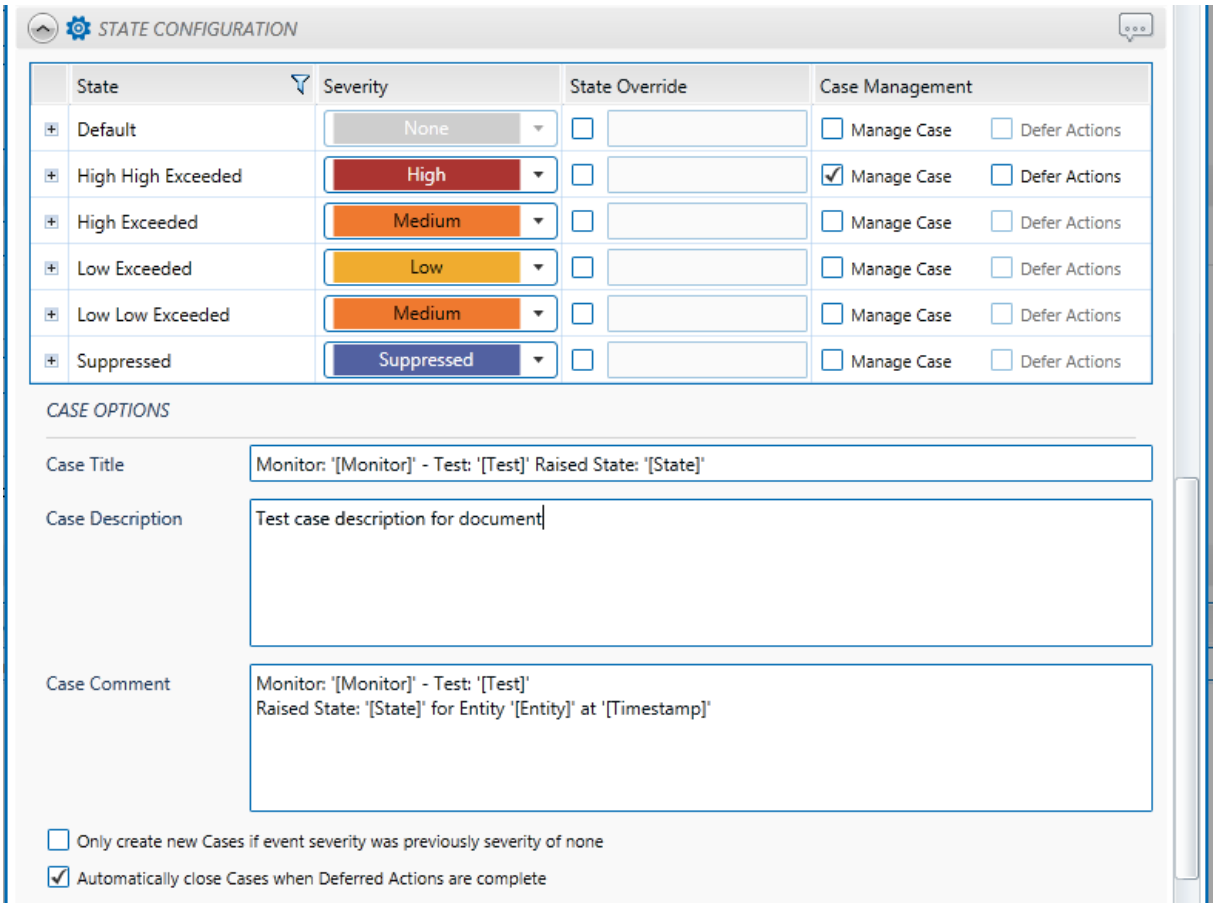
v. To close the state panel, click the collapse button in the left-most column of the state configuration grid.

Note: The **default** state cannot be configured; however, you can add a state override and comments.

3. Click the comment button on the top right corner of the *State Configuration* panel to add an optional comment describing the reasons why you have chosen the various state configurations.

Configure the Case Options

Case Options are only available if *Case Management* is configured for Sentinel.



1. The **Case Title** uses the default *Case Title* (set up in the Sentinel configuration file). You can edit this title, just for the test. This title is used for all cases raised from this test, and can contain tokens.

2. The **Case Description** uses the default *Case Description* (set up in the Sentinel configuration file). You can edit this description, just for the test. This description is used for all cases raised from this test, and can contain tokens.

3. The **Case Comment** uses the default *Case Comment* (set up in the Sentinel configuration file). You can edit this comment, just for the test. This comment is used for all cases raised from this test, except for where comments are overridden for a particular state. The case comment can include tokens.

4. Optionally select **Only create new Cases if event state was previously severity of none**.

   If this option is selected, a case is only raised if the event state has had a severity of **None** since the last case was raised

   – The Default state always has a severity of *None*.
   – Other states can have their severity configured to *None, Supressed, Low, Medium* or *High*.

5. Optionally select **Automatically close Cases when Deferred Actions are complete.**

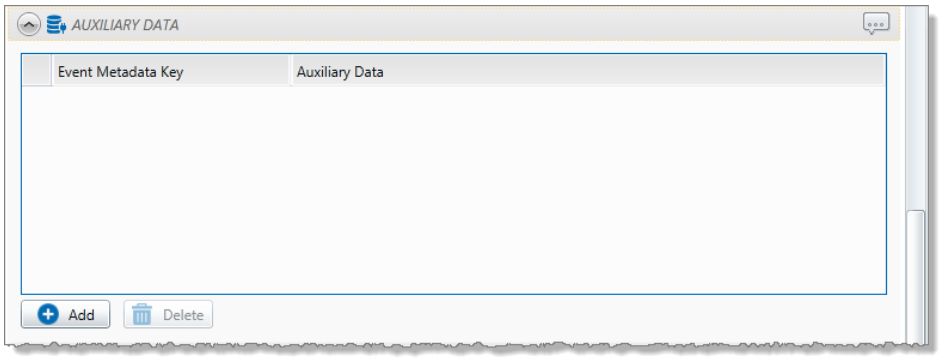
   If this option is selected and there are deferred actions, Sentinel carries out the deferred actions after a user confirms the case, then automatically closes the case. If there are no deferred actions set, Sentinel does not automatically close the case.

3.7 Add Auxiliary Data

You have the option to add auxiliary data to your test. This data is not monitored, but is saved with other event details when one of the test's monitored assets raises an event.

To add auxiliary data:

1. Expand the **Auxiliary Data** panel of the test.



2. Click **Add**.
3. Type in an Event Metadata Key. This is the reference name for the metadata and must be unique within the test.
4. Select the type of auxiliary data from the drop-down list, and the corresponding data:

Type of data (from drop-down list)	Data
Fixed Value	Type in a fixed value.
Attribute	1. Click the ellipsis to open the **P2 Server Attribute Picker**. 2. Select an attribute or an attribute value from one of the source entities.
Calculation	**If the source type is Entity or Hierarchy:** 1. Click the ellipsis to open the **Edit Calculation** window. 2. Type in *this*, followed by a source attribute name with a calculation. The source entity and attribute must be enclosed in curly brackets. For example: {this :thp} * 1.2
	If the source type is Tag: 1. Click the ellipsis to open the **Edit Calculation** window. 2. Type in *this* for the source tag token, enclosed in curly brackets, followed by the remainder of the calculation. For example: {this} * 1.2 Another example: 500 – {this}
Tag	1. Click the ellipsis to open the **P2 Server Browser** window. 2. Select a tag.
Entity Attribute	1. Click the ellipsis to open the **P2 Server Browser**. 2. Select an entity. The **P2 Server Attribute Picker** opens for that entity. 3. Select an attribute or an attribute value from the entity.

Note: If the process uses Raw as a sample method, select the **Process Parameter Data / Aux Data** checkbox and choose a sample method.

3.8 Assign Actions to Tests

Actions can be assigned to a test for various specified states. Within a monitor, all actions are available to all tests.

When you assign an action to a test, you need to select the following:

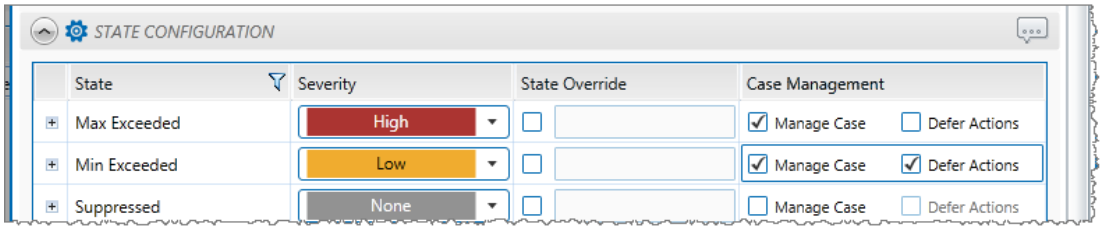
Name
The name, and the type of action (for example SMS), of the action used by the test.

State
The test must reach this state, for the action to be invoked. The default state for an action is **Any**. The other available states depend on which process is used by test.

Note: You can assign multiple actions to a test.

When an event occurs, any actions defined for the new state are carried out. Because the actions can be configured to respond to particular states, actions can be prioritised.

Note: If **Manage Case** is selected for a state, and the **Defer Actions** check box is selected, the actions for this state are deferred until the case relating to this event is confirmed. If the case is rejected, the deferred actions won't happen at all.
Case Management is only available in state configuration if it is enabled for Sentinel.



For example, **Test 2** may have the following four actions assigned:

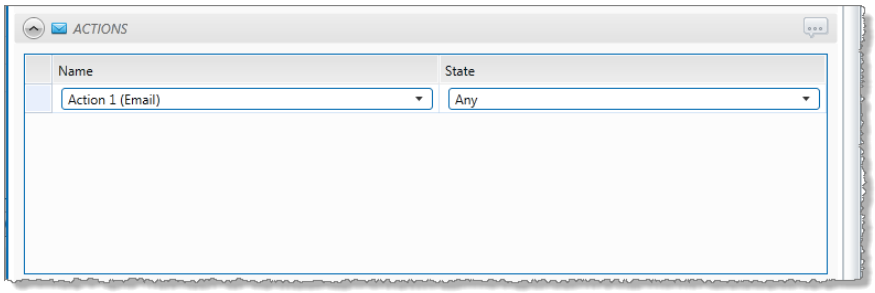
Name	State	When this state is reached...
Action 1 (Email)	High Exceeded	Action 1 email is sent to Action 1 specified personnel.
Action 2 (SMS)	Any	Action 2 SMS is sent to Action 2 specified personnel.
Action 3 (Email)	Low Low Exceeded	Action 3 email is sent to Action 3 specified personnel.
Action 4 (Web Service)	Low Low Exceeded	Action 4 web service is called.

In the **Test** page:

1. Expand the **Actions** panel.
2. Click **Add**.

Note: If there are no actions for this monitor, the **Add** button is unavailable.

A new action appears in the **Action** grid.



3. Select an action from the **Name** drop-down list in the grid.

   All of the monitor actions are listed here. For each available action, the action **name** in this list is made up of the name and the action type; for example, an *email* action named "High Exceeded Notification" appears in the list as "High Exceeded Notification (Email)", making it easier to identify the various actions available to the test.

4. Select a state from the **State** drop-down list. The default is **Any**.

   All possible state outcomes for the test process are listed in the *State* drop-down list. You may, for example, select the "High Exceeded Notification (Email)" as an action for the High Exceeded State. In this setup, whenever the High Exceeded state is raised, the *High Exceeded Notification* email action is triggered.

REMOVE AN ACTION FROM A TEST

1. Click the action on the **Actions** grid.
2. Click **Delete**.

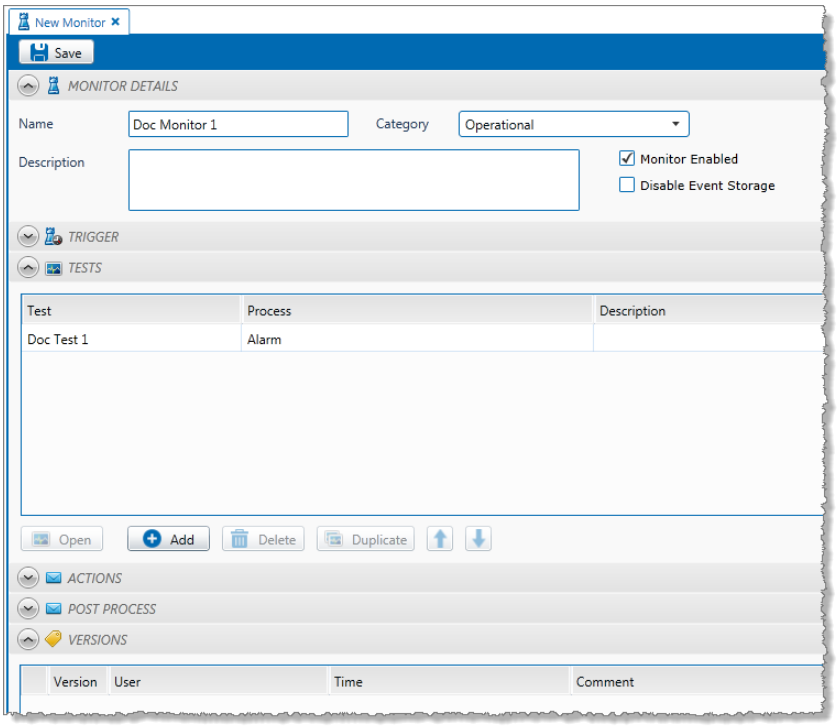
The action is removed.

3.9 Save Test

To save the test:

- Click **OK** in the lower right corner of the page.

The test is saved and is displayed in the grid, on the **Tests** panel of the monitor.



Note: If Entity Volume (the number of entities allowed for the licence group for this process) is exceeded, then the test can be saved and approved, but will not run. Entity volume limits are explained in the *Process* section.

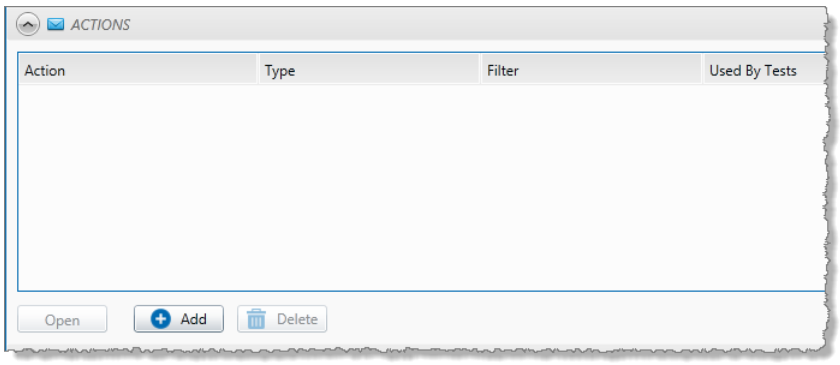
Step 4. Add Actions

This section shows you how to:

- Add an action
- Set group suppression for an action
- Edit an action
- Delete an action

All of the actions for a monitor are displayed in the **Actions** panel of the monitor. You can add multiple actions to a monitor.

- To display the actions grid, expand the **Actions** panel.



The actions grid is made up of four columns:

Action
The action name.

Type
The standard P2 Sentinel action is an SMS, an Email, an SMS via Web Service, or a Web Service action.

Filter
The default value is **None**. The other type of filter is *Group Suppression*.

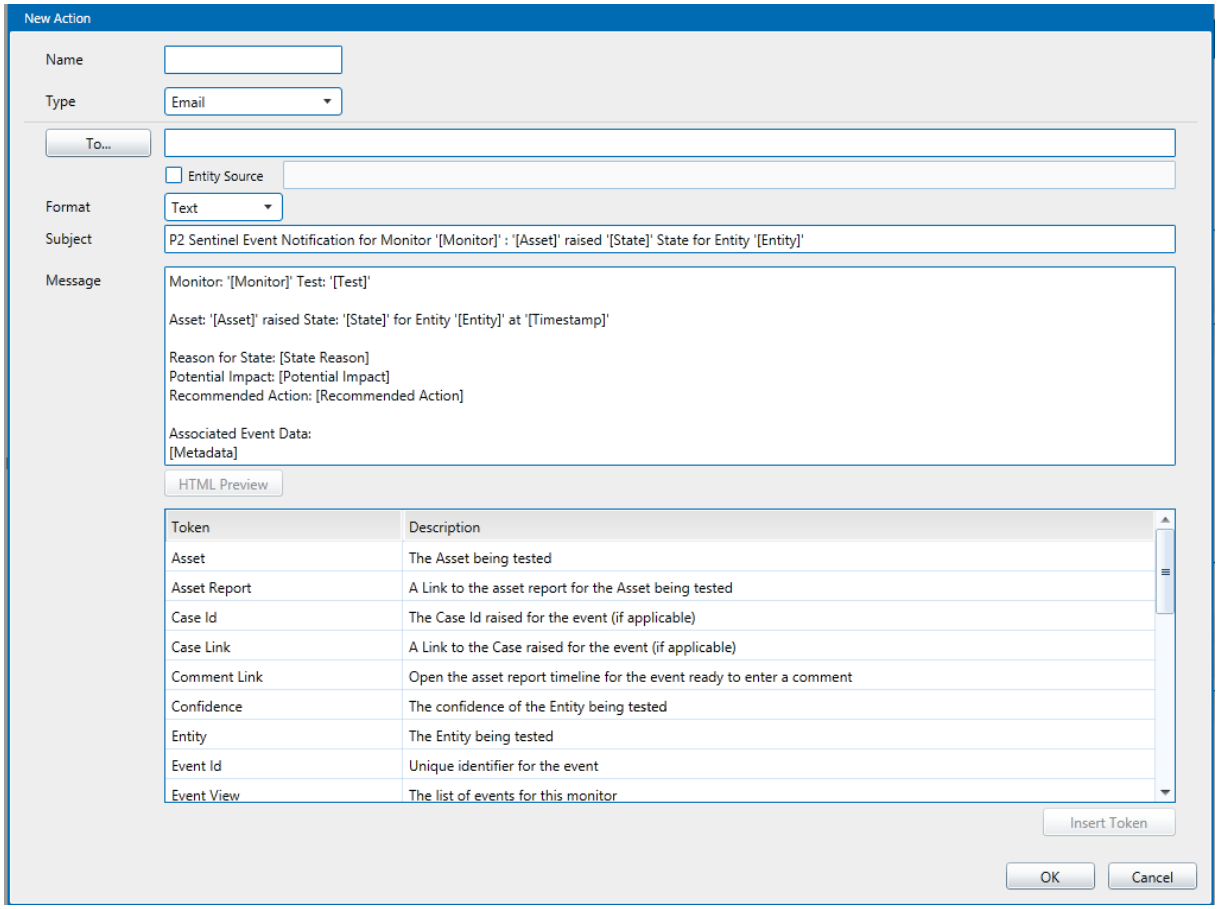
Used By Tests
When an action is assigned to a test, the test name is added to the list displayed in this column. Every test that uses this action is an item on the list.

ADD AN ACTION

1. Click **Add**.

   A **New Action** page appears.

   Note: There may already be default tokens in the subject box and the message box, as defined in the P2 Sentinel configuration file. For further information, refer to "**Update the P2 Sentinel Configuration File**" in the *P2 Sentinel Installation and Administration Guide*.



2. In the **Name** box, type a name for the action.

3. From the **Type** drop-down list, select a type of action (Email, A-Plus, SMS via Web Service, SMS or Web Service).

Note: For Web Service and A-Plus actions, the screen appearance changes to display the relevant text boxes.

4. Complete the details for the action type.

SMS, SMS via Web Service, or Email actions:

a. To assign contacts for the action, you can use one or more of the following methods:

i. Click **To**, to Assign Contacts using the contact lookup.

ii. In the **To** box, type a valid contact email address or a valid mobile telephone number. Alternatively, you can click one or more entries in the contact list.

- For **email** actions only, you can also select the **Entity Source** check box, and Define Entity Source contact.

b. For an email action:

i. From the **Format** drop-down list, select the type of email format you wish to send: Text or HTML.

ii. Type a subject line in the **Subject** box. You can include tokens in the subject line.

c. In the **Message** box, type the message that you want to send. You can include tokens in the message.

For HTML emails, you may use standard HTML mark-up tags in the message body. When you have finished the message, click the **HTML Preview** button to check that the formatting is correct.

Note: You can use the CSS 'severity' class within a span element to style the email content according to the event's severity colours. For example, the following snippet:

```
<span class=”severity”>[Severity]</span>
```

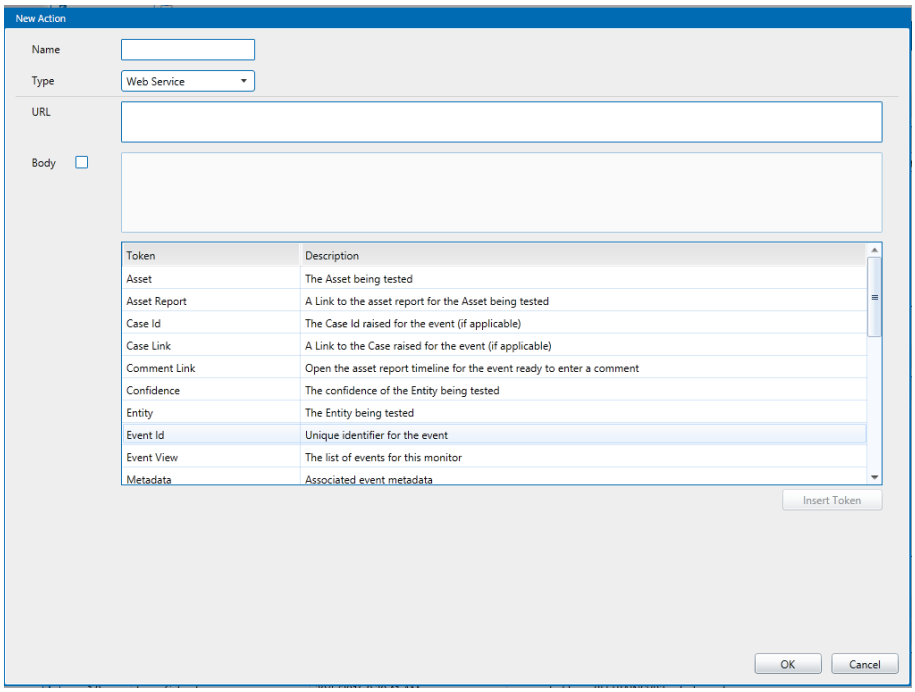
Would apply colouring like this for the severity text:

Asset:**'Asset 1'** raised State: 'High Exceeded' with Severity: 'Medium' for Entity **'Calc.SIN.Large'** at **'15/10/2013 4:31:00 PM'**

Web Service actions:

For a GET method, you only need to complete the URL details. For a POST method, you need to complete the URL details and the body details.

Note: You may require a basic understanding of HTTP principles in order to complete the Web Service action details.



a. Type a valid **URL** into the URL box. This is the URL that you want the action to call, and may contain tokens.

b. If you want to use the POST method, then add the body details.

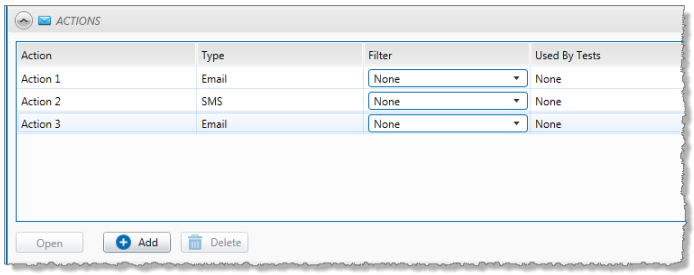
   i. Select the **Body** check box.

   ii. Type the relevant details in the **Body** text box. These should correspond to the requirements of the web service that the action will call.

Note: Sentinel will log an error if there are problems calling the Web Service action, due to invalid details supplied, invalid credentials, or due to a problem with the web service itself.

5. Click **OK** to save the action.

   The action is saved, and listed in the actions grid in the **Actions** panel of the monitor.



Note: You can assign the action to any of the tests within the monitor.

SETTING GROUP SUPPRESSION FOR AN ACTION

You can set a group suppression filter to group actions within a monitor.

1. Locate the action that you want to group.

2. In the **Filter** drop-down list, click **Group Suppression.**

EDIT AN ACTION

To edit an action:

1. In the actions grid, select the action that you want to change.
2. Click **Open**.
3. Follow the instructions in **Add an Action** (described earlier in this section).

DELETE AN ACTION

Note: You cannot delete an action if it assigned to a test.

To delete an action from the list:

1. In the actions grid, select the action that you want to remove.
2. Click **Delete**.
3. At the prompt, click **Yes** to confirm that you want to delete the action.

   The action is deleted.

Assign Contacts

A contact is the name, email address, and mobile telephone number of a person you want to notify when an event occurs.

Details for potential contacts are stored in the Mail Server database and are accessed through the **Choose Contacts** window.

Note: **Choose Contacts** is only available if Active Directory is set in the P2 Sentinel configuration file. For further information, refer to **"Update the P2 Sentinel Configuration File"** in the *P2 Sentinel Installation and Administration Guide*.

You can choose to look up a contact, or you can type in a contact name.

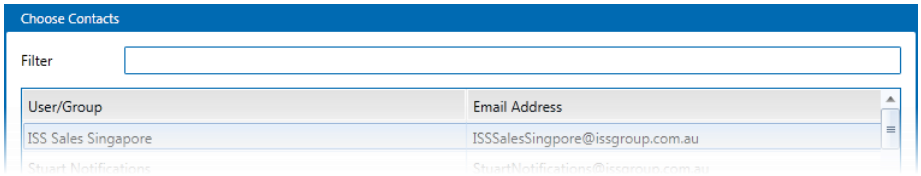
LOOK UP A CONTACT

1. Click **To** in the Action page.

   The **Choose Contacts** page opens, with a contact list.

   – For an email action, all of the Mail Server database contacts that have an email address are displayed in the list.

   – For an SMS action, all of the Mail Server database contacts that have a mobile telephone number are displayed in the list.



2. In the **Filter** box, type part of a contact name, or part of an email address to filter the contact list. To sort the list in alphabetical order (ascending or descending), click the *User/Group* heading or the *Email Address* heading.
3. To add a contact from the list, select a user or group and click **To**, or double-click. The User or Group is added to the **To** box, below the contact list.
4. Keep adding contacts following the instructions above.
5. Click **Add**.

The list of contacts is added to the **To** box in the action.

TYPE IN A CONTACT NAME

- In the **To** box, type the name and surname of that contact, and press **Enter**.

If this is a valid, correctly spelled contact name, the name and surname are retained and appended with a semi-colon; an invalid contact will be removed from the **To** box.

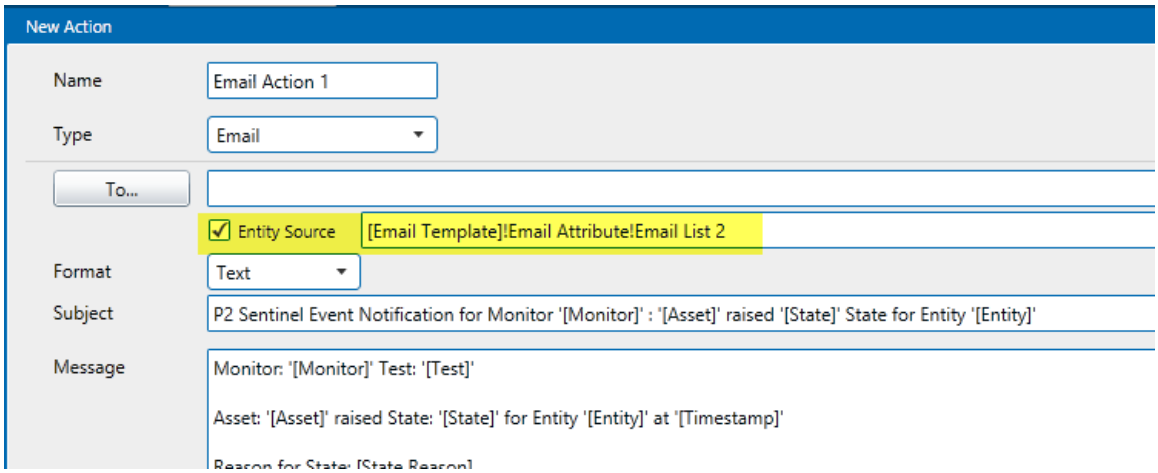
Define Entity Source

This advance feature applies to email actions only.

To add an entity source list of addresses:

1. Select the **Entity Source** check box.
2. Type the full definition for the attribute value that stores the list of recipients' email address, in the format: [template]:attribute!attribute value. For example:

   [Email Template]:Email Attribute!Email List 2



Note: In order for this feature to work, the source entities for tests that use this action must have the defined template assigned to them, and there should be at least one email address in the attribute value specified in the definition. To see how this is set up in Server, refer to the section: Entity Source Recipients.

Using Tokens

Tokens are system-generated variables that can be added to the message content of an action. The token variable name forms part of the text of an action message, once it has been added.

INSERTING TOKENS

In the **message** box of an action, insert tokens as follows:

1. Position your cursor where you want to add a token.
2. Click a row in the **Tokens** grid, which is positioned beneath the **Message** box, to select a token.
3. Click **Insert Token**.

   The selected token is inserted into the message, at the correct location. The token name is enclosed in square brackets, for example: **[Monitor]**.
4. Repeat the process to add more tokens.

REMOVING TOKENS

Tokens can also be removed from the message, and from the subject line.

- Position your cursor and press the delete key to delete the token from the message content, or from the subject line.

STANDARD AVAILABLE TOKENS

Token	Description
Asset	The asset being tested.
Asset Report	A link to the asset report for the asset being tested.
Case Id	The Case Id of the case raised for the event (if applicable)
Case Link	A link to the case raised for the event (if applicable)
Comment Link	Open the asset report timeline for the event ready to enter a comment.
Confidence	The confidence level for the entity being tested.
Entity	The entity being tested.
Event Id	Unique identifier for the event.
Event View	The list of events for this monitor.
Metadata	Associated event metadata.
Monitor	The name of the monitor.
Original State	The original state of the event (not overridden).
Potential Impact	The potential impact of the state.
Previous State	The previous state of the event.
Process	The name of the process.
Recommended Action	The recommended action to take.
Severity	The severity of the event.
State	The state of the event.
State Reason	The reason for the state (may be overridden).
Suppression Reasons	The reasons this event may have been suppressed.
Test	The name of the test.

Token	Description
Timestamp	The time of the event.
Trend	A link to the P2 Explorer trend for the entity being tested.
Trend End Time	The end time of the Trend used for creating a custom P2 Explorer Trend URL.
Trend Start Time	The start time of the Trend used for creating a custom P2 Explorer Trend URL.
Value	The value of the entity being tested.

Auxiliary Data Tokens

If the test has auxiliary data, this is available as a token in the message content. Type the event metadata key, enclosed in square brackets, so that the literal value at the time of the event is included in the message content. The auxiliary data is also included in the message under the [Metadata] token, below other event information.

Token Outcomes in a Message

When the action is invoked, the token is displayed as the literal value at the time of the event. For example:

Token	Literal Value in SMS or Email Action
[Monitor]	Monitor 1
[State]	High Exceeded
[Timestamp]	20/7/2011 2:18:00 PM
And below are some examples of auxiliary data tokens:	
Event Metadata Key	Auxiliary Data
[Ninety]	Fixed Value: 90
[Pressure]	Attribute :thp

Some of the tokens show a hyperlink, as described in the next section.

Action Hyperlinks

Some of the tokens available for use by actions include hyperlinks.

For actions that use these tokens, the hyperlink is included in the message.

These tokens are:

Asset Report

A link to the asset report for the asset being tested.

- Click the hyperlink in the message content to view the asset report.

Comment Link

A link to the comment tab of the **Event, Info and Comment** screen for the event that triggered the action.

- Click the hyperlink in the message content to open the *Event, Info and Comment* screen for the event that triggered the action. The timeline report appears, containing the event that caused the email action. The *Event, Info and Comment* screen is open, with the cursor in the comment box, in the *Comments* tab.

EventView

The list of events for this monitor.

- Click the hyperlink in the message content to view the list of events for the monitor.

Trend

A link to the P2 Explorer trend for the entity being tested.

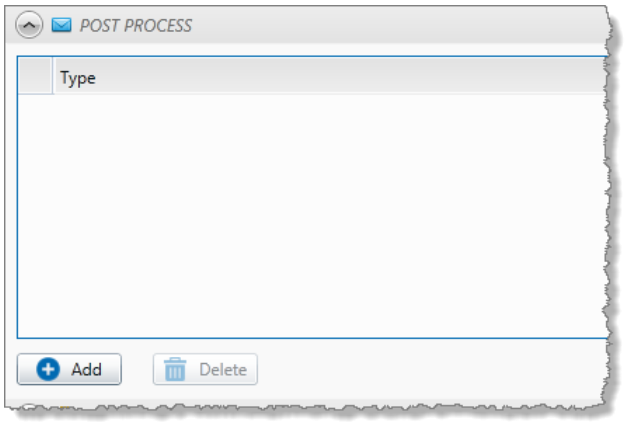
- Click the hyperlink in the message content to view the P2 Explorer trend for the entity.

Step 5. Add Post Process

The Post Process is an optional feature of a monitor. When the monitor finishes running, P2 Sentinel calls a web service, if this has been selected in the **Post Process** section of the monitor.

In the **Monitor** page:

1. Expand the **Post Process** panel.



2. Click **Add**.
3. Select *Web Service* from the **Type** drop-down list.

Note: The web service needs to be specified in the **Sentinel Configuration** file. Refer to the *P2 Sentinel Installation and Administration Guide*.

- To delete a post process, select it in the grid and click **Delete**.

Step 6. Save the Monitor

The monitor must be saved for any changes to take effect.

Note: If change management is configured for P2 Sentinel, the monitor must also be approved before any changes take effect. Refer to "**Update the P2 Sentinel Configuration File**" in the *P2 Sentinel Installation and Administration Guide*.

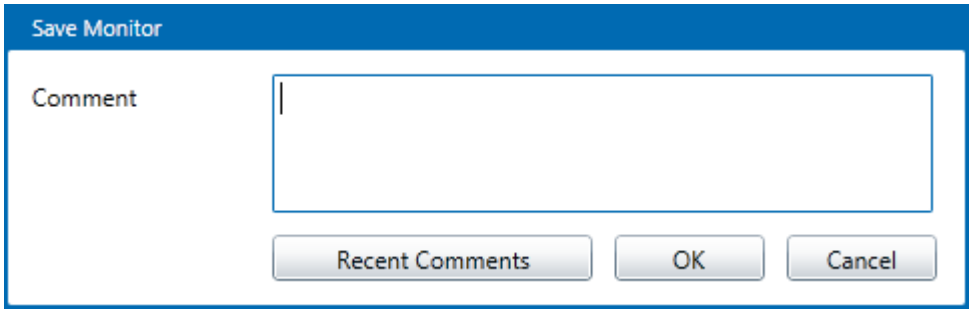
Depending on what is specified in the P2 Sentinel configuration file, the **Save Monitor Comment** is optional, mandatory, or unavailable.

SAVE A MONITOR WITH COMMENTS

If the monitor comment is mandatory or optional (as specified in the P2 Sentinel configuration file):

1. Click **Save**, at the upper left of the tab.

   The **Save Monitor** dialog box opens.



2. Add a comment.

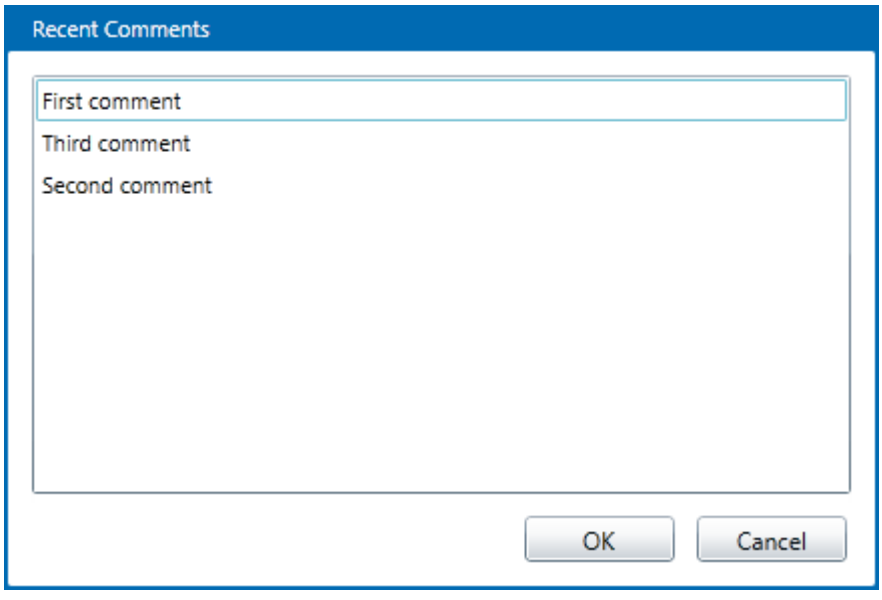
Note: You can skip this step if the message comment is optional.

- Type a comment in the **Comment** box.

or

a. Click **Recent Comments**, to use or refer to recent comments.

   The **Recent Comments** window shows a list of your ten most recent comments (de-duplicated) for saved monitors.



b. To use a comment, click on the comment in the list, then click **OK**.

   The Recent Comments window closes, and the selected recent comment appears in the **Comment** box, overwriting any text that was already there.

c. Type additional text in the **Comment** box, if necessary.

3. Click **OK** to save.

The monitor is saved with full version details.

Note: If change management is configured for P2 Sentinel, this is a minor version only.

SAVE A MONITOR WITHOUT COMMENTS

If monitor comments are not allowed (as specified in the P2 Sentinel configuration file):

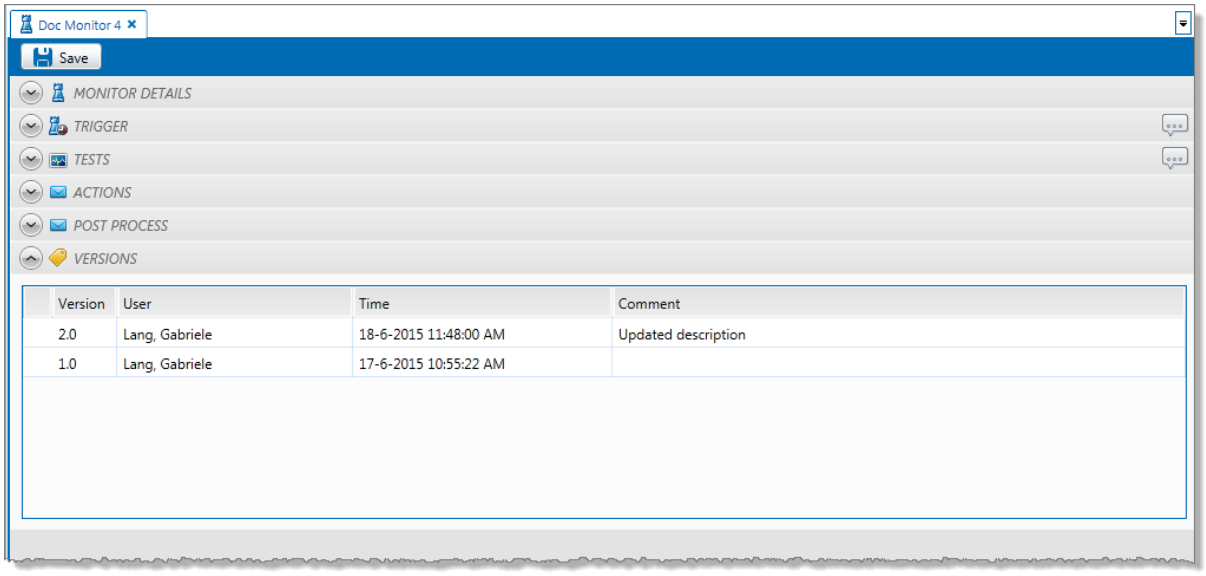
- Click **Save**, at the upper left of the tab.

The monitor is saved with full version details.

Note: If change management is configured for P2 Sentinel, this is a minor version only.

VERSIONS

Every time a monitor is saved, the version details are saved, and displayed in the **Versions** panel on the monitor page.



Version

The version number starts at one. Every time a monitor is saved, the version number is incremented by 1.

Note: If change management is configured for P2 Sentinel, this is a **minor** version and is incremented by 0.1. Each **major** version is incremented by 1.0. A minor version needs to be approved before it changes to a major version.

User

The user name of the person who saved the monitor

Time

The date and time that the monitor was saved

Comment

The user comment that was added when the monitor was saved

Note: Comments can only be added if they are enabled in the P2 Sentinel configuration file.

Review State

This is only applicable where change management is configured for P2 Sentinel. The possible review states are:

Approved

The version is approved. To see the approval details (approver, date, and comment), hover the mouse over the information icon.

Submitted for Approval

This monitor has been submitted for approval. If you decide you do not want the monitor to be submitted after all, click the **Unsubmit** button.

Note: You cannot change a monitor while it is in a submitted state.

Rejected

The version is rejected. To see the rejection details (approver, date, and comment), hover the mouse over the information icon.

Not Submitted

The version has not been submitted. If this is the latest version: to submit, click the **Submit for Approval** button.

SAVING A MONITOR THAT IS PENDING APPROVAL

You cannot save a monitor that is awaiting approval. Either unsubmit the monitor, or wait for it to be approved, before trying to save any changes.

SAVING A MONITOR WITH RECENT CHANGES

If you make changes to a monitor and it is then approved or saved by another user, you will not be able to save your changes.

A message appears in the monitor header: "*Saving is not allowed because changes have been made to this monitor. Press the refresh button to get the latest version*." A Refresh button appears on the far right of the monitor header.

1. Click **Refresh**.
2. Click **Yes** in the *Lose changes* confirmation window.

   The latest monitor details appear on the Monitor tab.
3. Edit the monitor, then click **Save**.

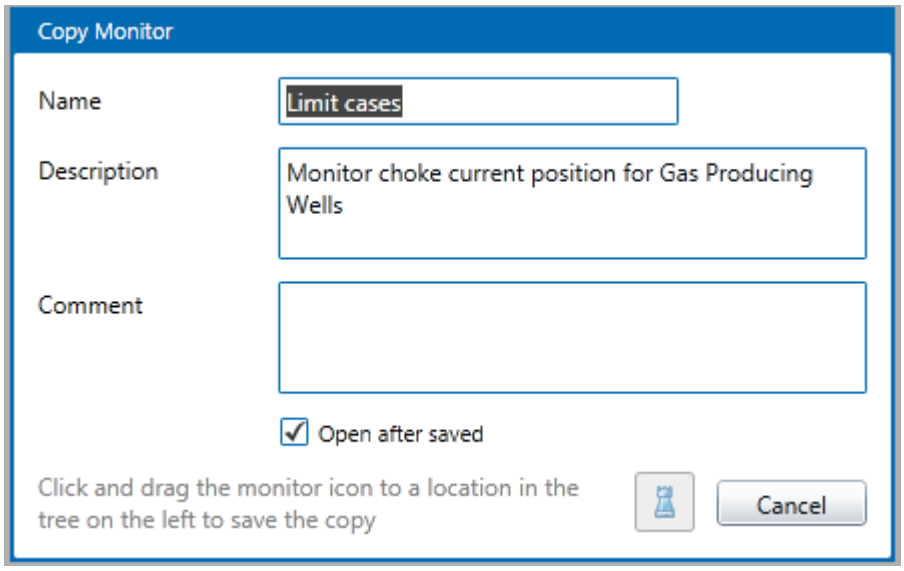
Copy an Existing Monitor

If you want to create a new monitor that contains elements of another monitor, you can copy an existing monitor and then build changes into the new monitor.

In the Workspace Panel, locate the **monitor** that you want to copy.

1. Right-click on the monitor.
2. Select **Make a Copy** from the monitor menu.

The **Copy Monitor** window appears, and monitor details are loaded.



A progress window is displayed while details of the existing monitor are copied.

3. In the **Name** edit box, type a unique monitor name. The monitor name defaults to the name of the copied monitor.

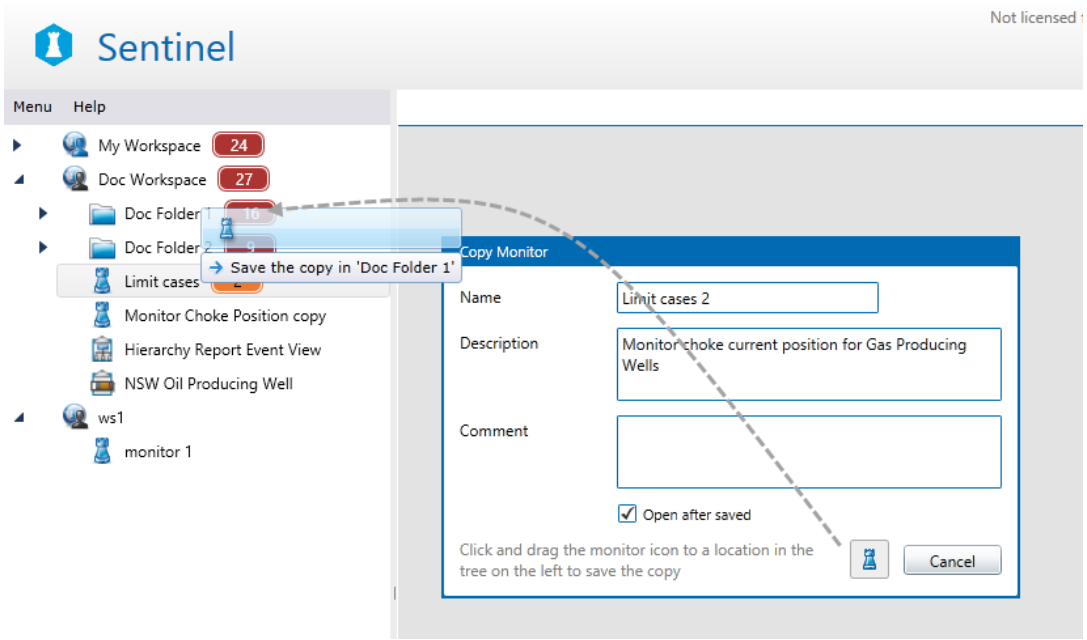
4. Optionally, in the **Description** edit box, type a description for the monitor.

5. In the **Comment** box, type a comment.

Note: Depending on what is specified in the P2 Sentinel configuration file, the **Comment** is optional, mandatory, or disabled.

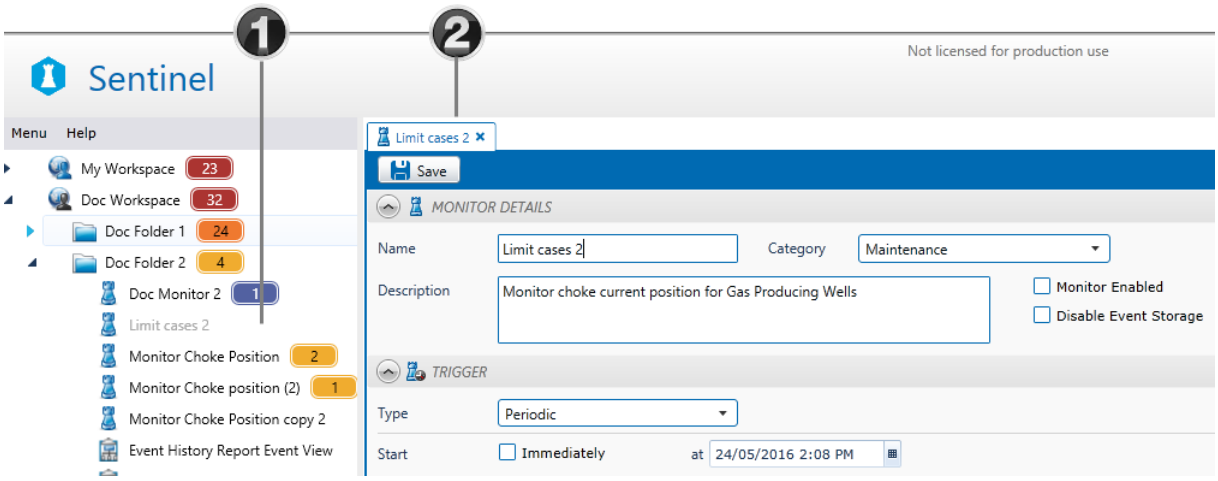
6. Select the **Open after saved** check box, if you want the new monitor to open in a new tab on the Main panel as soon as it is ready.

7. Click and drag the monitor icon to a location (workspace or folder) in the tree on the Workspace panel on the left.



The monitor copying process takes a few seconds. This is indicated by the progress icon, on the *Copy Monitor* window.

When the monitor copy is complete, the *Copy Monitor* window closes.



1. The new monitor is saved to the specified location, in the **Workspace Panel**.
2. If **Open after saved** was selected, the new monitor appears on a new tab in the **Main Panel**.

8. You can now edit the new monitor, if required.
9. To enable the monitor, select the **Enabled** check box on the Monitor Details panel.

Note: If change management is configured for P2 Sentinel, this is a minor version of the new monitor, and still needs to be approved.

Edit a Monitor

Editing a monitor is similar to adding a new one.

Note: You cannot change a monitor while it is in a submitted state. The submitted state only applies where P2 Sentinel is configured to use change management.

You need to edit a monitor to perform the following tasks:

- Change the monitor details.
- Enable or disable the monitor.
- Update the trigger.
- Add, edit, or delete monitor tests.
- Add, edit, or delete monitor actions.

In the Workspace panel, locate the **monitor** that you want to edit.

1. Right-click on the monitor.
2. Select **Edit** from the monitor menu.

   The monitor opens in a new tab in the **Main Panel**.
3. Apply changes to the monitor.

- Change the Monitor Details. Follow the instructions in *Step 1. Add Monitor Details*.
- Change the Trigger. Follow the instructions in *Step2. Add a Trigger*.
- Change Tests:
  - Add Tests
  - Edit Tests
  - Delete Tests
  - Organise Tests
- Change Actions. Follow the instructions in *Step 4 Add Actions* to:
  - Add Actions
  - Edit Actions
  - Delete Actions

4. Save the monitor.
   a. Click **Save**.
   b. Add a comment (if comments are enabled in the Sentinel configuration file).
      i. Type a comment in the **Comment** box, in the **Save Monitor** dialog box.
      ii. Click **OK**.

Note: If P2 Sentinel has been configured to use change management, it is important that you add a meaningful comment to assist with the approval process.

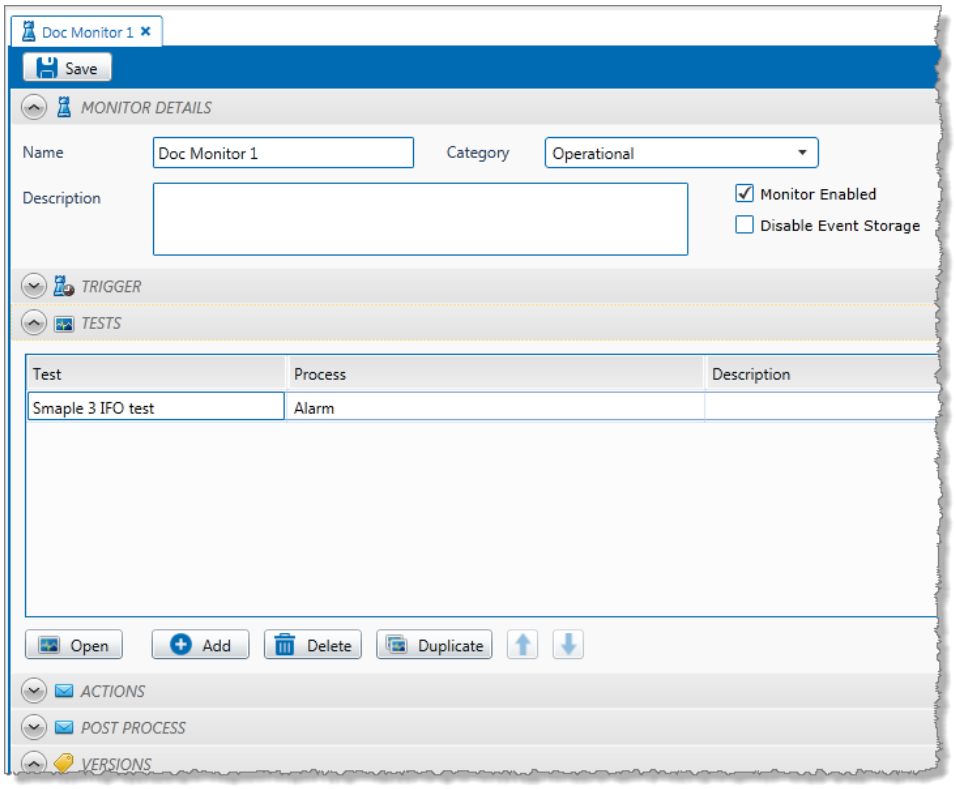
The monitor is saved with the latest version information. If P2 Sentinel has been configured to use change management, this includes a minor version number.

Note: If P2 Sentinel has *not* been configured to use change management, any changes to the monitor take effect as soon as you save the monitor. If P2 Sentinel *has* been configured with change management, the changes only take effect when the monitor is approved.

Edit a Test

You need to edit a test in order to perform the following tasks:

- Change the test details.
- Change the test source.
- Add, change, or remove preconditions.
- Change the test process.
- Change the state configuration.
- Change the test actions.



Perform the following steps to edit a test:

1. In the **Test** panel of the monitor, click a row on the test grid to select it.
2. To open the test, double-click on the row or select the row and click the **Open** button.

   The test opens in a new tab in the Main Panel.
3. Apply changes to the test. Follow the instructions in *Step 3. Add Tests*.
4. Click **OK** to save the test.

The test is saved. All changes will take effect when the test is invoked at the next trigger time, and only after the monitor is saved (and the new version is approved if P2 Sentinel uses Change Management).

Delete a Test

To delete a test:

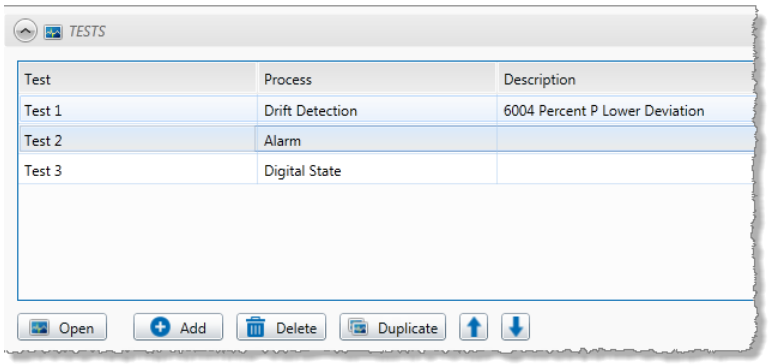
1. In the **Test** panel of the monitor, click a row on the test grid to select it.
2. Click the **Delete** button.
3. At the prompt, click **Yes**.

The test is deleted, as well as all of its associated events and cases.

Note: The monitor must be saved (and approved if P2 Sentinel uses Change Management) for this change to take effect.

Organise Tests

Tests can be moved up or down in the **Tests** grid. This has no functional effect, other than providing a way for you to organise tests within the monitor.



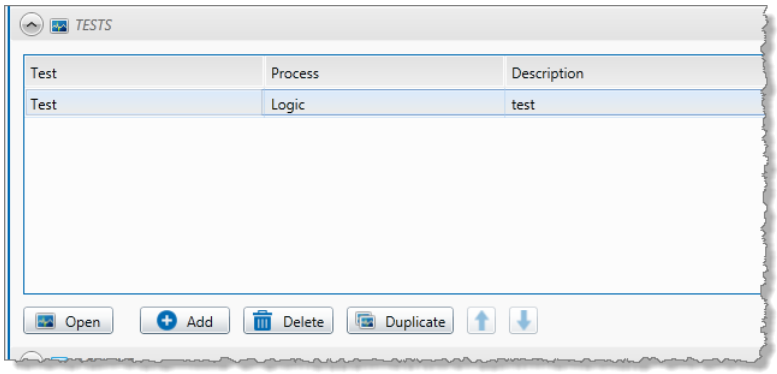
In the **Test** panel:

1. Click a row on the test grid to select it.
2. Move the row up or down a level.
   - Click **Up** to move the test up one level in the grid.
   - Click **Down** to move the test down one level in the grid.
3. Repeat step 2 until the test is in the preferred position on the grid.

Note: The monitor must be saved (and approved if P2 Sentinel uses Change Management) for this change to take effect.

Duplicate a Test

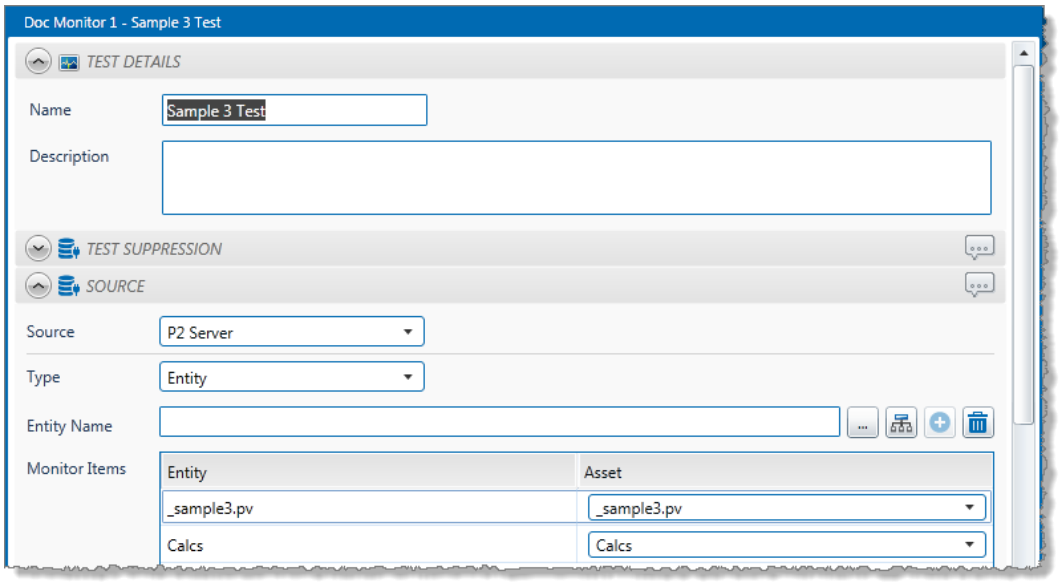
A P2 Sentinel test can be duplicated within the same monitor. Every test within a monitor must have a unique name; other than this, all features of the test are identical to the original. You can change any part of the new test to suit its purpose.



To copy a test:

1. In the **Test** panel of the monitor, click a row on the test grid to select it.
2. Click the **Duplicate** button.

   The copied test page appears.



3. Type a new test name in the **Name** box.
4. You can change any of the test features, such as suppression details, preconditions, process details, and so on, following the instructions in **Step 3. Add Tests**.
5. Click **OK** to save the test.

Delete a Monitor

Because monitors can be quite complex to set up, you should not delete them unless you are absolutely certain that you need to.

To delete a monitor:

1. In the Workspace panel, locate the **monitor** that you want to delete.
2. Right-click on the monitor.
3. Select **Delete** from the monitor menu.
4. At the prompt, click **Yes**.

The monitor is deleted. All events and cases associated with the monitor are also deleted.

Note: A monitor can also be disabled.

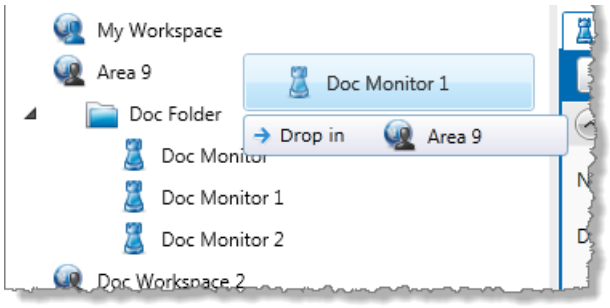
Move a Monitor

You can move a monitor to a different workspace, or to a different folder.

In the Workspace panel, locate the **monitor** that you want to move.

1. Click and drag the monitor to the destination workspace or folder.

   Tip: The destination workspace or folder is displayed when the monitor is correctly positioned.



2. Release the mouse button.

The monitor is moved to the destination workspace or folder.

Disable a Monitor

If you do not want a monitor to run, you can disable it. You can enable it when you are ready to use it again.

A disabled monitor has a grey label in the Workspace panel. In the screenshot below, the monitors "Copy of Stuck Value Random Tag" and "Monitor 2" are both disabled.

To disable a monitor:

1. Right-click on the **monitor** you want to disable.
2. Select **Edit** from the monitor menu, to open the monitor.
3. In the Monitor Details panel, clear the **Enabled** check box.
4. Save the monitor.

   The monitor is disabled.

Note: If change management is configured for P2 Sentinel, the monitor must also be approved before any changes take effect.

- To enable a monitor, follow the same steps, this time *selecting* the **Enabled** check box.

Note: New monitors are enabled by default, whereas copied monitors are disabled by default.

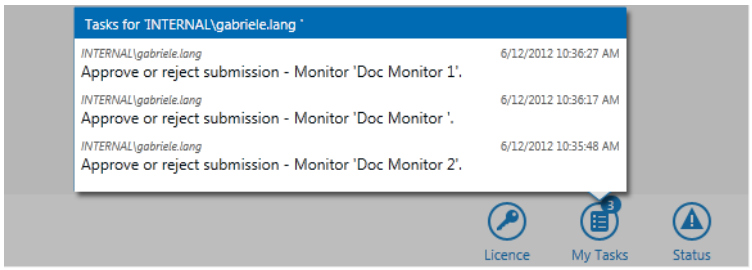
Approve Monitor Changes from My Tasks

Approval or rejection of monitors is part of Change Management, and only applies if P2 Sentinel has been configured to use change management. Refer to "**Update the P2 Sentinel Configuration File**" in the *P2 Sentinel Installation and Administration Guide*.

To approve or reject monitor changes from **My Tasks**:

1. Click **My Tasks** at the lower right corner of the Main Panel.

   A window appears, with a list of tasks. Change management tasks are listed for each *pending approval* monitor that belongs to a workspace for which you have approver privileges.



   Monitor Approval Change Management Tasks
   Each change management task that relates to monitor approval consists of the following:

   User Name
   The name of the user who submitted the monitor for approval

   Date
   The date and time that the monitor was submitted for approval

   Task
   The task description, as well as the monitor name.

2. Click on a task in the window.

   A **Pending Approvals** tab opens, for the workspace to which the selected monitor belongs.

   Note: All *pending approval* monitors within the workspace are listed.

3. Approve or reject the various monitors, as explained in the section **Approve or Reject a Monitor**.

4. To close the *My Tasks* window, click any part of the Sentinel screen, apart from the *My Tasks* window itself.

Re-run a Monitor

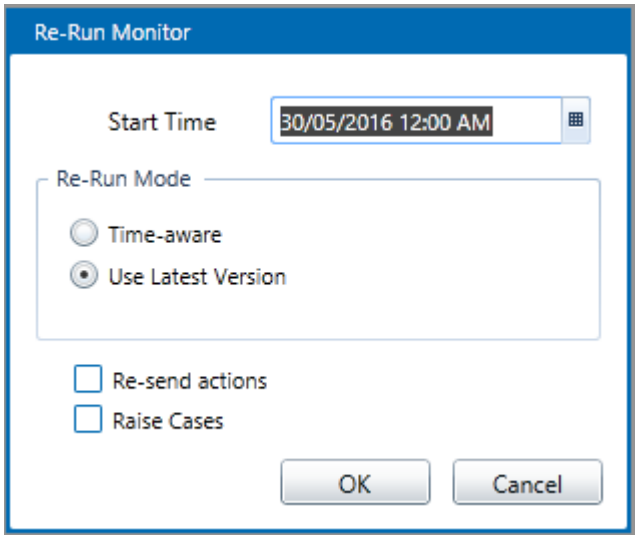
Privileges: To re-run a monitor, you need a security role that has the **Workspaces Re-Run** privilege.

You can re-run a monitor from any time in the past. If you want to re-run a monitor from the time before it was first created, you can do so by using the Latest Version mode (see below). You need appropriate security privileges to re-run a monitor.

If Case Management is enabled in Sentinel, then all cases that were previously raised by the monitor's events since the Start Time specified in the Re-Run are deprecated.

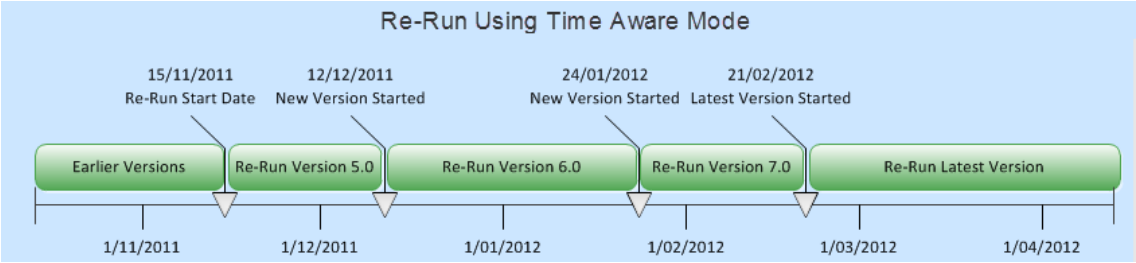
1. In the Workspace panel, locate the **monitor** that you want to re-run.
2. Right-click on the monitor.
3. Select **Re-Run** from the monitor menu.

   The **Re-Run Monitor** screen appears.



4. To select a start date and time, click the calendar icon in the **Start Time** edit box. The default date and time is 12:00 AM of the current date.
5. Select the **Re-Run Mode.**

   Time-aware
   The monitor runs using every major version of the monitor from the selected start time.



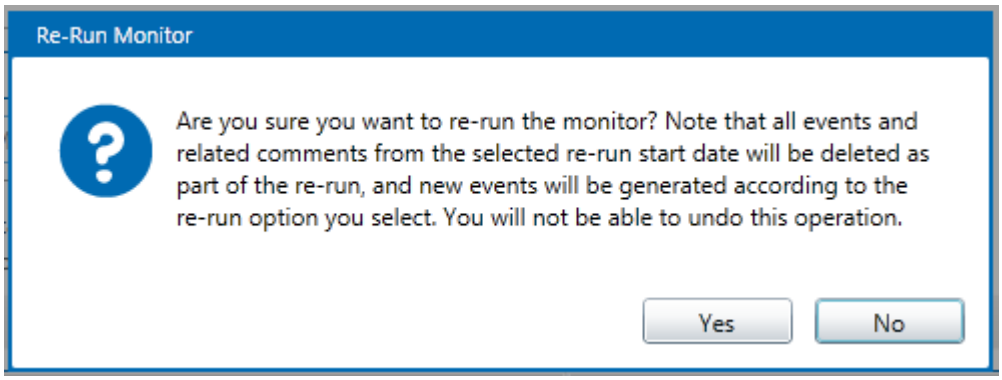
   Use Latest Version
   The latest major version of the monitor runs through all data from the start time.

6. If you want actions to be raised, select the **Re-send actions** check box. Actions will be sent where they are triggered, for the entire period covered by the re-run.
7. If you want to raise cases, select the **Raise Cases** check box.

Note: This option is only available if **Case Management** is enabled.

8. Click **OK.**

9. Click **Yes** on the **Re-Run Monitor** confirmation screen that appears.

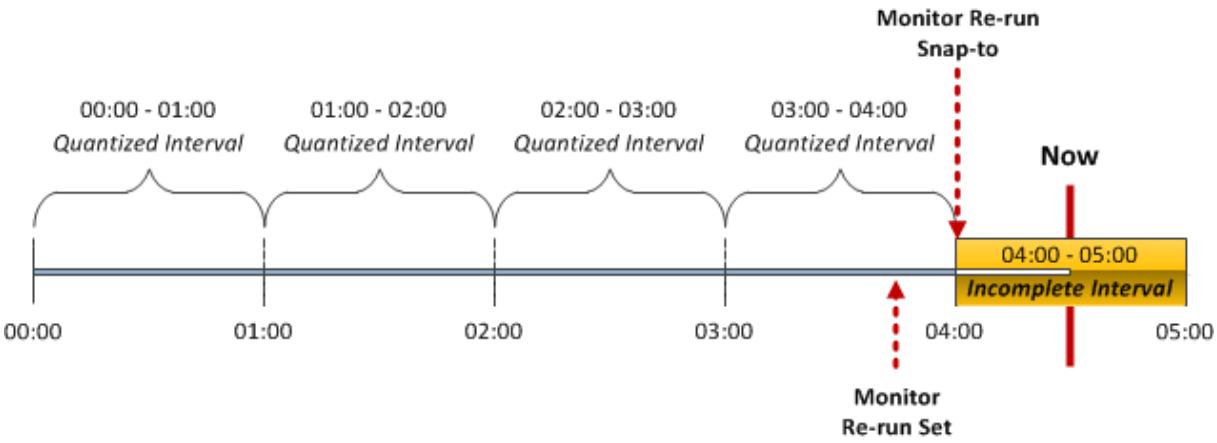


Note: All the events and related comments from the selected re-run start date will be deleted as part of the re-run, and cases will be deprecated. New events will be generated according to the re-run option you select.

The monitor starts the re-run immediately, starting from the selected start time and continuing into current time, using the selected re-run mode.

Note that while the monitor is re-running over historical data, current events are not triggered. You may edit a monitor while it is undergoing a re-run.

Note: You cannot re-run a quantized monitor if it does not have a full period of data to process. Let's say the current time is 4:30 and we have a quantized monitor set to run at hourly intervals (commencing at the beginning of the hour and ending at the end of the hour). If you schedule a monitor re-run for, say, 3:45, the re-run will snap to the nearest hour (4:00) due to it being a quantized monitor, and it will attempt to re-run the period commencing at 4:00. However, as it does not have a full hour to process (as the current time is 4:30), the monitor re-run will fail.



Delete a Monitor's Events

Privileges: To delete events, you need a security role that has the **Sentinel Events Delete** privilege.

If you have the required privileges, you can delete events from a monitor. Note that any cases raised from these events will also be deleted.

To delete a monitor's events:

1. In the Workspace panel, locate the **monitor** whose events you want to delete.
2. Right-click on the monitor.
3. Select **Delete Events and Reset** from the monitor menu.
4. At the prompt, click **Yes**.

The monitor's events are deleted, as well as any cases that were raised by these events.

Viewing Events

Privileges: Users who can view a workspace, can view any of the events in the workspace. See Workspace Security Roles. To add or edit an event view you need a security role that has the **Sentinel Workspaces Edit** privilege. To delete an event view, you need a security role that has the **Sentinel Admin** privilege.

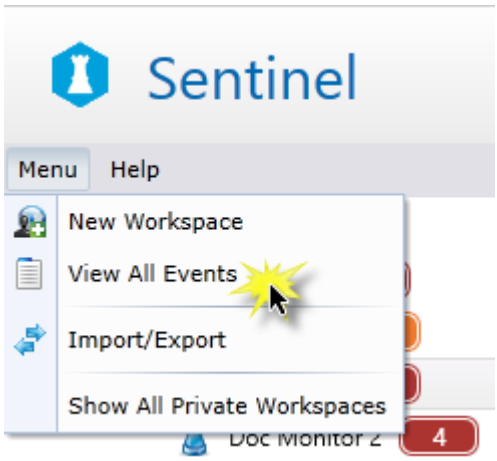
In Sentinel, you can view all current events across all public workspaces, or you can view all current events for a workspace, a folder, or a monitor. If you have privileges, you can edit events, from within the event viewer.

If you have privileges, you can delete events (and related cases) for a monitor. This is described in an earlier section, Delete a Monitor's Events.

Note: You can also view an event using a Sentinel Event Viewer URL.

Viewing All Events

1. Click the Menu button below the Sentinel header.
2. Click **View All Events**



All current events (for every monitor in P2 Sentinel) are displayed in a new events page, entitled **All Events**, in the Main panel.

Viewing Workspace Events

1. In the Workspace panel, locate the workspace.
2. View events for the workspace.
   - Right-click on the **workspace** and select **View Events** from the list.

     or

   - Click the event notification 6 icon to the right of the workspace. (There may be more than one of these icons, if different severities are shown separately. You can click on any of them.)

All current events (for every monitor in every folder of the workspace) are displayed in a new events page in the Main panel. The page title is the workspace name.

VIEWING FOLDER EVENTS

1. In the Workspace panel, locate the folder.
2. View events for the folder.
   - Right-click on the **folder** and select **View Events** from the list.

     or

   - Click the event notification 6 icon to the right of the folder. (There may be more than one of these icons, if different severities are shown separately. You can click on any of them.)

All current events (for every monitor in the folder) are displayed in a new events page in the Main panel. The folder name is used as the page title.

VIEWING MONITOR EVENTS

1. In the Workspace panel, locate the monitor.
2. View events for the monitor.
   - Right-click on the **monitor** and select **View Events** from the list.

     or

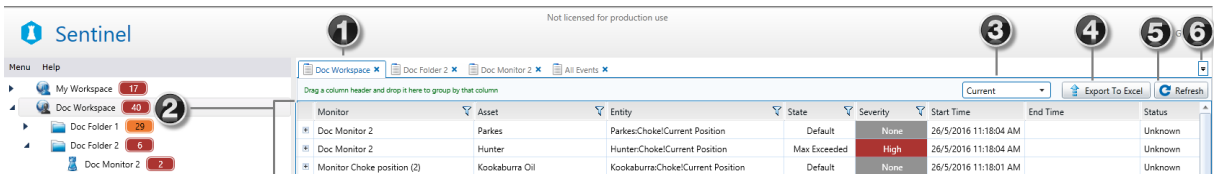
   - Click the event notification 6 icon to the right of the monitor. (There may be more than one of these icons, if different severities are shown separately. You can click on any of them.)

All current events (for the workspace) are displayed in a new events page in the Main panel. The page title is the monitor name.

THE EVENTS PAGE

The events page is named after the workspace, folder, or monitor that it relates to (see above sections). For all events in P2 Sentinel, the page is named *All Events*.

The events page contains an events grid with a list of all current events for the workspace, folder, or monitor, or for the whole of P2 Sentinel.



The important features in the events page are:

	Feature Name	Description
1	Events page title	The workspace, folder or monitor name, or *All Events*.
2	Events grid	All of the current events for the workspace, folder, or monitor, or all of P2 Sentinel.

	Feature Name	Description
3	Period selector	Select current events, or also include events that ended within the selected period (for example, events that ended within the last 24 hrs).
4	Export to Excel	Click to export the grid to a Microsoft® Excel® spreadsheet.
5	Refresh	Click to refresh the page. The latest events are displayed.
6	Selecting an Open Tab	Click the downward-pointing arrow, and select an open tab from the drop-down list.

EVENTS GRID

The events grid (when viewed from the events page) displays the current event state of every test item for the selected monitors.

- To close the page, click the close icon next to the page name.

EVENT DISPLAY OPTIONS

Note that all current events, regardless of when they began, and including suppression events, are shown in the events grid. Thus, there may be no event notification label for a monitor (if, for example, the current event options is set to show events that started today, and no current events actually started today); however, you can still view current events that started before today in the events grid.

Events Grid

The events grid consists of the following columns:

Leftmost column
This column has buttons to expand + or collapse − the event details.

Monitor
The name of a monitor that has tests with current events

Note: This column is only displayed for Workspace Events and Folder Events.

Asset
The name of an asset that has a current event; you can view the asset reports from here.

Entity
The name of the entity that defined the asset

State
The state that was reached to raise the current event displayed.

Note: Where state override has been applied in the state configuration, the override state is displayed here.

Severity
The configured state severity of the event that was raised

Start Time
The start time of the event; this is the time that the data reached a value to cause the current event.

End Time
The end time of the event

Note: This time is only known and displayed in the event log.

Status
Note: This column only appears if *Case Management* is configured.

An event has three possible statuses, relating to case management:

Unknown
This is for an event that either hasn't raised a case, or there is a case that is still in the **New** or **Investigating** status (in P2 Explorer).

Valid
The event has raised a case which has the **Confirmed** status (in P2 Explorer).

Invalid
The event has raised a case which has the **Rejected** status (in P2 Explorer).

State Duration
The duration of the current event

Test
The name of a test that has test items with current events

Comments
The total number of event comments is displayed here.

Most Recent Comment
The most recent event comment is displayed here.

The events grid appearance can be manipulated in the following ways:

- You can sort most of the columns in the grid.
- You can group by a column header for the following columns:
  - Monitor
  - Test
  - Asset
  - Entity
  - State
  - Severity
  - Status

FILTER EVENTS

Most of the column headers offer the ability to filter data according to specified criteria:

- You can filter on any of the columns that have a filter icon in the header.

EXPORT EVENTS

To export the event list for workspace events, folder events, or monitor events:

- Click the **Export to Excel** button, at the upper right of the tab, to export the events.

The events are exported to a Microsoft ® Excel ® spreadsheet.

REFRESH EVENTS

The event for any entity will continue (as recorded in State Duration) until a state change causes a new event.

Refresh the events page to see the latest State Duration figure for a continuing event, or to view new event details.

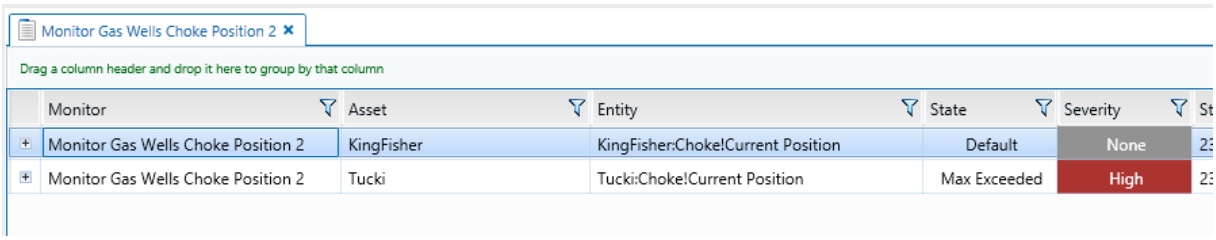
- Click the **Refresh** button at the upper right of the tab.

The latest event information appears on the tab.

Editing Events

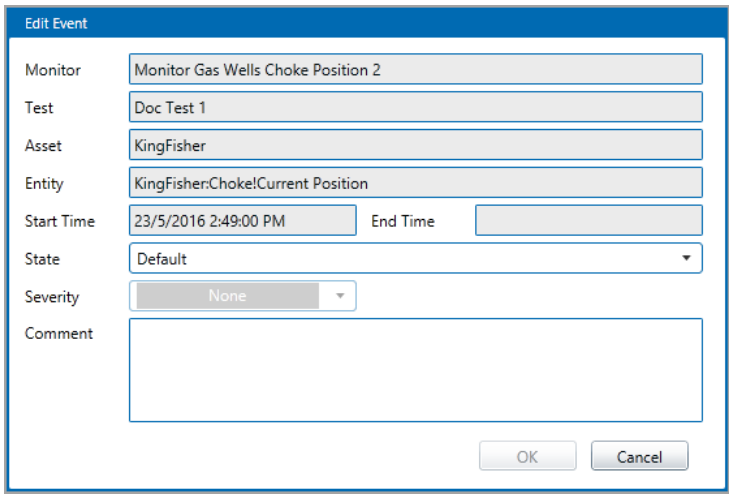
To edit an event:

1. In the events grid, locate the event you want to edit.



2. Double-click on the event in the grid.

   The **Edit Event** window opens:

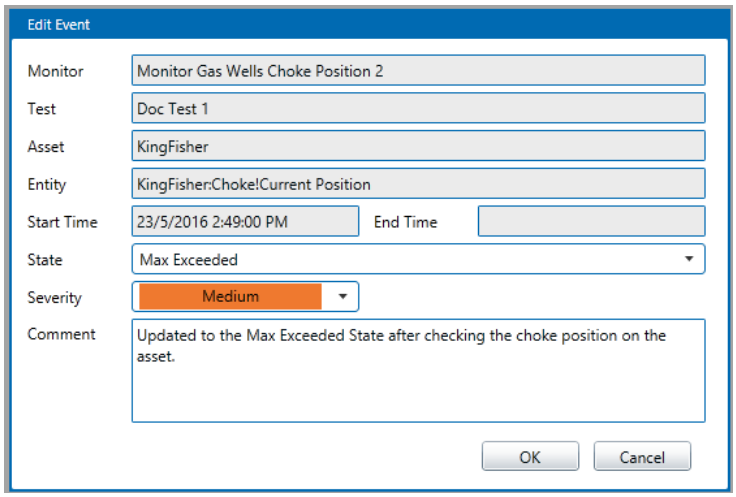


3. To change the state, select a new **State** from the drop-down list.
4. To change the severity, select a new **Severity** from the drop-down list.

   Note: You cannot change the severity of the **Default** state.

5. Type a **Comment** in the edit box.

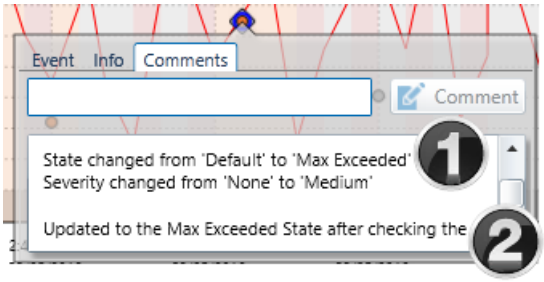
   Note: This is required for all event updates.



6. Click **OK**.

   The event is updated with your comment, and a system comment.

1. Sentinel system comment
2. User comment

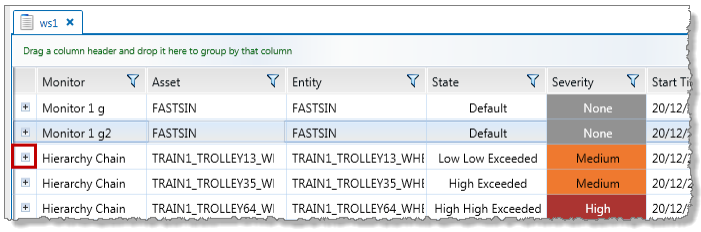


View Event History and Comments

Every event is caused by the monitor item reaching certain values during a test process, to exceed a defined limit or to reach a predefined state.

These values are stored in the P2 Sentinel database, and can be viewed from the events grid. You can also view event comments from the events grid.

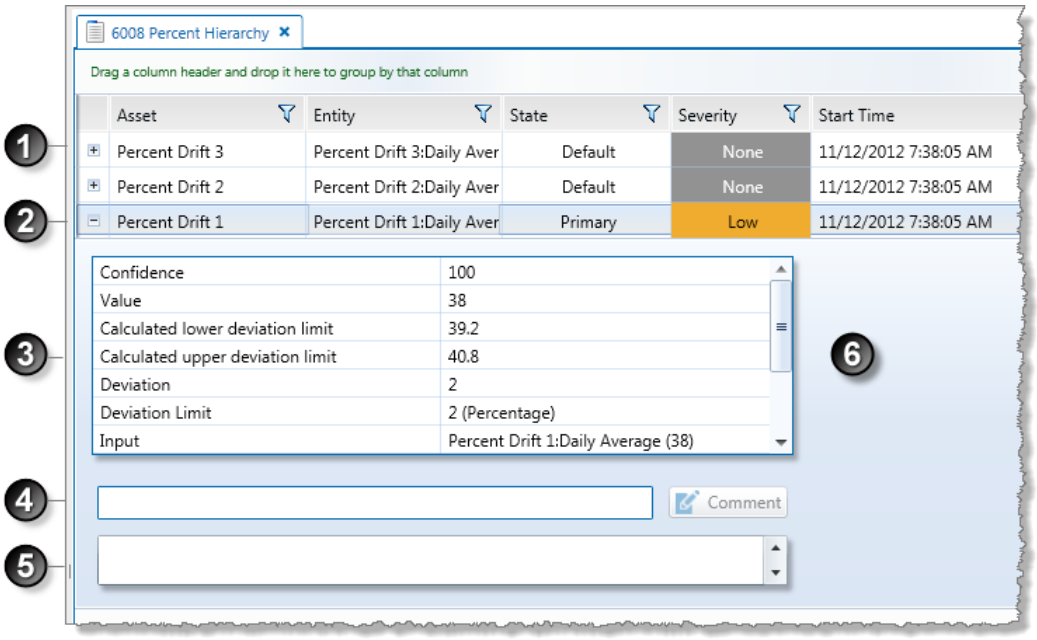
Note: Events are not stored for a monitor if you have selected **Disable Event Storage**.



To view the event history and comments:

- Click the expand ⊞ button in the left-most column of the event grid.

The event history is displayed below the row, on a separate panel (the event history panel).



1. The event grid
2. The event
3. Event history table
4. Comment box
5. Comment history
6. The event history panel

The events history panel is positioned between two rows in the events grid, and consists of the following components:

Events history table

This is a table showing the state of the test entity at the time that the event was reached. Depending on the type of process used, various different fields are described. These may include the following:

Confidence

The confidence value of the test entity data.

Value

The value of the test entity data.

Event Values Relating to Process

These values depend on the process used, and also on the current state for this event. Some examples are:

High High Limit

The value of high high limit at the time of the event.

High Limit

The value of high limit at the time of the event.

Min

The value of min at the time of the event.

Max
The value of max at the time of the event.

Integral
The integral at the time of the event.

First Primary State Time
The start time of the primary state which preceded the current state; or, if this is currently a primary state, the start time of the event.

First Secondary State Time
The start time of the secondary state which preceded the current state; or, if this is currently a secondary state, the start time of the event.

Potential Impact
If the state configuration for this state outcome of the monitor test has a *Potential Impact*, this is stored and displayed.

Recommended Action
If the state configuration for this state outcome of the monitor test has a *Recommended Action*, this is stored and displayed.

State Reason
If the state configuration for this state outcome of the monitor test has a *Reason for State*, this is stored and displayed.

Auxiliary Data
Any auxiliary data that has been added to the test is displayed in the format of *Event Metadata Key*, *Auxiliary Data* (for example *Pressure*, *80*).

Original State
The state that the test entity reached to cause the event; this row is only shown if there is a state override in the test's state configuration.

Comment box
The input area for an event comment.

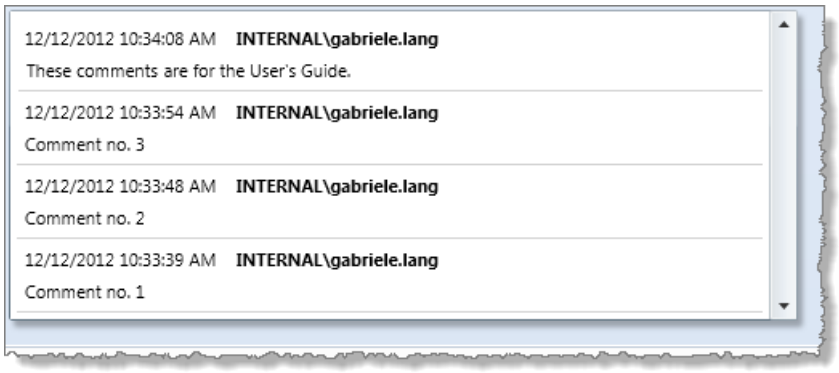
Comment History list
This is a list of all comments that have been added for this event. The most recent comment is first on the list.

Each comment has the following:

Date and time
The date and time that the comment was added.

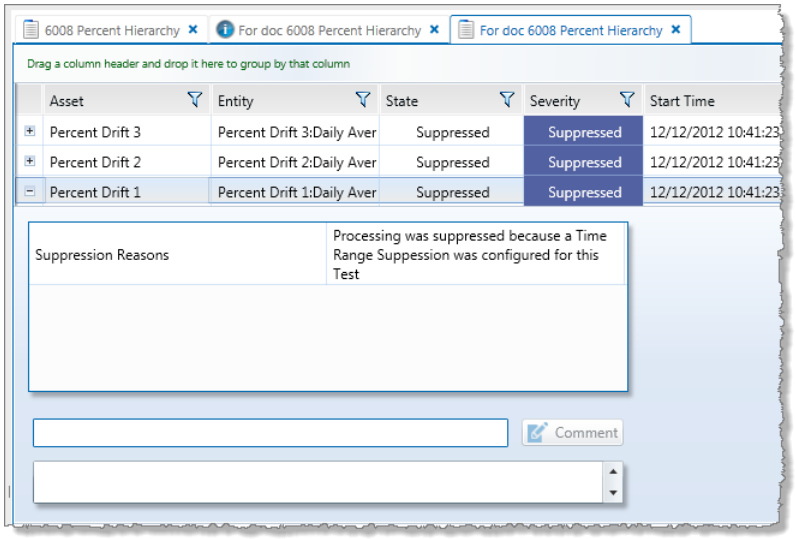
User name
The user name of the person who added the comment.

Comment
The comment that was added.



EVENTS HISTORY TABLE FOR SUPPRESSED EVENTS

If an event is suppressed the event history table show the suppression reason, as illustrated in the example screen image below:



For suppressed events, the event history shows a suppression reason, which may be one of the following:

Time Suppression
Processing was suppressed because a Time Suppression was configured for this Test.

Precondition Suppression
Processing was suppressed due to a precondition that was met.

Missing Data Suppression
Processing was suppressed because no data was returned.

Standard Precondition Out of Suppression Delay
Processing was suppressed for an additional period after a precondition suppression, based on an *Out of Suppression Delay* setting.

Bad Data
Bad Data (*Low Confidence* data).

Monitor Chaining

Processing was suppressed because the test configured for Chaining was not in the configured state.

For more information on suppressed data, refer to the **Suppressed State** section in the overview on States.

CLOSE EVENT HISTORY AND COMMENTS

To close the event history and comments tab:

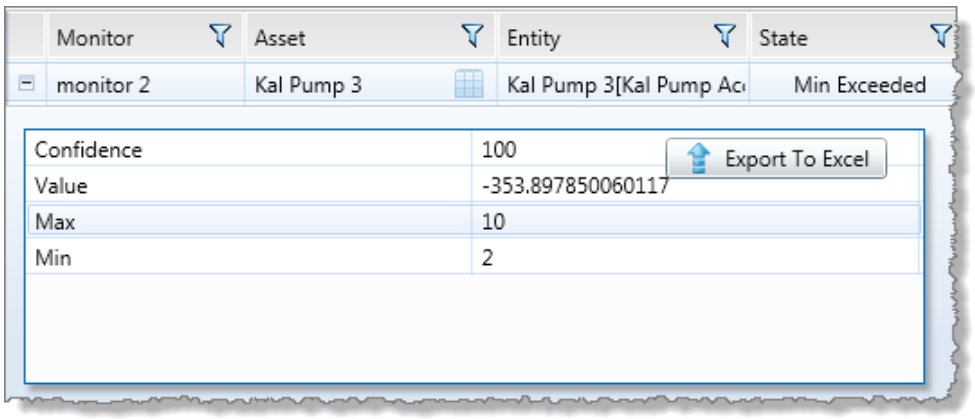
- Click the collapse button of the event row.

Export Event History

To export the event history details, follow these steps:

1. Open the history and comment details for an event.
2. Hover the mouse over the event history table.

   An **Export to Excel** button appears on the upper right of the events history table.



3. Click on **Export to Excel** to export to a Microsoft Excel spreadsheet.

   The event history is exported to a Microsoft Excel spreadsheet.

4. Click the collapse button of the event row, to close the event history and comments tab.

Add Event Comments

You can add event comments from:

- The events grid on the Events page.
- The Edit Event window (see Editing an Event).
- An event point in the Timeline report.
- Directly from a URL, or from an email hyperlink (produced by an event action).

Note: You can add more than one comment to an event.

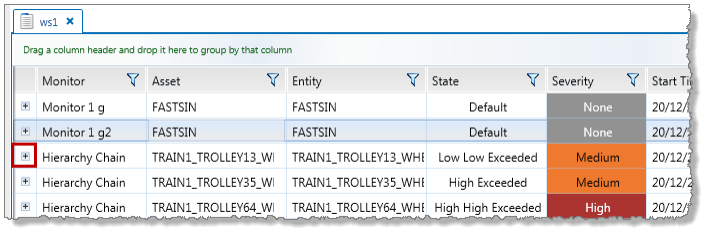
To add comments to an event, follow the steps below for:

- Adding comments from the events page.
- Adding comments from the timeline report.

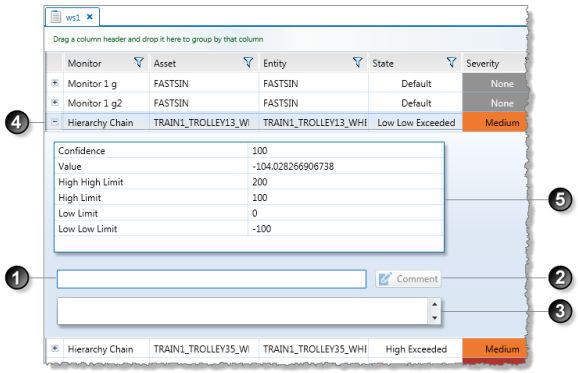
- Adding comments from an action email.

Adding Comments from the Events Page

1. Click the expand button in the left-most column of the event grid.



The events detail and comment screen opens:



1. Comment box
2. Comment button
3. Comment history list
4. Collapse icon of the event row
5. Event details

2. Type a comment in the comment box.

   The comment box expands.

   Note: The comment box has scroll bars for lengthy comments.

3. Click the **Comment** button to save the comment.

   The comment box is cleared and the **Comment** button appears dimmed.

   The comment is saved, with a time stamp and the user name. This is displayed in the comment history list.

4. Click the collapse button of the event row, to close the event history and comments tab.

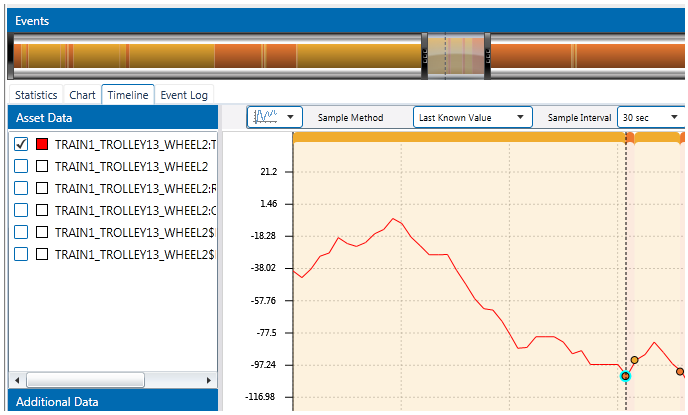
Note: You can add more than one comment to an event.

Adding Comments from the Timeline report

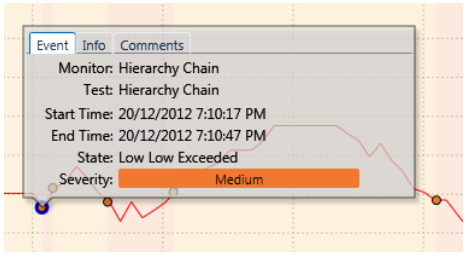
1. Find an event on the timeline report.

2. Click the event icon.

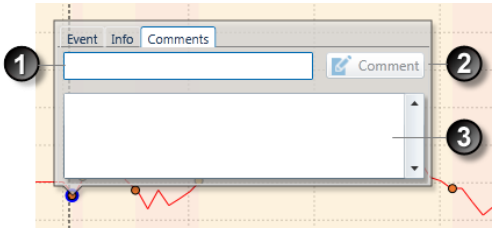
Note: The event icon is circled in blue when you hover the mouse over it.



An **Event, Info and Comment** screen appears.



3. Click the **Comments** tab of the **Event, Info and Comment** screen.



1. Comment box
2. Comment button
3. Comment history list

4. Type a comment in the comment box.

   The comment box expands.

Note: The comment box has scroll-bars for lengthy comments.

5. Click the **Comment** button to save the comment.

   The comment box is cleared and the **Comment** button appears dimmed.

   The comment is saved, with a time stamp and the user name. This is displayed in the comment history list.

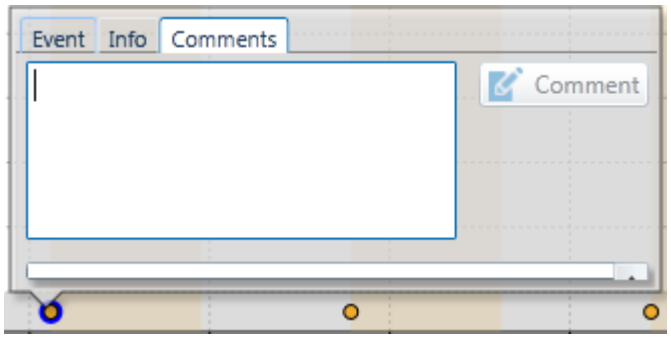
6. To close the **Event, Info and Comment** screen, click any part of the timeline report.

Adding Comments from an Action Email URL

If an action email includes a URL to the event comment (where the **Comment Link** token is included in the email action), you can open the asset report timeline with the comment box open.

1. Open the action email.
2. Click on the comment link.

   The timeline report appears, containing the event that caused the email action. The **Event, Info and Comment** screen opens, with the cursor in the comment box, in the **Comments** tab.



3. Type a comment. Then click the **Comment** button to save the comment.

Note: Alternatively, you can set the appropriate parameters in the asset report URL, and use this URL to open the comment tab for the relevant event.

Sentinel Event Viewer URLs

There is a URL command for the Event Viewer, which uses the **EventViewer.aspx** page on the Sentinel Server.

URL FOR AN EVENT VIEWER

The following URL applies to the Event Viewer:

```
https://[server name]/Sentinel/EventViewer.aspx?MonitorName=[monitor name]
```

The first section of the URL is always:

`https://[server name]/Sentinel/EventViewer.aspx` where [server name] is the name of the Sentinel Server.

The remaining portion of the URL uses one of the three parameters:

- MonitorName
- FolderName
- WorkspaceName

Note: All three parameters are case sensitive.

The parameters are defined as follows:

MonitorName
The name of the monitor to show events for, for example "Pressure Monitor".

FolderName
The name of the folder to show events for, for example "Wells".

WorkspaceName
The name of the workspace to show events for, for example "Operations".

Using the values used in the various parameter definitions above, the final URL will look like this (with a server name of myServer):

Sentinel Event Viewer URL for a monitor:

```
https://myServer/Sentinel/EventViewer.aspx?MonitorName=Pressure Monitor
```

Sentinel Event Viewer URL for a folder:

```
https://myServer/Sentinel/EventViewer.aspx?FolderName=Wells
```

Sentinel Event Viewer URL for a workspace:

```
https://myServer/Sentinel/EventViewer.aspx?WorkspaceName=Operations
```

Note: When constructing the URL, ensure that the first parameter is preceded by the question mark (?) symbol. Subsequent parameters must be preceded by the ampersand (&) symbol.

ADDITIONAL PARAMETERS

As well as specifying the monitor name, folder name or workspace name you can optionally add one or both of the following parameters.

TimePeriod
The period selected dictates the start time for the range of events displayed in the report. Valid periods are:

- Current
- 5 mins
- 30 mins
- Hour
- 24 hrs
- 48 hrs
- 7 Days
- 2 Weeks
- 30 Days
- 60 Days
- 90 Days

Sentinel Event Viewer URL for a workspace with a time period:

https://myServer/Sentinel/EventViewer.aspx?WorkspaceName=Operations&TimePeriod=7 Days

EndTime

Report end time in date time format DD/MM/YYYY hh:mm, for example 10/6/2016 12:00 for midday on 10th June 2016.

Note: The **EndTime** parameter will only work if a **TimePeriod** parameter is also specified.

Custom Event View

Privileges: Users who can view a workspace, can view any of the event views in the workspace. See Workspace Security Roles.

Custom event views offer another way of viewing events from the P2 Sentinel database. With custom event views, you are able to view events based on the P2 Server hierarchical structure.

Assets Presented in the Event Views

The following assets (*event view assets*) are displayed in event views: all assets that are monitored in P2 Sentinel, that belong to the selected *hierarchy*, from the selected *starting point*, occur in the selected *template,* and are monitored by monitors in the selected workspace.

Custom Event View Reports

There are four types of custom event view that you can create in P2 Sentinel. All of the views relate to events for the *event view assets*.

Event Report

This report shows all events, for the selected date/time period, in an events grid, for the event view assets from the selected hierarchy and starting point. The report can be selected for all workspaces, or just for the current workspace.

Event History Report

This report shows all events, for the selected history, in an events grid, for the event view assets from the selected hierarchy and starting point. The report can be selected for all workspaces, or just for the current workspace.

Event Timeline Report

All events for the *event view assets*, over the selected *period*, optionally filtered for *Severity of None*. For saved reports, events for the *latest* period are displayed every time you open the page to view the report.

The event timeline view shows the affected assets, with a corresponding percentage time chart, and an event timeline, as well as the highest severity and the event count, per asset.

Hierarchy Report

All current events for the *event view assets*. For saved reports, *current* events are displayed every time you open the page to view the report.

The hierarchy view essentially shows an events grid for the affected assets.

Note: Only events that have been raised by P2 Sentinel may be viewed in the custom event view reports.

Copy Link to Clipboard

You can copy the link to a custom report.

- Click the **Copy Link to Clipboard** button, at the upper right of the report page.

You can paste the link to the message content of an email, or you can open a new page in your web browser, to view the report on a separate tab.

Create an Event View

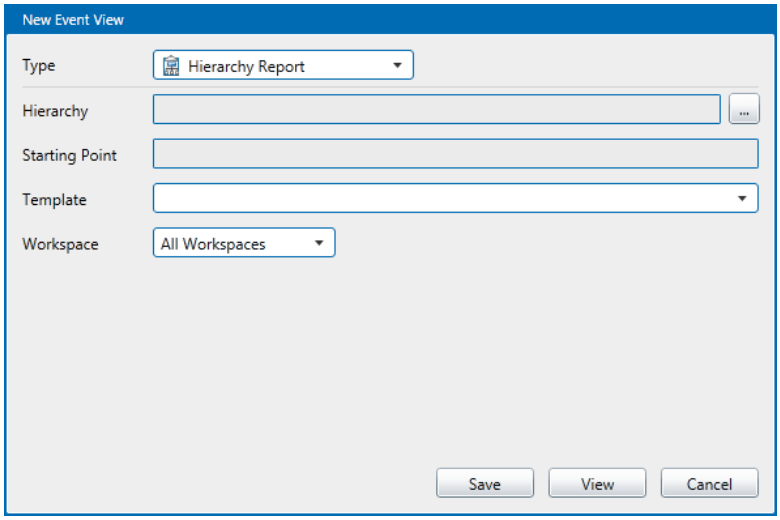
You can create custom event views within a workspace or folder. The custom report can be independent of any of the monitors stored under a particular workspace or folder, and you may move a saved report to another workspace or folder, without affecting the report.

Note: If you select the report for **This Workspace**, then the report only applies to monitors in the workspace where it resides (created or moved to).

To create a new event view:

1. In the Workspace panel, right-click on the Workspace or Folder where you want to create the new event view.
2. Select **New Event View** from the list.

   The **New Event View** window appears in the Main panel.



3. Select a report type, to create a hierarchy report, event report, event history report, or an event timeline report.

   – **To create a Hierarchy Report:**

   i. From the **Type** drop-down list, select *Hierarchy Report*.

   ii. Click the **P2 Server Browser** button next to the **Hierarchy** edit box, and select the Hierarchy (and optionally the Entity for the *Starting Point*) from the P2 Server Browser.

   The selected hierarchy and starting point appear in the **Hierarchy** edit box and the **Starting Point** edit box, respectively.

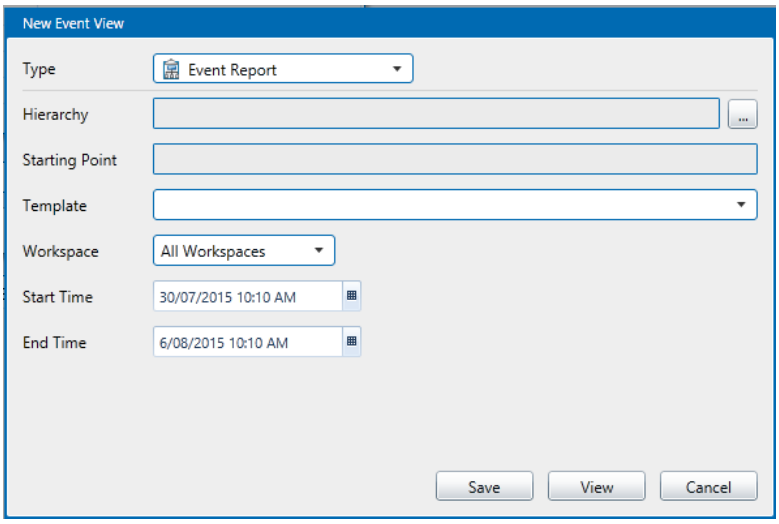
   iii. Select a template or *All Templates* from the **Template** drop-down list.

   Note: Templates listed are those that use the selected entity within the selected hierarchy, from the starting point.

   iv. From the **Workspace** drop-down list, select which workspace (*This Workspace* or *All Workspaces*) on which to base the report.

   – **To create an Event Report:**

i. From the **Type** drop-down list, select *Event Report*.



ii. Click the **P2 Server Browser** button next to the **Hierarchy** edit box, and select the Hierarchy (and optionally the Entity for the *Starting Point*) from the P2 Server Browser.

The selected hierarchy and starting point (if selected) appear in the **Hierarchy** and **Starting Point** edit boxes, respectively.

iii. Select a template, or *All Templates*, from the **Template** drop-down list.

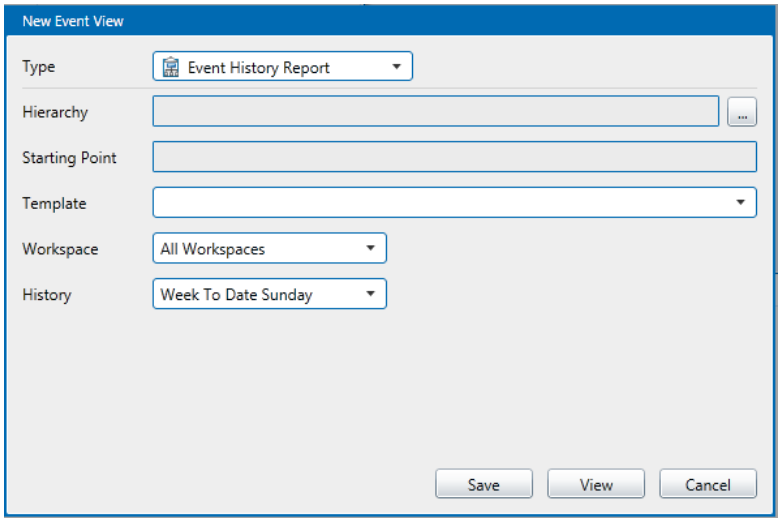
Note: Templates listed are those that use the selected entity within the selected hierarchy, from the starting point.

iv. From the **Workspace** drop-down list, select which workspace (*This Workspace* or *All Workspaces*) on which to base the report.

v. From the **Start Time** date-time picker, select a start time. From the **End Time** date-time picker select an end time. Events that started within this period are shown in the report.

– **To create an Event History Report:**

i. From the **Type** drop-down list, select *Event History Report*.



ii. Click the **P2 Server Browser** button next to the **Hierarchy** edit box, and select the Hierarchy (and optionally the Entity for the *Starting Point*) from the P2 Server Browser.

iii. The selected hierarchy and starting point (if selected) appear in the **Hierarchy** and **Starting Point** edit boxes, respectively.

iv. Select a template, or *All Templates*, from the **Template** drop-down list.

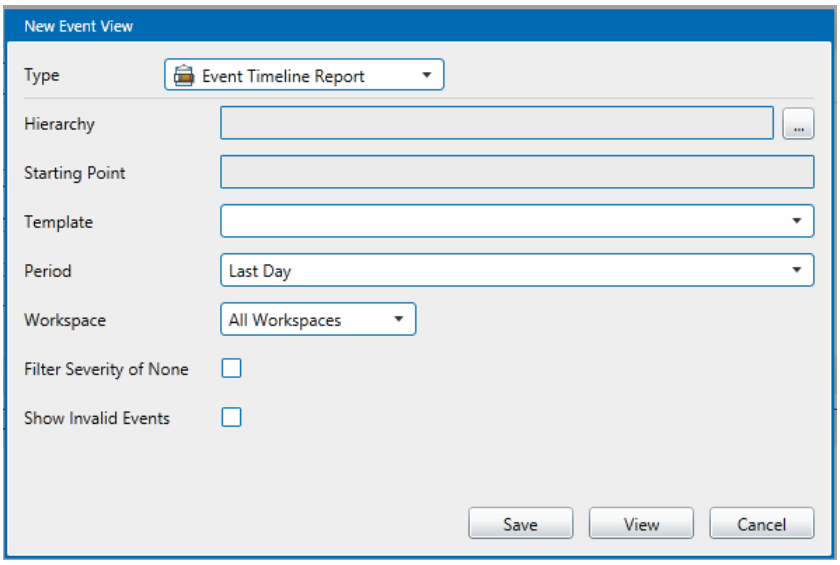
Note: Templates listed are those that use the selected entity within the selected hierarchy, from the starting point.

v. From the **Workspace** drop-down list, select which workspace (*This Workspace* or *All Workspaces*) on which to base the report.

vi. From the **History** drop-down list, select a period. Events that started within this period are shown in the report. For example, select *Week to Date Sunday* to show events that started in the current week (including Sunday).

– **To create an Event Timeline Report:**

i. From the **Type** drop-down list, select *Event Timeline Report*.



ii. Click the **P2 Server Browser** button next to the **Hierarchy** edit box, and select the Hierarchy (and optionally the Entity for the *Starting Point*) from the P2 Server Browser.

The selected hierarchy and starting point (if selected) appear in the **Hierarchy** edit box and the **Starting Point** edit box, respectively.

iii. Select a template, or *All Templates*, from the **Template** drop-down list.

Note: Templates listed are those that use the selected entity within the selected hierarchy, from the starting point.

iv. Select a *Period*, from the **Period** drop-down list. The period you select dictates the *start time* for the range of events displayed in the report, with current time being the *end time*. Periods to choose from are:

- Last Hour
- Last Day

- Last Week
- Last Month

v. From the **Workspace** drop-down list, select which workspace (*This Workspace* or *All Workspaces*) the report is based on.

vi. Select the **Filter Severity of None** check box, if you do not want events of severity **None** displayed in the event timeline.

vii. Select the **Show Invalid Events** check box, if you want invalid events to be included in the report.

Note: This option is only available if Case Management is enabled in Sentinel. An event is *Invalid* if its related case was rejected in P2 Explorer.

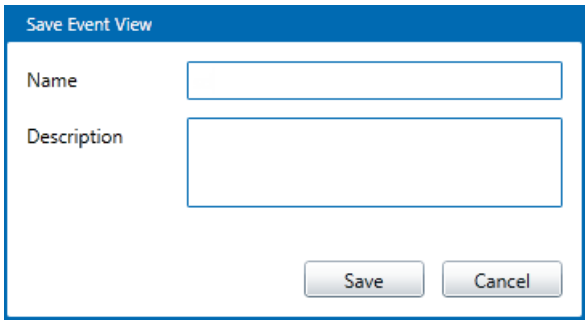
4. ***Save*** or ***view*** the new report.

Note: You cannot save changes to a report while viewing it from the **New Event View** window. If you want to save the report, save it first and view it later.

To Save the Report:

a. Click **Save**.

The **Save Event View** window appears.



b. In the **Name** edit box, type a name for the report.

c. In the **Description** edit box, type a description.

This is an optional description of the report, which appears when you hover the mouse over the report in the Workspace panel.

d. Click **Save**.

The new event view report is saved under the folder or workspace under which you created it.

To View the Report:

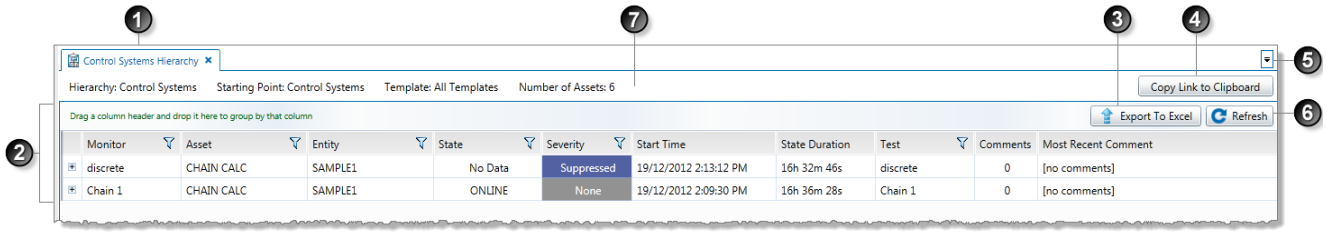
- Click **View.**

- For ***hierarchy*** reports: The report is displayed in a new **Hierarchy Report** tab in the Main panel.
- For ***event timeline*** reports: The report is displayed in a new **Event Timeline Report** tab in the Main panel.

- For ***event*** reports: The report is displayed in a new **Event Report** tab in the Main panel.
- For ***event history*** reports: The report is displayed in a new **Event History Report** tab in the Main panel.

Hierarchy Report

The hierarchy report resembles the view events tab. It contains a header section, with the report parameters, and an events grid.



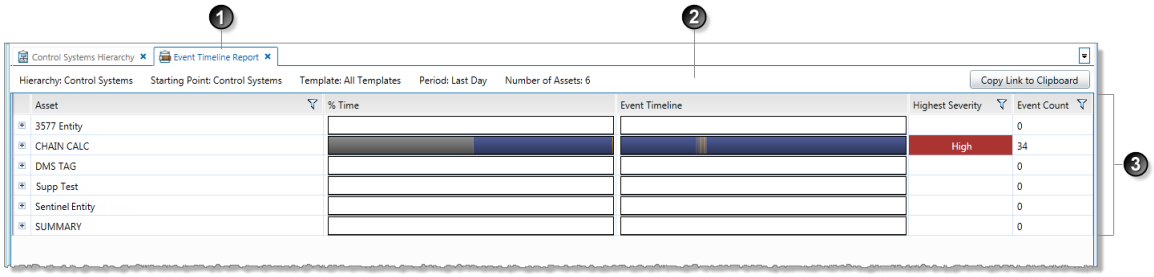
The *Hierarchy* report is made up of the following:

	Feature Name	Description
1	Hierarchy report title	The report name.
2	Events grid	All of the current events for the hierarchy report, displayed in an events grid.
3	Export to Excel	Click to export the grid to a Microsoft Excel spreadsheet.
4	Copy link to clipboard	Click to copy link to clipboard, as described in the next section.
5	Select an open tab	Click the downward-pointing arrow, and select an open tab from the drop-down list.
6	Refresh	Click to refresh the page. The latest events are shown.
7	Report parameters and properties	• **Hierarchy:** The hierarchy used for the report. • **Starting Point:** The hierarchy starting point. • **Template:** The selected report template, in which assets must exist to be part of the report. • **Number of Entities:** Number of entities found in the hierarchy.

- To close the tab, click the close icon next to the tab name.

Event Timeline Report

The Event Timeline report contains a header section and a report section.



The Hierarchy report is made up of the following:

	Feature Name	Description
1	Event Timeline report title	The report name.
2	Report parameters and properties	• **Hierarchy:** The hierarchy used for the report. • **Starting Point:** The hierarchy starting point. • **Template:** Assets must exist in the selected report template, to be included in the report. • **Period:** The period (hour, day, month) to report from. • **Number of Assets:** Number of assets found in the selected portion of the hierarchy, and also found in the selected template.
3	Report body	• **Asset:** A list of all assets (within the selected hierarchy, and existing in the selected template) that have events in the reporting period. Hover over the asset name, and click the asset icon that appears, to view the asset report. To expand the asset, click the expand button to the left of the asset name. This expands the report to show detail for the asset, as described in the next section. • **% Time:** A horizontal bar graph displays the total percentage of time that events of each severity occurred over the reporting period. • **Event Timeline:** This displays a magnified view of the asset events that occurred within the reporting period. Move the report hairline to get an exact time for any point in the timeline. • **Highest Severity:** The highest severity, for this asset, within the reporting period. • **Event Count:** The number of events for this asset, within the reporting period.

To limit the report result set:

- Filter one or more of: the Asset list, the Highest Severity list, or the Event Count list.

To close the page:

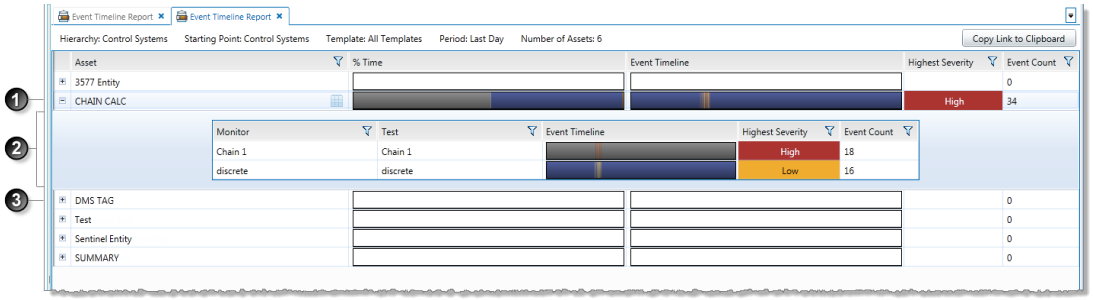
- Click the close icon next to the page name.

Note: Every time you open this report, the reporting period adjusts so that the end of the period is *current time*; the start of the reporting period is determined by the period parameter.

ASSET DETAIL

When you click on the expand button next to an asset, the report shows event details for every test that uses that particular asset, within the reporting parameters.

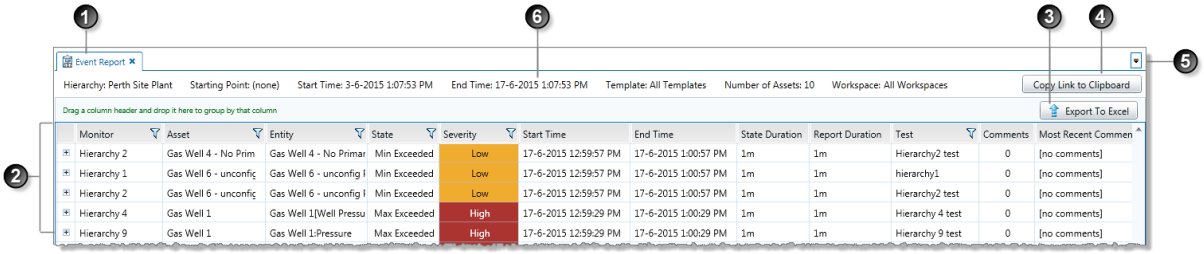
In this section of the report, the report body shows the monitor name and the test name for the expanded asset.



1. The expanded asset
2. Monitor and test detail for the expanded asset
3. The next asset in the report

Event Report

The event report resembles the view events tab. It contains a header section, with the report parameters, and an events grid.



The *Event Report* is made up of the following:

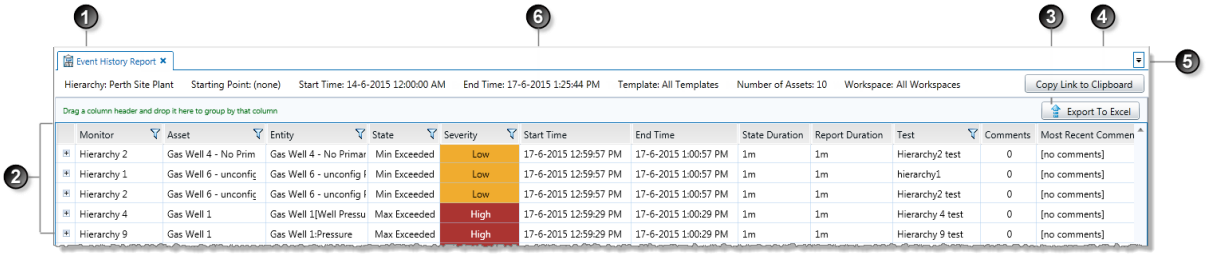
	Feature Name	Description
1	Event report title	The report name.
2	Events grid	All of the current events for the event report, displayed in an events grid. Also included is a column called Report Duration. This shows the duration from the start of the event to the end of the report time selection.
3	Export to Excel	Click to export the grid to a Microsoft Excel spreadsheet.
4	Copy link to clipboard	Click to copy link to clipboard, as described in the next section.
5	Select an open tab	Click the downward-pointing arrow, and select an open tab from the drop-down list.
6	Report parameters and properties	• **Hierarchy:** The hierarchy used for the report. • **Starting Point:** The hierarchy starting point. • **Start Time:** The selected report start time. • **End Time:** The selected report end time. • **Template:** The selected report template, in which assets must exist to be part

	Feature Name	Description
		of the report. • **Number of Assets:** Number of assets found in the hierarchy. • **Workspace:** The selected report template, in which assets must exist to be part of the report.

- To close the tab, click the close ✖ icon next to the tab name.

Event History Report

The event history report resembles the view events tab. It contains a header section, with the report parameters, and an events grid.



The *Hierarchy* report is made up of the following:

	Feature Name	Description
1	Event History report title	The report name.
2	Events grid	All of the current events for the event history report, displayed in an events grid. Also included is a column called Report Duration. This shows the duration from the start of the event to the end of the report time selection.
3	Export to Excel	Click to export the grid to a Microsoft Excel spreadsheet.
4	Copy link to clipboard	Click to copy link to clipboard, as described in the next section.
5	Select an open tab	Click the downward-pointing arrow, and select an open tab from the drop-down list.
6	Report parameters and properties	• **Hierarchy:** The hierarchy used for the report. • **Starting Point:** The hierarchy starting point. • **Template:** The selected report template, in which assets must exist to be part of the report. • **Number of Assets:** Number of assets found in the hierarchy. • **Workspace:** The selected report template, in which assets must exist to be part of the report.

- To close the tab, click the close ✖ icon next to the tab name.

Custom Event View URLs

An alternative to using the **Copy Link to Clipboard** function is to create a URL, using the applicable format.

There is URL command for the Hierarchy report, the Event Timeline report the Event Report and the Event History Report. All of the URLs use the **EventView.aspx** on the Sentinel Server.

Note: All parameters must be valid values from P2 Server, in order for report generation to work.

URL for a Hierarchy Event View

The following Event View URL applies to the Hierarchy Report:

```
https://[server name]/Sentinel/EventView.aspx?EventViewName=Hierarchy Report&Hierarchy=[hierarchy]&StartingPoint=[starting point]&Template=[template name]&WorkspaceFilter=[workspace name]&Private=[Private]
```

The first section of the URL is always:

`https://[server name]/Sentinel/EventView.aspx?EventViewName=Hierarchy Report` where [server name] is the name of the Sentinel Server.

EventViewName
Hierarchy Report

The remaining portion of the URL lists the parameters as follows:

```
&Hierarchy=[hierarchy]&StartingPoint=[starting point]&Template=[template name]
```

Hierarchy
The name of the hierarchy, for example "Well 1".

StartingPoint
The starting point of the hierarchy. This an entity within the hierarchy (for example, "Tubing Head Pressure").
Where the hierarchy is a *root* node, you can also use the hierarchy name, preceded by the symbols "^^^", to incorporate the complete hierarchy from the root node. For example: "^^^Well 1".

Template
Assets must exist within the template in order to be part of the report. For example, "WATER INJECTION WELL". To clear this filter, you can use "All Templates".

WorkspaceFilter
Events must be generated by monitors that exist within the workspace. To clear this filter, you can use "All workspaces".

Note: The *WorkspaceFilter* parameter is case sensitive.

Private
If set to true, users will only see events from monitors existing in their own private workspace, called **My Workspace**. Valid values are:

- True
- False

Using the example values, the final URL looks like this (using a server name of myServer):

```
https://myServer/Sentinel/EventView.aspx?EventViewName=Hierarchy
Report&Hierarchy=Well 1&StartingPoint=Tubing Head Pressure&Template=WATER
INJECTION WELL&WorkspaceFilter=All Workspaces
```

Note: When constructing the URL, ensure that the first parameter is preceded by the question mark (?) symbol. Subsequent parameters must be preceded by the ampersand (&) symbol.

URL for an Event Timeline Event View

The following Event View URL applies to the Event Timeline report.

```
https://[server name]/Sentinel/EventView.aspx?EventViewName= Event Timeline
Report&Hierarchy=[hierarchy]&StartingPoint=[starting point]
&Template=[template name]&Period=[Period]
&FilterSeverityOfNone=[FilterSeverityOfNone]&WorkspaceFilter=
[doc workspace]&Private=[Private]
```

The first section of the URL is always:

```
https://[server name]/Sentinel/EventView.aspx?EventViewName=Event Timeline Report
```

where [server name] is the name of the Sentinel Server.

EventViewName

Event Timeline Report

The remaining parameters are defined as follows:

Hierarchy

The name of the hierarchy, for example "Well 1".

StartingPoint

The starting point of the hierarchy. This an entity within the hierarchy (for example, "Well 1"). Where the hierarchy is a *root* node, you can also use the hierarchy name, preceded by the symbols "^^^", to incorporate the complete hierarchy from the root node. For example: "^^^Well 1".

Template

Assets must exist within the template in order to be part of the report. For example, "WATER INJECTION WELL". To limit this restriction, you can use "All Templates".

Period

The period selected dictates the start time for the range of events displayed in the report. Valid periods are:

- Last Hour
- Last Day
- Last Week

FilterSeverityOfNone

Filter events of no severity in the event timeline. Valid values are:

- True
- False

WorkspaceFilter

Events must be generated by monitors that exist within the workspace. To limit this restriction, you can use "All workspaces".

Private

If set to true, users will only see events from monitors existing in their own private workspace, called **My Workspace**. Valid values are:

- True
- False

Using example values, the final URL will look like this (using a server named myServer):

```
https://myServer/Sentinel/EventView.aspx?EventViewName=Event Timeline
Report&Hierarchy=Well 1&StartingPoint=Tubing Head Pressure
&Template=All Templates&Period=Last Hour&FilterSeverityOfNone=False
&WorkspaceFilter=All Workspaces&Private=False
```

or like this:

```
https://myServer/Sentinel/EventView.aspx?EventViewName=Event Timeline
Report&Hierarchy=Well 1&StartingPoint=^^^Well 1&Template=All Templates&Period=Last
Hour&FilterSeverityOfNone=False&Private=False
```

Note: When constructing the URL, ensure that the first parameter is preceded by the question mark (?) symbol. Subsequent parameters must be preceded by the ampersand (&) symbol.

URL for an Event Report

The following Event View URL applies to the Event Report:

Error! Hyperlink reference not valid. time]

The first section of the URL is always:

`https://[server name]/Sentinel/EventView.aspx?EventViewName=Event Report` where [server name] is the name of the Sentinel Server.

The event view name parameter is 'Event Report'.

EventViewName

Event Report

The remaining parameters are defined as follows:

Hierarchy

The name of the hierarchy, for example "Well 1".

StartingPoint

The starting point of the hierarchy. This an entity within the hierarchy (for example, "Well 1"). Where the hierarchy is a *root* node, you can also use the hierarchy name, preceded by the symbols "^^^", to incorporate the complete hierarchy from the root node. For example: "^^^Well 1".

Template

Assets must exist within the template in order to be part of the report. For example, "WATER

WorkspaceFilter

Events must be generated by monitors that exist within the workspace. To limit this restriction, you can use "All workspaces".

StartTime

Report start time measured in seconds since 1970 (UTC). Example: 635983556579240000

EndTime

Report end time measured in seconds since 1970 (UTC). Example: 635984420579246888

Using example values, the final URL will look like this (using a server named myServer):

```
https://myServer/Sentinel/EventView.aspx?EventViewName=Event%20Report&Hierarchy=P2%20Corporate&StartingPoint=P2%20Energy%20Solutions&Template=Oil%20Producing%20Well&WorkspaceFilter=All%20Workspaces&Private=False&StartTime=635978382120436961&EndTime=635984430120436961
```

Note: When constructing the URL, ensure that the first parameter is preceded by the question mark (?) symbol. Subsequent parameters must be preceded by the ampersand (&) symbol.

URL for an Event History Report

The following Event View URL applies to the Event History Report.

```
https://[server name]/Sentinel/EventView.aspx?EventViewName= Event History Report&Hierarchy=[hierarchy]&StartingPoint=[starting point]
&Template=[template name]&Period=[Period]
&FilterSeverityOfNone=[FilterSeverityOfNone]&WorkspaceFilter=
[doc workspace]&Private=[Private]
```

The first section of the URL is always:

```
https://[server name]/Sentinel/EventView.aspx?EventViewName=Event History Report
```

where [server name] is the name of the Sentinel Server.

EventViewName

Event Timeline History Report

The remaining parameters are defined as follows:

Hierarchy

The name of the hierarchy, for example "Well 1".

StartingPoint

The starting point of the hierarchy. This an entity within the hierarchy (for example, "Well 1"). Where the hierarchy is a *root* node, you can also use the hierarchy name, preceded by the symbols "^^^", to incorporate the complete hierarchy from the root node. For example: "^^^Well 1".

Template

Assets must exist within the template in order to be part of the report. For example, "WATER INJECTION WELL". To limit this restriction, you can use "All Templates".

WorkspaceFilter

Events must be generated by monitors that exist within the workspace. To limit this restriction, you can use "All workspaces".

Private

If set to true, users will only see events from monitors existing in their own private workspace, called **My Workspace**. Valid values are:

- True
- False

History

The **History** dictates the period for which events are shown.
Valid values for *History* are:

- Week To Date Sunday
- Week To Date Monday
- Last Week Sunday
- Last Week Monday
- Month To Date
- Last Month
- Year To Date
- Last Year

Using example values, the final URL will look like this (using a server named myServer):

```
https://myServer/Sentinel/EventView.aspx?EventViewName=Event%20History%20Report&Hierarchy=P2%20Corporate&StartingPoint=P2%20Energy%20Solutions&Template=Oil%20Producing%20Well&WorkspaceFilter=All%20Workspaces&Private=False&History=Week%20To%20Date%20Sunday
```

Note: When constructing the URL, ensure that the first parameter is preceded by the question mark (?) symbol. Subsequent parameters must be preceded by the ampersand (&) symbol. Use `%20` for spaces between words.

Viewing an Event View Report

To view an event view report:

1. In the Workspace panel, within a workspace or folder, locate the event view (hierarchy report, event report or event history report or event timeline report) that you want to view.
2. Right-click on the event view, and select **View** from the list, or double-click the event view.
   - For hierarchy reports, the report is displayed in a **Hierarchy Report** page in the Main panel.
   - For event timeline reports, the report is displayed in an **Event Timeline Report** page, in the Main panel.
   - For event reports, the report is displayed in an **Event Report** page, in the Main panel.
   - For event history reports, the report is displayed in an **Event History Report** page, in the Main panel.

Editing an Event View Report

To edit an event view report:

1. In the Workspace panel, within a workspace or folder, locate the event view (hierarchy report, event report or event history report or event timeline report) that you want to edit.
2. Right-click on the report.
3. Select **Edit** from the list.

The **Edit Event View** window appears in the Main panel.

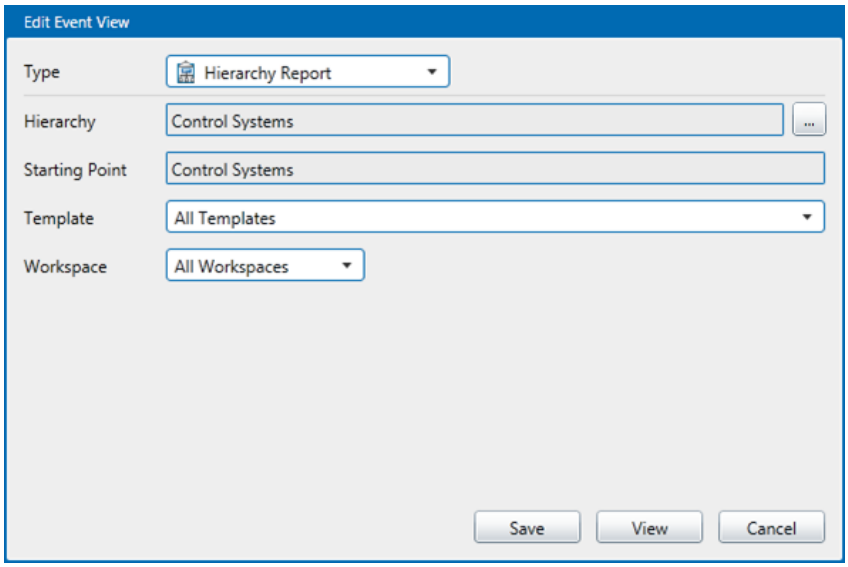


Figure 10: Edit Event View window, for a Hierarchy Report

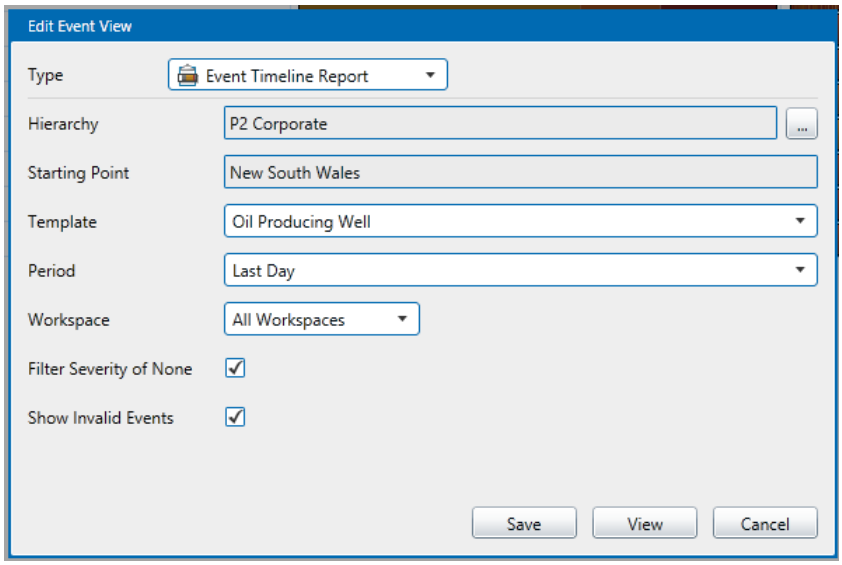


Figure 11: Edit Event View window, for an Event Timeline Report

4. Edit the report.

– **To update the report type:**

- Select another report type from the **Type** drop-down list.

The screen changes according to the new type selected; see **Figure 10** and **Figure 11** (above) for the different screen layouts.

– **To update the Hierarchy and Starting Point**:

i. Click the **P2 Server Browser** button next to the **Hierarchy** edit box.

ii. Select the Hierarchy for the **Hierarchy** edit box, and the Entity for the **Starting Point** box from the P2 Server Hierarchy Picker.

- To update the template, select a *Template* from the **Template** drop-down list.
- To change the period (this applies to *event timeline* reports only), select another *Period* from the **Period** drop-down list.
- To change the workspace, select *All Workspaces* or *This Workspace* from the **Workspace** drop-down list.
- To show or hide events with a severity of *None*, select or deselect the **Filter Severity of None** check box (this applies to *Event Timeline* reports only).

5. ***Save*** or ***View*** the changes.

Note: You cannot save changes to a report while viewing it from the **Edit Event View** window. If you want to save the report, save it first then view it later.

To Save the Report:

a. Click **Save**.

The **Save Event View** window appears.

- To change the report name, type a new name in the **Name** edit box.
- To change the report description, type a new description in the **Description** edit box.

b. Click **Save** again.

The **Save Event View** and the **Edit Event View** windows close, and the event view report is saved with changes.

To View the Report:

- Click **View.**

- For ***hierarchy*** reports: The edited report is displayed in a new **Hierarchy Report** page, in the Main panel.
- For ***event*** reports: The edited report is displayed in a new **Event Report** page, in the Main panel.
- For ***event history*** reports: The edited report is displayed in a new **Event History Report** page, in the Main panel.
- For ***event timeline*** reports: The edited report is displayed in a new **Event Timeline Report** page, in the Main panel.

Deleting an Event View Report

To delete an event view report:

1. In the Workspace panel, within a workspace or folder, locate the event view (hierarchy report or event timeline report) that you want to delete.
2. Right-click on the report.
3. Select **Delete** from the list.
4. Click **Yes** at the **Delete event view** prompt.

The event view report is deleted.

Moving an Event View Report

You may move an event view report to a different workspace, or to another folder.

1. In the Workspace panel, locate the event view (hierarchy, event, event history  report or event timeline  report) that you want to move.
2. Drag the custom event view report to the destination workspace or folder.

   Tip: The destination workspace or folder is displayed when the report is correctly positioned.
3. Release the mouse button.

The event view report is moved to the destination workspace or folder.

Note: For event views where the workspace is defined as *This Workspace*, the report will only include events relating to monitors that belong to the destination workspace.

Viewing Asset Reports

Every asset in the event page, or event timeline report, has the following reports and tables:

- Timeline
- Event Log
- Statistics
- Chart

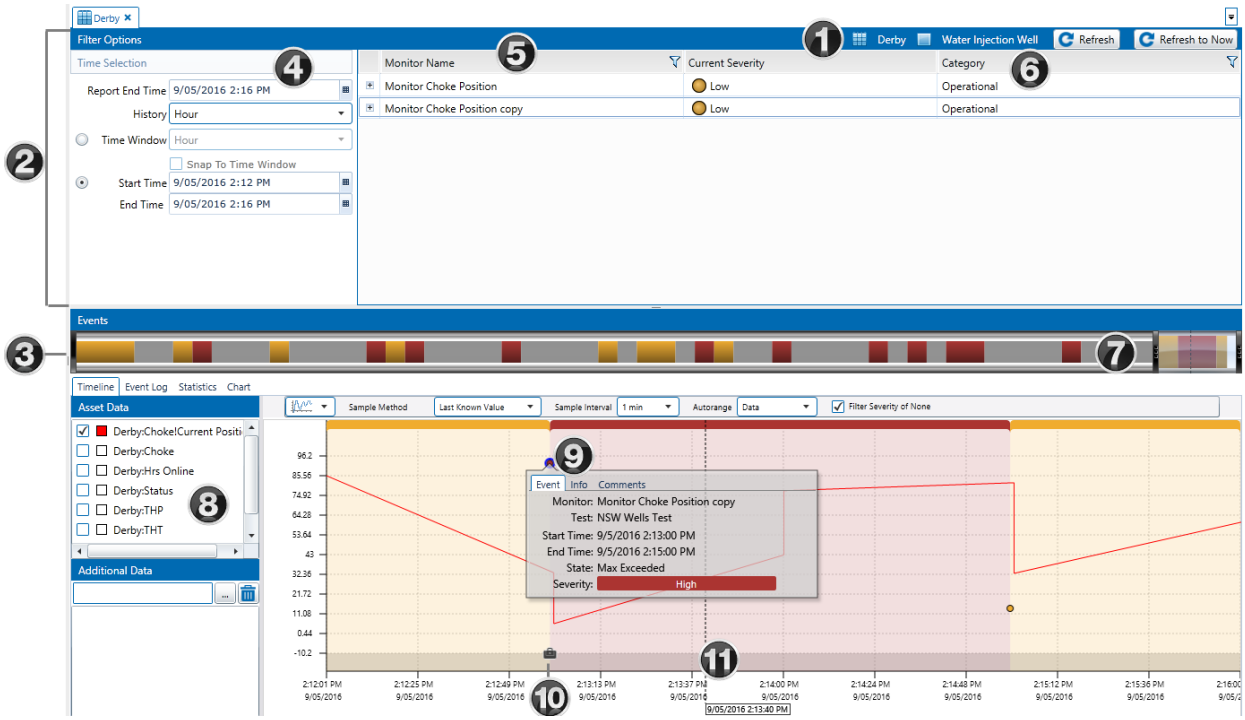
To view the reports for any asset:

1. Open the events page or an event timeline report.
2. In the events grid, locate the asset whose reports you want to view.
3. Hover the mouse over the asset.
4. Click the **View Asset Report** icon that appears.

   A new page opens in the main panel. The page title consists of the asset icon, the asset name and the primary template name.

Note: You can also view an asset report using a Sentinel Asset Report URL.

The important features of the Asset page are numbered in the screenshot below:



	Feature name	What it's useful for
1	Asset Report header	The Asset report header frames the page, and contains the asset name, as well as the primary template name. There is a refresh button on the far right. Click **Refresh** for the latest event information.
2	Filter Options pane	The Filter Options section allows you to refine what is displayed in the Events pane. It includes the Time Selection, Category, and Monitor Name overview (see below for details).

	Feature name	What it's useful for
3	Events	A summary representation of the report events, for the **History** period. Each colour band represents a change in the maximum severity of all events (within the filtered group) over that portion of time.
4	Time selection	The Time Selection panel allows you to specify the time period on which you want to report.
5	Monitor Name	The Monitor Name lists the monitors that have the **asset** as a monitor item. You can filter the monitors to limit them in the report.
6	Category	The Category panel displays the categories to which the monitors belong. You can filter the categories to limit the number displayed. Categories are defined in the monitor details panel of a monitor.
7	Time slider	Allows you to change the start time and end time for the events to be displayed in the report. The slider, which spans the time range specified in the **Start Time** and **End Time** in the **Time Selection Panel**, provides a visual clue for you to detect where the events of most interest occur. Hover the mouse over the time slider to see a hairline. The hairline matches the hairline in the Event Timeline.
8	Reports Pane	The Events pane contains the details of the event reports, and allows you to choose from four types of reports or logs: • **Timeline** • **Event Log** • **Statistics** • **Chart**
9	The **Event, Info and Comment** screen	The details for the selected event are shown when the report opens.
10	**Case icon**	Click on the icon to see the case details.
11	Report Hairline Date/Time Label	The exact date and time on the graph at the point of the hairline. Click and drag the report hairline to zoom in and further refine what is shown on the graph.

Time Selection

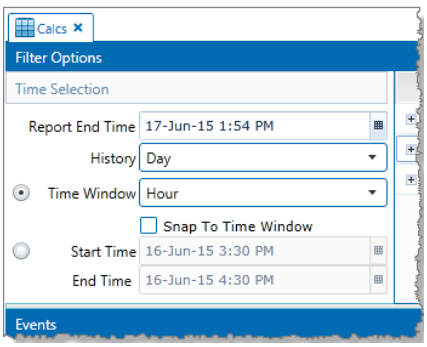
The **Time Selection** panel on the Asset Report allows you to specify the time period on which you want to report.

Note: Large periods of over a month may considerably slow down the report generation.

You can define the following options:

Report End Time

The report only displays data up to the selected report end time. Report End Time defaults to current time.



History

The history limits the amount of data displayed in the report. You can choose to display data for the past hour, day, week, month, 3 months, 6 months, year, or 2 years.

Time Window

You can specify the report to display events within a

defined time window. Depending on the *History* selected, you can choose from day, shift, week, month, 30 days, or year.

The **Snap to Time Window** check box controls the **Start Time** and **End Time**, and the time slider. The end time is always the current time, and the start time is one time window period in the past. For example, if the **time window** is set to an hour, the end time is set to current time, and the start time is set to one hour ago.

Start Time and End Time

You can choose to display events with a specific start and end time, instead of specifying a time window.

Dates are displayed in DD/MM/YYYY format (by default), and you can click the calendar ▦ button to select the date from a calendar.

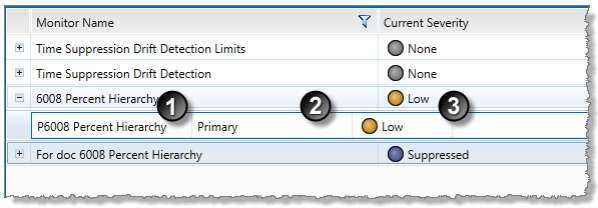
Times are displayed in HH:MM AM/PM format (by default), and you can select half-hour intervals from the drop-down list, or type the time directly into the field.

The start time and end time provide a manual way of setting the time slider.

Note: The date and time formats can be changed in the P2 Sentinel configuration file. Refer to "**Update the P2 Sentinel Configuration File**" in the *P2 Sentinel Installation and Administration Guide*.

Monitors in the Asset Report

The **Monitor Name** pane in the asset report lists a group of monitors. To be listed, a monitor must contain a test that has an entity of the report asset as a monitor item, where that entity has caused an event.



Monitor List

The full list of monitors in the asset report.

Monitor Name

The monitor name.

Current Severity

The current highest severity of the monitor; this is the highest severity reached by any test within the monitor.

Any of the rows in the monitor name grid can be expanded, to show the tests within the monitor that use an entity of the asset.

- In the grid, click the expand button to the left of the monitor name.

Test Details

Tests that use an entity of the asset are listed beneath the monitor name, displaying the following features:

1 **Test Name**: The name of the test containing the entity that uses the asset as a process input.

2 **State**: The current state of the entity for the asset in this test.

3 **Severity**: The severity of the event.

Note: The symbol current severity of an event is black if the event is not current.

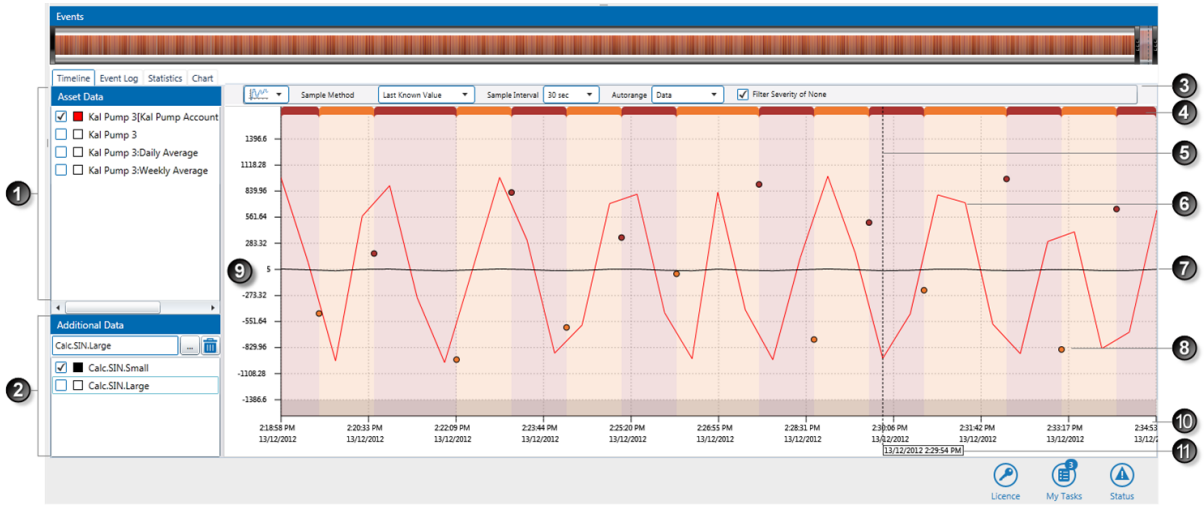
View Timeline

The **Timeline** report shows a timeline for the events raised against the entities of the reported asset.

In the Asset Report, you can filter the events using Time Selection, Category, and Monitor Name.

The report asset events are limited by the filtering options. You can further limit the report asset events by adjusting the time slider. The time slider works with the time selection.

- Click the **Timeline** tab in the Events pane to view the Timeline.
- Use the **time slider** and other controls to refine what is shown on the graph.
- Click and drag the **report hairline** to zoom in and further refine what is shown on the graph.



The timeline report shows the event data for the asset, over a period of time. Events are displayed on the graph as circles, each one rendered in its severity colour.

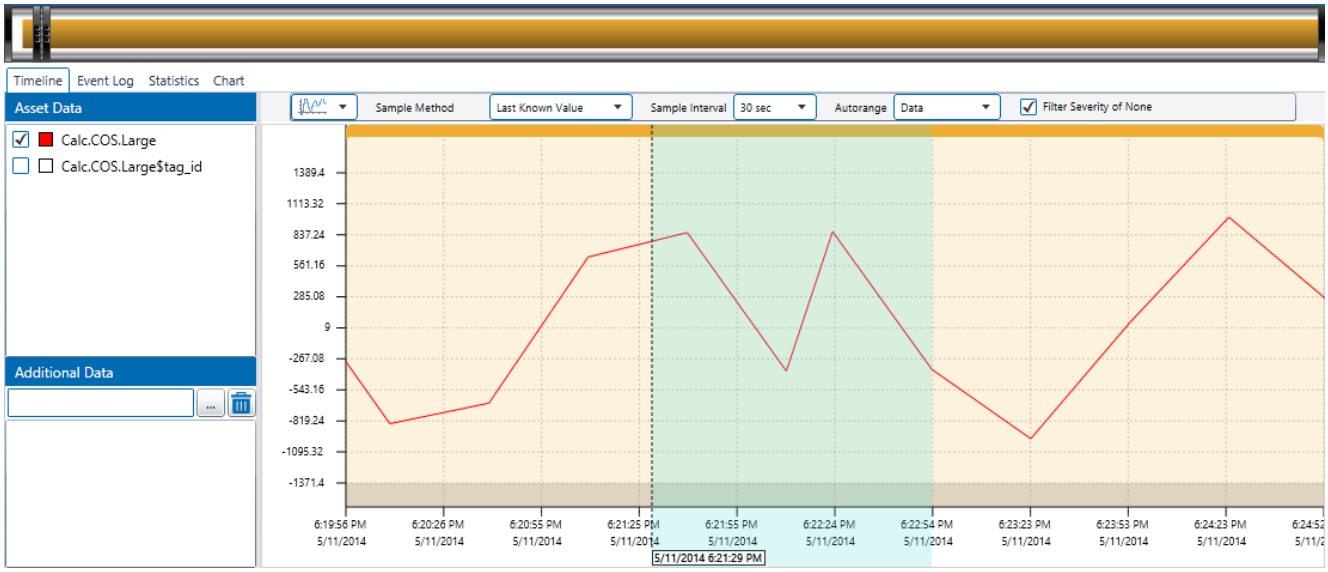
In addition to the events, the asset data can also be displayed on the graph.

The important features of the Timeline Report are:

	Feature name	Applies to:	What it's useful for
1	Asset Data	Asset Data	The test process input entity is automatically selected here. For attributes: all other attributes of the source entity asset, as well as the source asset itself, can be selected here. Select the check box for the entity or attribute. A colour is assigned and displayed in the corresponding colour key box ■. Asset data is for the primary template attributes, as well as any secondary template attributes. For primary template attributes, the template is implicit in the asset name, for example: **Derby:Oil Production** (the primary template [Production] is not included in the name here). For secondary template attributes it is explicit, for example: **Derby[Water Injection Well]:Choke**, where [Water Injection Well] is a secondary template. If the asset is a tag, this is displayed here. Note that you cannot select data that is based on a calculation.
2	Additional Data	All Data on the Graph	Select any additional data (irrespective of the Asset Data in this report) using the P2 Server Browser. Add tags, attributes or

	Feature name	Applies to:	What it's useful for
			attribute values, as shown in the following section. A colour is assigned and displayed on the graph in the colour of the corresponding colour key box .
3	Report Presentation	Asset Data	• **Graph Type:** Select a data representation icon from the drop-down list. Select the continuous data representation icon to view continuous data, or the discrete data representation icon to view discrete data. • **Sample Method:** Select Raw, Linear Interpolate, Average or Last Known Value data from this drop-down list. • **Sample Interval:** Select the regular interval to collect sample data from the source. At every sample interval, the collected data is prepared according to the sample method used. • **Autorange:** Select **Events** from the drop-down list to set the graph range to best represent the event data. Select **Data** to set the graph range to best represent the asset data. The third option is **None**: this provides a standard range of 0 through 10,000. • **Filter Severity of None**: Select this check box to filter the events so that those of severity **None** are not displayed.
4	Event Severity	Event Data	This is a linear representation of event severity and duration over the full timeline of the graph. The colouring represents the severity, and the width of each portion represents the duration. **Note:** this is the maximum severity over the period.
5	Report Hairline	All Data on the Graph	Move the report hairline to get an exact time for any point in the timeline. To zoom in to a segment of the period, click and drag the hairline.
6	Asset Data Plot	Asset Data	Entities, attributes, or attribute values that are selected in the Asset Data and Additional Data selection are plotted on the graph, in their respective colours (as shown in the colour keys).
7	Additional Data Plot	All Data on the Graph	Selected assets from the additional data list are plotted on the graph, in their respective colours (as shown in the colour keys).
8	Event	Event Data	Every event within the selected report period is displayed on the graph. Click an event icon to view event details, view event information, and add or view comments, as described in the Timeline Events section.
9	Value Axis	All Data on the Graph	These mark the different values reached by event data and asset data. The range is automatically generated, to cover the full scope of either event data or asset data, depending on which auto-range (see notes above) is selected.
10	Time Axis	All Data on the Graph	The timeline, for the full duration of the report period, divided into the time intervals specified in Sample Interval.
11	Report Hairline Date and Time Label	All Data on the Graph	The exact date and time on the graph at the point of the hairline.

When you **click and drag** a hairline and then **release**, you can zoom in on a specific section of the graph to view more detail, as shown below. To zoom out again, click **Refresh** or **Refresh to Now** on the tab header bar.

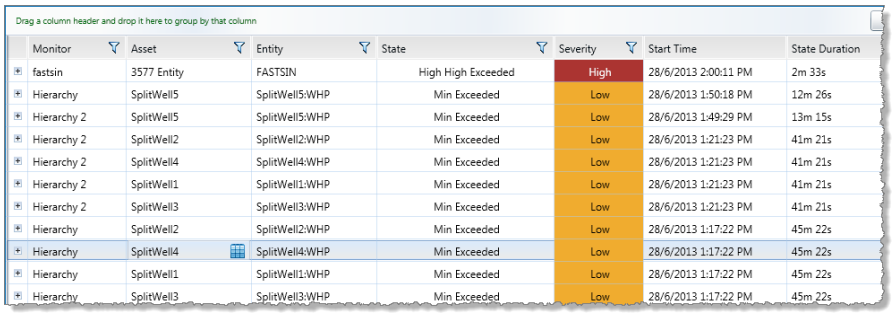


Rotate the mouse wheel to scroll over a trend. This moves the time slider. Scroll down to move the time slider backwards, and up to move the time slider forwards.

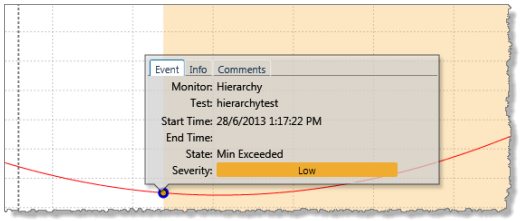
Opening a Timeline for an Event

In the events grid, every time you click the **View Asset Report** icon, a new asset report opens for the event. This report focuses on the event you have selected, with the **Event, Info and Comment** screen already open for that event.

For example, if you click on the *view asset report* icon for the selected row:



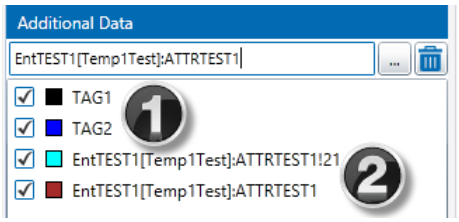
The **Event, Info and Comment** screen appears in the timeline report for this event:



Adding Additional Data

As well as the event data, you can add additional, non-related data. This can be tags, attributes, or attribute values.

1. Tags
2. Attribute and attribute value

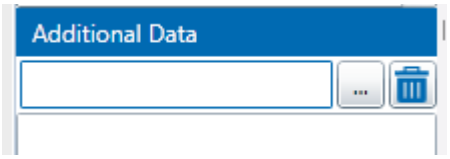


ADDING A TAG

1. In the **Additional Data** panel, type a valid **Tag Name** in the edit box.

   or

   Click the *ellipsis* button next to the edit box and select a **Tag** from the P2 Server Browser (see Selecting Tags or Entities).



2. Click in the **Additional Data** text box, and press **Enter**.

   The tag is added to the list of additional data.

3. Select the check box to the left of the item, to plot it on the graph, or clear the check box to remove it from the graph.

ADDING AN ATTRIBUTE OR ATTRIBUTE VALUE

1. Select an attribute or attribute value.

   a. In the **Additional Data** panel, type a valid **Entity Name** in the edit box.

   b. Click the *ellipsis* button next to the edit box and select an attribute or attribute value from the P2 Server Attribute Picker (see P2 Server Attribute Picker).

   or

   a. Click the *ellipsis* button next to the edit box and select an **Entity** from the P2 Server Browser (see Selecting Tags or Entities).

   The P2 Server Attribute Picker opens for the selected entity.

   b. Select an attribute or attribute value from the P2 Server Attribute Picker (see P2 Server Attribute Picker)

2. Click in the **Additional Data** text box, and press **Enter**.

   The attribute or attribute value is added to the list of additional data.

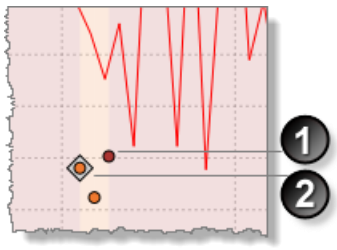
3. Select the check box to the left of the item, to plot it on the graph, or clear the check box to remove it from the graph.

Note: To remove additional data from the graph, click on the item in the list and click the *remove* button.

Timeline Events

The different events on the Timeline graph are each represented as a circle coloured in the correlating event severity colour. Events that have comments are depicted with a small diamond background.

For example:



1. An event with a High Severity (Red).
2. An event with a Medium Severity (Orange). The event contains comments, as depicted by the diamond-shaped background icon.

Note: Asset lines for events with a confidence lower than 100 appear faded; the lower the confidence, the more faded the asset line appears.

To view timeline event details, information and comments, or to add event comments:

- Click on an event in the graph.

A small event screen is displayed, with three tabs: the **Event** tab, the **Info** tab, and the **Comments** tab.

Event tab

This tab displays general information relating to the event.

Monitor
The name of a monitor containing the test that raised this event.

Test
The test that raised this event.

Start Time
The date and time (to the second) that the event began.

End Time
The date and time (to the second) that the event ended.

State
The state that was reached to cause the event.

Severity
The state severity.

Info tab

This tab shows the state of the test entity at the time that the event was reached. Use the scroll bar located on the right to see the full list.

Original State
The state that the test entity reached to cause the event. This row is only shown if there is a state override in the state configuration of the test.

Value
The value of the test entity.

Confidence
The confidence value of the test entity.

Limit Values
The values of the different process limits as set up in the test.

Depending on the process used, these could be any of the following:

High Limit
The value of high limit at the time of the event.

High High Limit
The value of high high limit at the time of the event.

Min
The value of min at the time of the event.

Max
The value of max at the time of the event.

And so on. The value may be a fixed value, or a P2 Server entity or attribute value, depending on how the limits are defined in the test process.

Auxiliary Data
If there is auxiliary data for the test, this appears in the Info tab.

[Event Metadata Key 1]
Auxiliary Data (1) value

[Event Metadata Key 2]
Auxiliary Data (2) value

Etc.

State Reason
If the state configuration for this event's state has a *State Reason*, this is saved with the event and displayed here.

Potential impact
If the state configuration for this event's state has a *Potential Impact*, this is saved with the event and displayed here.

Recommended Action
If the state configuration for this event's state has a *Recommended Action*, this is saved with the event and displayed here.

Comments tab

This is a list of all comments that have been added for this event. The most recent comment is at the top of the list. Use the scroll bar located on the right, to see the full list of comments.

Each comment has the following:

Date and time
The date and time that the comment was added.

User name
The user name of the user who added the comment.

Comment
The comment that was added.

To Add an Event Comment

In addition to any comments that already exist for this event, you can add new comments.

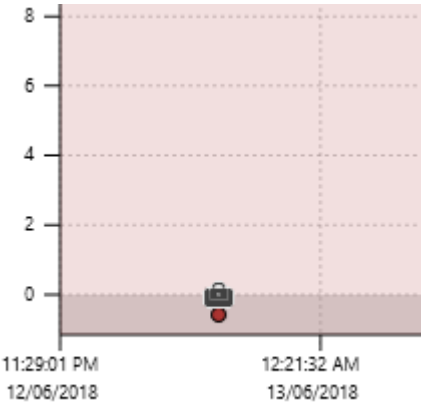
- Click on the comments tab, and add event comments.

To Close the Timeline Events Screen

- Click on any part of the graph to close the events screen.

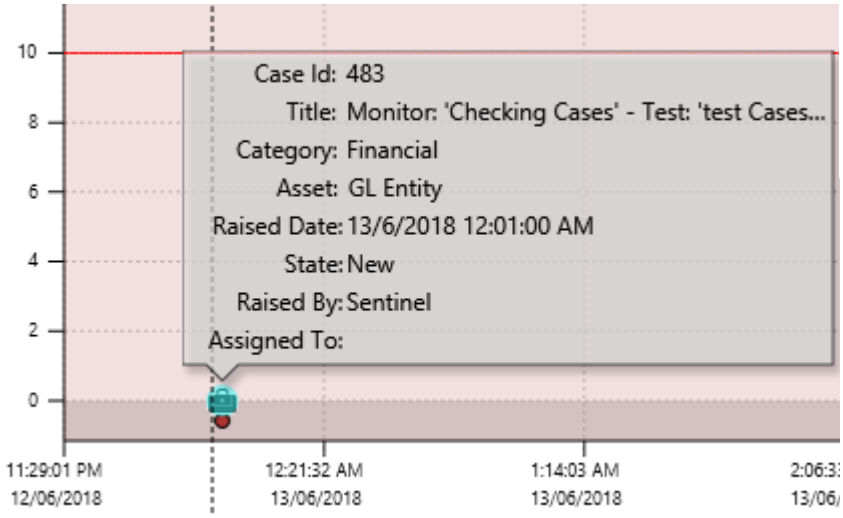
Cases on the Timeline

If Case Management is enabled, cases relating to events appear on the Event Timeline, on the X Axis directly below an event.



- To open the Case Info panel, click the case icon.

The Case Panel opens, showing the following Case Information.



Case Id

A unique number identifying the case.

Title

The case's title. This is defined in Sentinel, but can be edited in P2 Explorer.

Category

When a case is raised in Sentinel, it is allocated the same category as the monitor whose test outcome raised the case.

Asset

The asset is the subject of a case. This matches the subject of the current asset report.

Raised Date

The same date and time that the event was raised.

State

This refers to the case's status. When a case is raised, its status is **New**. Cases are manually progressed through various statuses in P2 Explorer. Possible statuses are New, Investigating, Confirmed, Closed, and Rejected, and Deprecated.

Raised By

The system that raised the case. For Sentinel cases, this is the display name of the Sentinel Super User.

Assigned To

When a case is raised, it is unassigned.

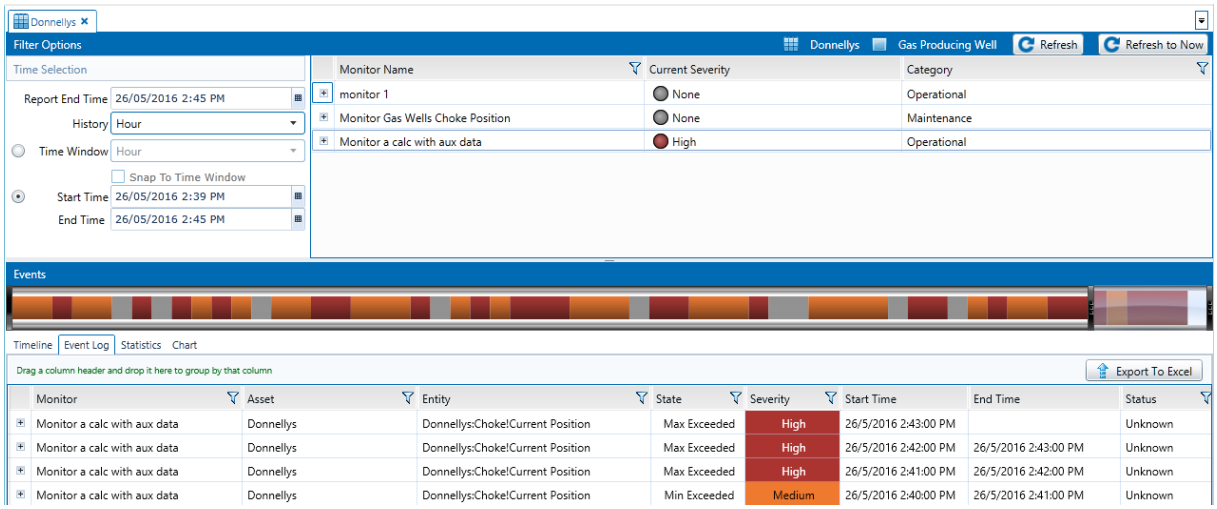
View Event Log

The Event Log shows a detailed history for the events raised against the entities of the reported asset.

In the Asset Report, you can filter the events using Time Selection, Category, and Monitor Name.

The report asset events are limited by the filtering options. You can further limit the report asset events by adjusting the time slider. The time slider works with the time selection.

- Click the **Event Log** tab in the Events pane to view the Event Log.



The events grid, when viewed from the event log report, displays the history of events for the report selection. This report can be viewed in the same way as the Events page events. The only difference is that the event log shows **past** events; thus each event has an end time (except for the current event).

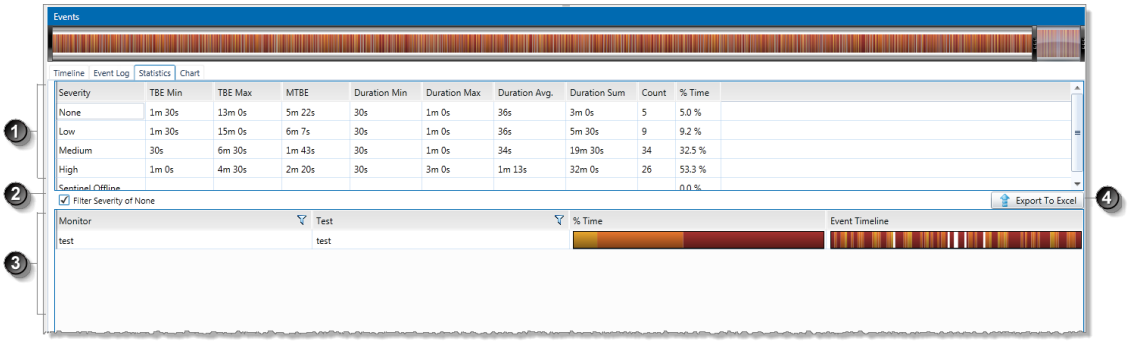
View Statistics

The Statistics Report displays detailed information and statistics for the events raised against the entities of the reported asset.

In the Asset Report, you can filter the events using Time Selection, Category, and Monitor Name.

The report asset events are limited by the filtering options. You can further limit the report asset events by adjusting the time slider. The time slider works with the time selection.

- Click the **Statistics** tab in the Events pane to view the Statistics report.



The important features of the Statistics Report are:

	Feature name	What it's useful for
1	Severity table	The severity table displays statistics for the severity of events that have occurred for the defined time period, and is based on the filter options. It displays the following statistics: • **TBE Min**: Minimum time between events of this severity • **TBE Max**: Maximum time between events of this severity • **MTBE**: Mean (average) time between events of this severity • **Duration Min**: Shortest duration of events of this severity • **Duration Max**: Longest duration of events of this severity • **Duration Avg**: Average duration of events of this severity • **Duration Sum**: Total duration of events of this severity • **Count**: The number of times events of this severity occurred • **% Time**: The percentage of time events of this severity occurred. Percentage is calculated within the time selected in the time slider. The table also displays the percentage of time that Sentinel was offline (not running).
2	Filter Severity of None	Selecting this check box filters events so that those of severity **None** are not displayed in the event timeline.
3	Time analysis	The time analysis section displays a magnified visual of the severity of events for the monitor tests during the specified time period. • **Monitor**: The monitor name • **Test**: A test within the monitor, that contains the asset being reported • **% Time**: A horizontal bar graph is a visual display of the total percentage of time that events of each severity occurred. • **Event Timeline**: This displays a magnified view of the events that occur within the specified time window. Move the report hairline to get an exact time for any point in the timeline.
4	Export button	The Export button allows you to export the severity table to an Excel file.

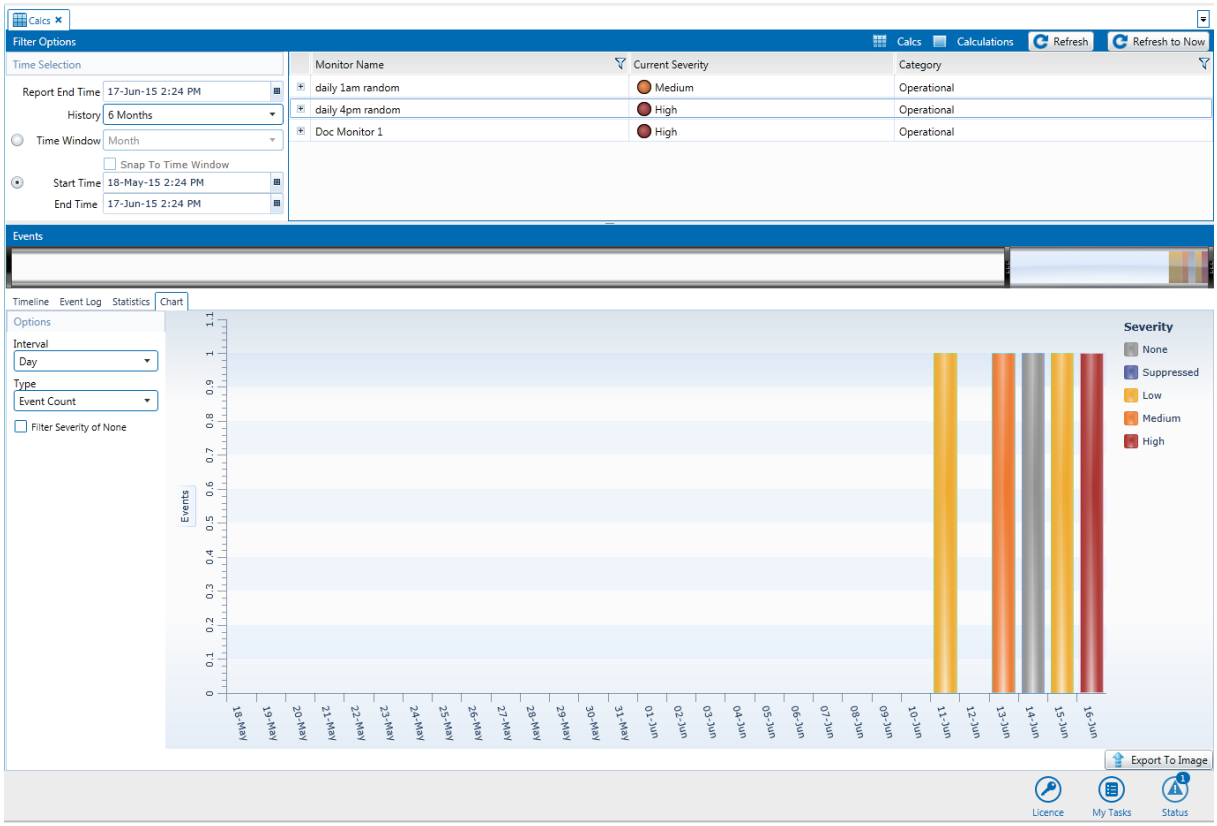
View Chart

The **Chart** report shows a chart for the events raised against the entities of the reported asset.

In the Asset Report, you can filter the events using Time Selection, Category, and Monitor Name.

The report asset events are limited by the filtering options. You can further limit the report asset events by adjusting the time slider. The time slider works with the time selection.

- Click the **Chart** tab in the Events pane to view the Chart report.



The Chart report displays a stacked bar graph showing the events of each severity type for the asset during the selected time window, with the colours of the stacked bar corresponding to the severity of the event.

You can manipulate the graph by changing the following:

Interval

The options available in the Interval drop-down list depend on the selected *time window*. This function offers the facility to change the sample interval (displayed on the x-axis) for increased granularity of results. Example intervals are *Hour* and *12 hours*.

Type

Change the way the graph displays the event severities. Note that the chart displays all the results for the asset. Therefore if the asset is monitored in several monitors then the result is multiplied by the number of monitors.

Event Count

The number of times the severity occurs for the asset during each time interval.

Event Time
The total amount of time the severity occurs for the asset during each time interval.

Filter Severity of None
Select this check box if you do not want to display severities of *None*.

Export To Image
The **Export To Image** button allows you to export the chart to an image file.

Sentinel Asset Report URLs

There is a URL command for the Asset Report, using the **AssetReport.aspx** page on the Sentinel Server.

URL for an Asset Report

The following URL applies to the Asset Report:

```
https://[server name]/Sentinel/AssetReport.aspx?Asset=[asset
name]&MonitorIds=[monitor
ids]&Private=[Private]&AddComment=[true/false]&ShowEventId=[EventId]
```

The first section of the URL is always:

`https://[server name]/Sentinel/AssetReport.aspx` where [server name] is the name of the Sentinel Server.

The remaining portion of the URL lists the parameters as follows:

```
?Asset=[assetname]&MonitorIds=[monitor ids]&Private=[Private]
```

Asset
The name of the asset to show events for, for example "Well 1".

Note: The asset parameter is case sensitive.

History
The history limits the amount of data displayed in the report. You can choose to display data for the past hour, day, week, month, 3 months, 6 months, year, or 2 years.

Use one of the following values:

- Hour
- Day
- Week
- Month
- 3 Months
- 6 Months
- Year
- 2 Years

Time
You can specify the report to display events within a defined time window. Depending on the *History* selected, you can choose from day, shift, week, month, 30 days, or year.

Use one of the following values:

- Hour
- Shift

- Day
- Week
- 30 Days
- Month
- 3 Months
- Year

Snap

Set to **True** or **False**

This controls the **Start Time** and **End Time**, and the time slider. The end time is always the current time, and the start time is one time window period in the past. For example, if the **time window** is set to an hour, the end time is set to current time, and the start time is set to one hour ago.

Use in conjunction with the **Time** parameter.

StartTime

You can choose to display events with a specific start and end time, instead of specifying a time window.

If you are using the StartTime parameter, you need to use the EndTime parameter as well.

The format is: **ddMMyyyyHHmmSS**

EndTime

You can choose to display events with a specific start and end time, instead of specifying a time window.

If you are using the EndTime parameter, you need to use the StartTime parameter as well.

The format is: **ddMMyyyyHHmmSS**

MonitorIds

(Optional) A semicolon-separated list of monitors to select when the report is opened; for example "1;2;3" will cause monitors with these ids to be selected, if present in the report.

Note: This optional parameter is used internally by Sentinel.

Private

(Optional) Set to **True** to include events from the user's private workspace (My Workspace). Otherwise, set to **False**.

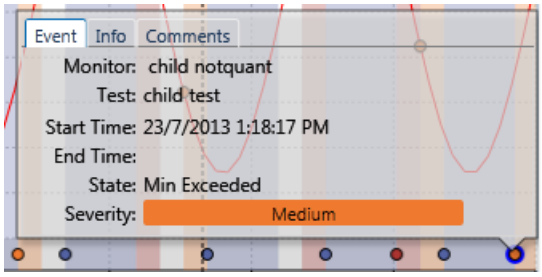
AddComment

(Optional) Set to **True** to open the **Event, Info and Comment** screen, with the cursor in the comment box, in the **Comments** tab, ready for you to add a new comment.

Note: This parameter works in conjunction with the *ShowEventId* parameter (described below). If this is not set, then the *AddComment* parameter will not work.

ShowEventId

(Optional) Set this parameter to an event id to open the **Event, Info and Comment** screen, for a particular event. The screen opens on the *Event* tab, unless you have set the AddComment parameter to **True**, in which case the screen opens on the *Comment* tab.



Note: The event id of an event can be returned as an action token (**Event Id**).

Using example values, the final URL looks like this (with a server name of myServer):

```
https://myServer/Sentinel/AssetReport.aspx?Asset=Well
1&MonitorIds=1;2;3&Private=False
```

Note: When constructing the URL, ensure that the first parameter is preceded by the question mark (?) symbol. Subsequent parameters must be preceded by the ampersand (&) symbol.

Viewing Monitor Status

The monitor status tab shows information on the current status of the monitor.

The monitor status can include any of the following:

- Started
- Stopped
- Waiting for trigger
- No approved version (The initial version of the monitor needs to be approved before it can be triggered. This only applies to installations that include Change Management.)
- Disabled
- Running
- Re-running
- Deleting Events

The monitor stops for the following reasons:

- Licence errors
- Engine errors
- Service errors
- Warnings

The P2 Sentinel configuration file specifies when the monitor stops due to any of these reasons. For example, a monitor stops after five warnings if this is specified in the configuration file.

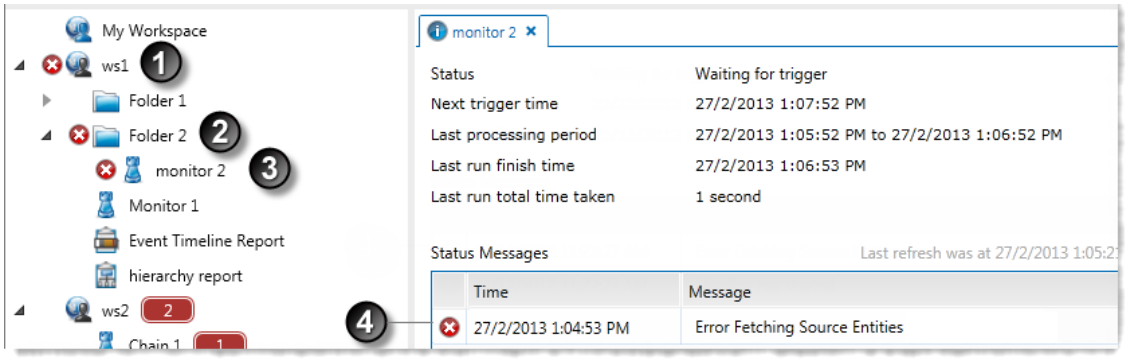
Status Message Types

There are four icons indicating the type of status message:

	Status Message Type	Example
	Information	Monitor has started.
	Warning	Error fetching data for entity.
	Engine Error	Error fetching source entities.
	Action Error	Error processing a Web Service Action. This could be due to the web service itself, or incorrect details entered in the URL and body section of the action.
	Licence Error	The licence for the process 'Alarm' has expired. Tests using this process will not run.

Where a monitor has an error or warning status, the monitor name is preceded by an error or warning icon. The folder and workspace names are also preceded by an error or warning icon. You can detect an error or warning status from a high level, and then find the monitor with that status, by navigating through the folders on the workspace. It is also helpful to know the P2 Sentinel status.

In this example the error is traced by following the error icon from the workstation to the folder to the monitor:



1. Workspace with error icon
2. Folder with error icon
3. Monitor with error icon
4. The monitor status message with error icon, on the monitor status page

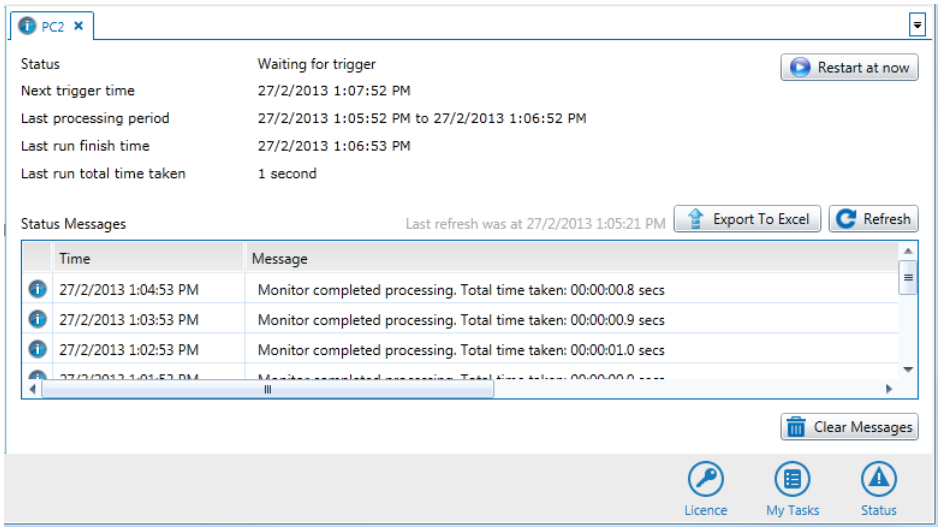
To view the monitor status:

1. In the Workspace panel, locate the monitor you are interested in.
   a. Right-click on the **monitor** .
   b. Click the **View Status** item.
2. Alternatively, for monitors with an error or warning status, click the error or warning icon.

   The Monitor Status page opens in the Main panel.

THE MONITOR STATUS PAGE

The page title consists of the relevant status icon and the monitor name.



The status page features are:

Status

The current monitor status. Possible values are:

- Started
- Stopped
- Waiting for trigger
- No approved version
- Disabled
- Re-Running
- Deleting events

Next trigger time

The next time that the monitor tests are triggered; there is no *next trigger time* for disabled monitors. Instead, there is a message showing that the monitor is disabled.

Last processing period

The last period for which the monitor collected sample data and ran its tests.

Last run finish time

The last time that the trigger ran; this is left blank for monitors that have not triggered yet.

Last run total time taken

The time that was taken for all the monitor tests to run; this is rounded to the nearest second. For example a run that takes 00:00:00.8 seconds has a **Last run total time taken** of 'Less than 1 second'.

Current processing period

The current period for which the monitor collects sample data and runs its tests.

Note: The current processing period only appears when a monitor is currently processing data.

Licence Error

If the process that is used by this monitor has expired, a flashing message appears, containing the name of the expired process.

Note: The licence expiry message only appears when the relevant P2 Sentinel process has expired.

Status Messages

A log of all status messages, sorted by most recent status message.

Note: The number of status messages stored and displayed is defined in the P2 Sentinel configuration file.

Icon

The icon displays the type of status message; for example, an information icon.

Time

The date and time (to the second) that the monitor status was reached.

Message

A message to describe the status, which includes the total time taken for the current run time

Export to Excel

Click **Export to Excel** to export the status messages to a Microsoft Excel spreadsheet.

Refresh

Click **Refresh** to get the latest monitor status.

Clear Messages

Click **Clear Messages** to clear all messages from the monitor status message log.

Note: Only user groups with appropriate permissions can perform this function.

Restart

Click **Restart** to restart a monitor that has stopped. The monitor will process for the period from **Last run finish time** through **Next trigger time**, and then continue with the normal trigger periods.

Note: This button is only displayed on the status page for **stopped** monitors.

Restart at now

Click the **Restart at now** button to restart a monitor. The monitor will process for the period from **now** (current time) through **Next trigger time**, and then continue with the normal trigger periods.

Last Refresh

The date and time that the **Refresh** button was last clicked.

ERROR MESSAGES ON THE MONITOR STATUS TAB

For detailed information regarding error messages that appear on the Monitor Status page, see Troubleshooting, or contact P2 Customer Support for assistance.

Importing and Exporting

The P2 Sentinel configuration can be copied from one Sentinel database to another, using the Import/Export functionality. You may want to import from a development environment to a production environment, or you may want to import various workspaces, folders, monitors or event views from one production environment to another.

Important: None of the events or run-time data can be exported or imported. Only workspaces, folders, monitors and event views (in their configurations) can be exported and imported.

The P2 Sentinel Import/Export feature allows you to select exactly which workspaces, folders, monitors and event views to export. When importing, all workspaces, folders, monitors and event views in the migration package are imported.

Import/Export Privileges

To import or export, you need a security role that includes the **Sentinel Admin** privilege.

Version Compatibility

The P2 Sentinel Import/Export procedure requires that the version of Sentinel used between the export and import are compatible, and also that the package version numbers are compatible.

Sentinel Version Compatibility

Sentinel version compatibility (for the purpose of importing) requires that the instance of Sentinel used for the import is of an equal or later version than that used for the export.

Package Version Compatibility

Package version compatibility (for the purpose of importing) requires that the version of Sentinel used for the import has the same *package number* as that of the Sentinel version used for the export (for example, a migration package from *package version* 1.0 can be imported to a Sentinel instance of *package version* 1.0, but not to a Sentinel instance where the *package version* is 2.0).

Each version of P2 Sentinel has a package version number. This number can be the same across several versions of P2 Sentinel.

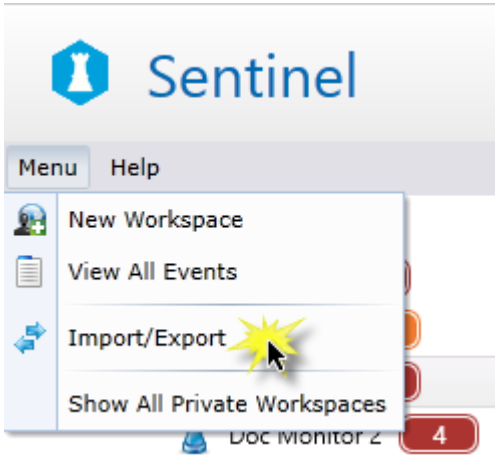
The package version number is displayed in the **Export** tab of P2 Sentinel.

Exporting from a P2 Sentinel Environment

You can export some or all of the public workspaces, folders, monitors and event views from a P2 Sentinel environment. The exported package can then be used to import some or all of these workspaces, folders, monitors and event views to another P2 Sentinel environment.

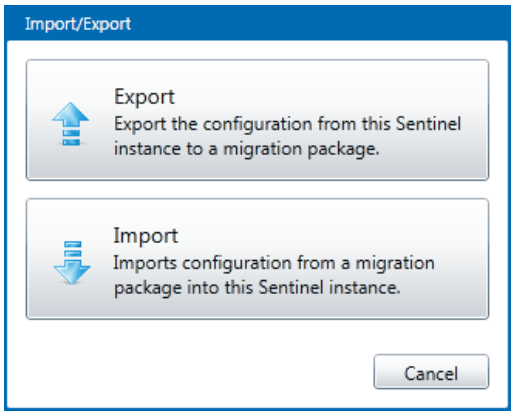
To export from P2 Sentinel:

1. Click the **Menu** button below the Sentinel header.
2. Click  **Import/Export**.



Note: This menu option only appears to users who have import or export permissions.

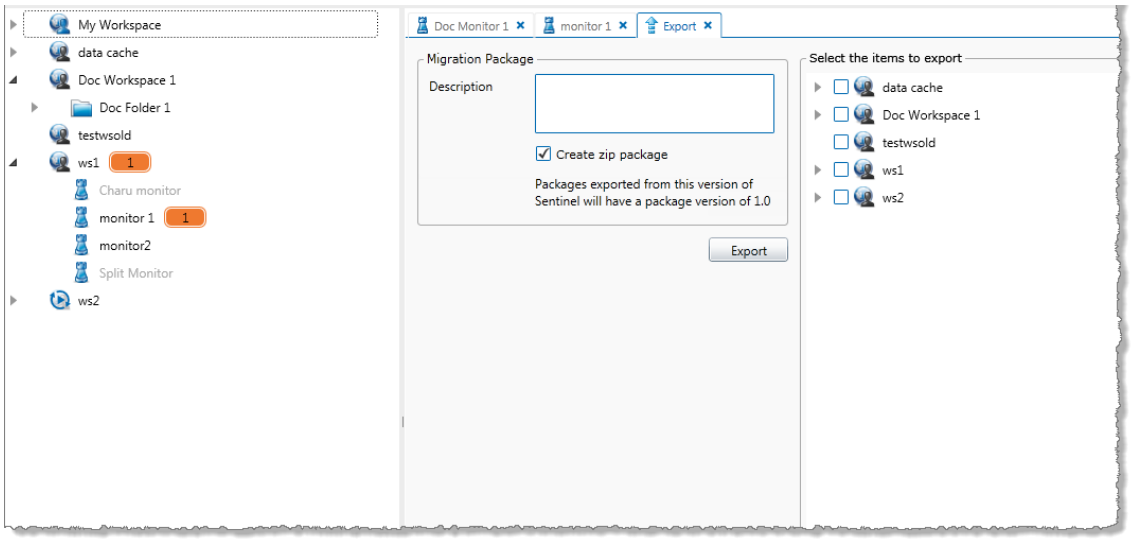
The **Import/Export** window appears.



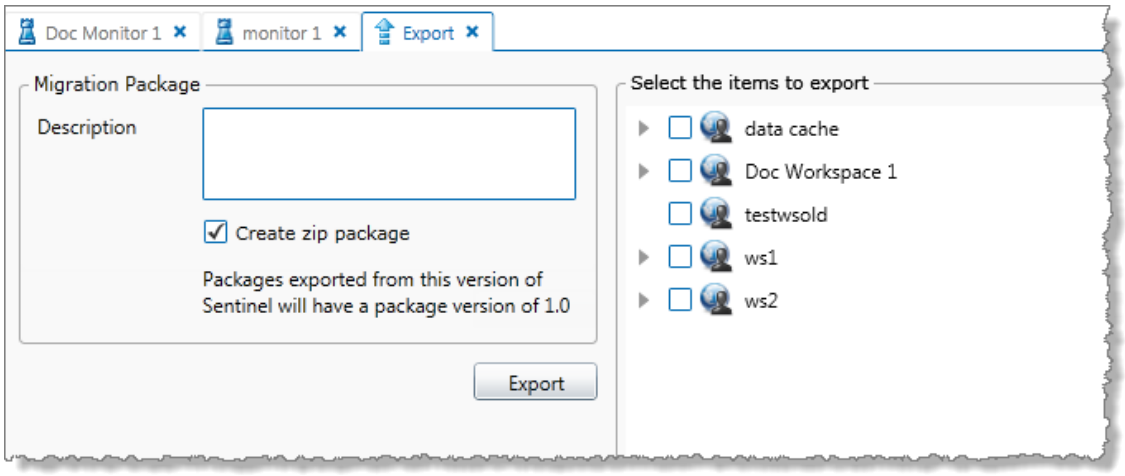
3. Click the **Export** panel.

Note: This panel is not available if you do not have permissions to export from a P2 Sentinel environment.

The **Export** tab opens.



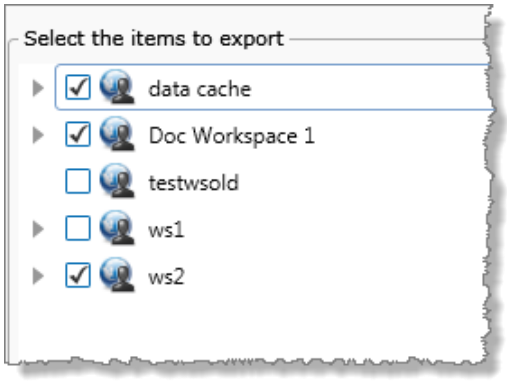
All of the public workspaces appear in a tree, on the right side panel, named **Select the items to export**.



4. Select the workspaces, folders, monitors and event views that you want to export.

To select workspaces in the Export tab:

- Select the check box next to each workspace that you want to export.

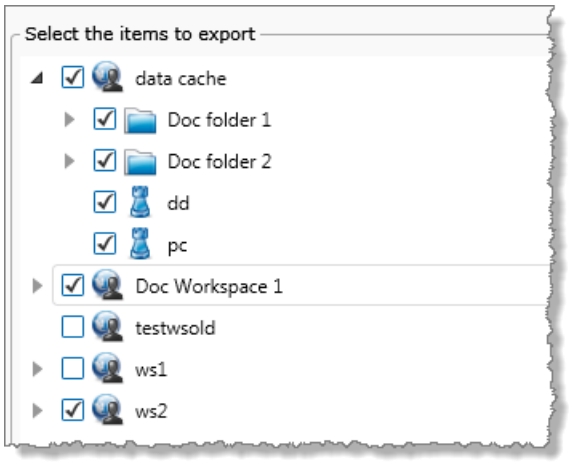


Note: All of the folders, monitors and event views within the selected workspaces are selected for export.

To select or deselect folders in the Export tab:

a. Expand a workspace by clicking the little grey arrow ▶ to the left of the workspace name. You can only expand a workspace if it contains folders or monitors.

The grey arrow is replaced by a downward-pointing black arrow ◢ and the folders contained in the workspace appear in a tree structure below the workspace. If the workspace is selected, then all of the folder and monitor check boxes are selected.

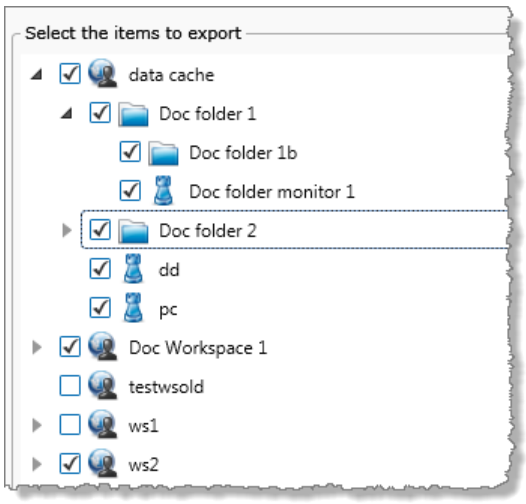


b. Select or deselect the check boxes next to each folder that you want to include in the export.

To select or deselect monitors in the Export tab:

a. Expand a folder by clicking the little grey arrow ▶ to the left of the folder name. You can only expand a folder if it contains sub-folders or monitors.

The grey arrow is replaced by a downward-pointing black arrow ◢ and the folders and monitors contained in the folder appear in a tree structure below the folder. If the folder is selected, then all of the folder and monitor check boxes are selected.



b. Select or deselect the check boxes next to each monitor that you want to include in the export.

Selecting an item without selecting its parents within the hierarchy:

If you do not select a folder, but select one or more items (folders, monitors or event views) contained within the folder, the folder is partially selected, as indicated by a dash ▬ in the check box.

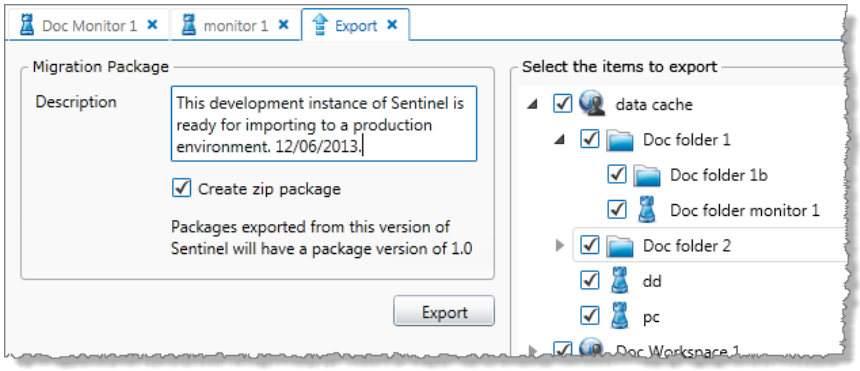
Selecting a monitor that is part of a chain:

Monitors that use the Monitor Chaining trigger, and monitors that are used as a Monitor Training trigger, are part of a linked chain of monitors. To export a monitor that is part of a chain, you need to also select the linked monitor.

5. When you have selected all of the monitors, folders and workspaces that you want to export, prepare the export package.

   a. In the Migration Package panel, on the left of the Export tab, type a description in the **Description** box, to be used as the migration package file name.

   b. Deselect the **Create zip package** check box if you want to create a non-zip file.



Note: The package version number for the Sentinel version that you are exporting from is displayed in the lower half of the Migration Package panel.

6. Click **Export**.

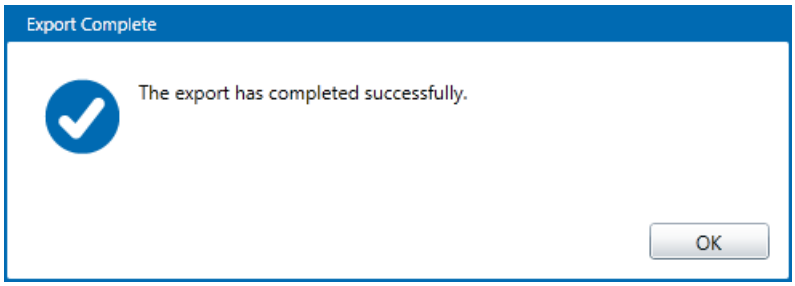
   A **Save As** dialog box opens.

7. Navigate to the folder where you want to save the file.

8. Type a file name in the **File name** box.

9. Click **Save** to save the file.

   A dialog appears to confirm that the export completed successfully.



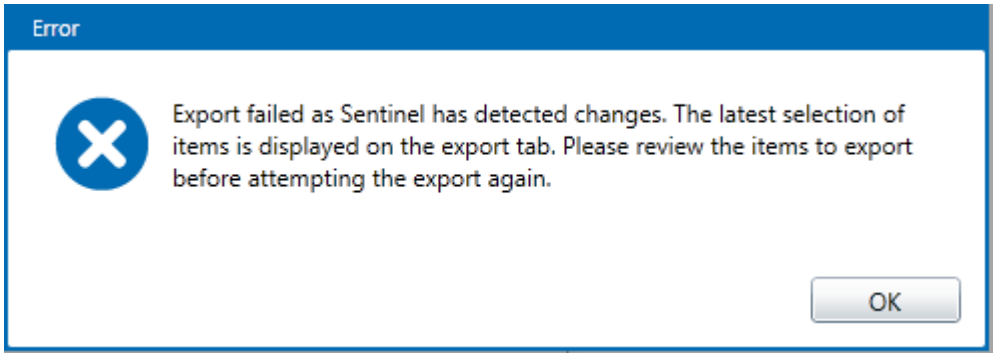
10. Click **OK** to close the dialog.

Special Behaviour during a Sentinel Export

The following sections describe some of the behaviour you can expect when doing a Sentinel export.

Changes to the Sentinel Configuration during Export

If the Sentinel workspace, folder and monitor configuration changes while the export tab is open, an error message is displayed after you attempt the export.



- Click **OK** to close the message.

The latest changes to workspaces, folders and monitors are displayed in the Export tab.

The migration package description and the previously selected items remain (except for items that may have been deleted from the workspace).

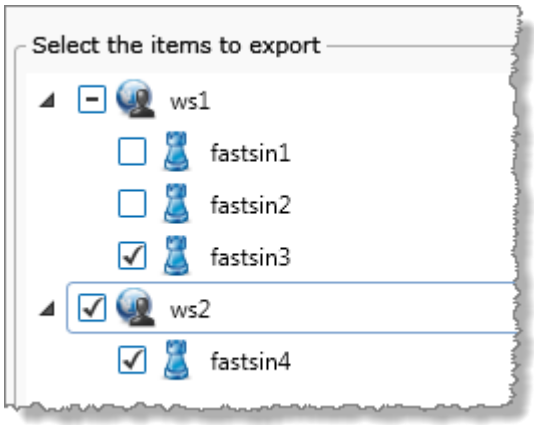
You can attempt to export the selected items again.

Private Workspaces

Private workspaces cannot be exported. If you want to export folders or monitors from a private workspace, you first need to move these to public workspaces.

Selecting Child Items within the Hierarchy

If you do not select a folder, but select one or more items (folders, monitors or event views) contained within the folder, the folder is partially selected, as indicated by a dash ▬ in the check box. This folder is exported. When the package is imported, the folder will only be included *if it does not already exist*. This ensures that the structure remains intact for the selected items, but that *no updates are made for the partially selected item*.



The same rule applies to any workspace that has not been selected, but where items within that workspace have been selected.

In the example depicted above, workstation **ws1** is exported. During importing, it will only be imported if it does not already exist in that instance of Sentinel.

Exporting Linked Monitors

Monitors that use the Monitor Chaining trigger, and monitors that are used as a Monitor Chaining trigger are part of a linked chain of monitors. In order to export a monitor that is part of a chain, you need to also select the linked monitor. The affected monitor has a label *"Select monitor [monitor name] to export this chain"* to help you identify the linked monitor.

If you select a monitor that is used as a Monitor Chaining trigger, the monitors that use this trigger are automatically selected as well (see Figure 13, where monitor **4171** has been selected, and **Monitor 1** and **Monitor 2** are auto-selected).

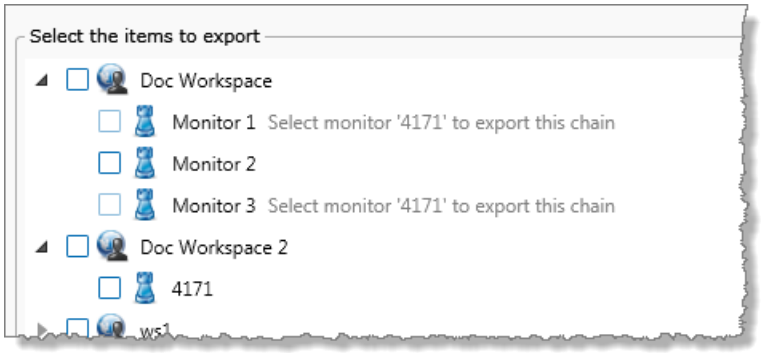


Figure 12: Exporting with no items selected

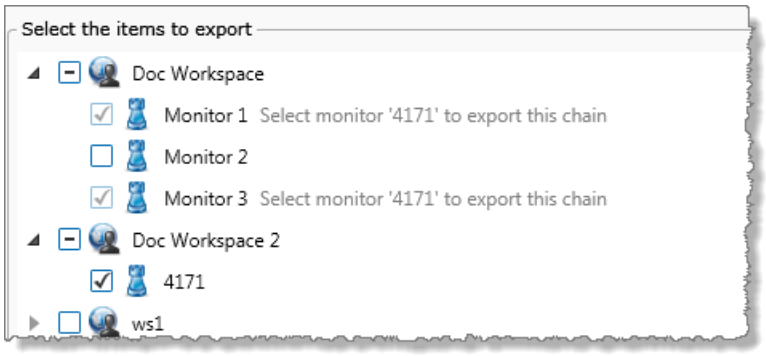


Figure 13: Select the chained monitor; the linked monitors are auto-selected.

Note that you cannot select the monitors that use monitor chaining triggers; these can only be auto-selected.

Exporting Monitors Containing User Processes

If you export a monitor that has a user process attached, the user process will also be exported at the version that the monitor is using.

The Sentinel Migration Package

When you have finished exporting, you can move, copy or email the migration package so that it can be used for an import.

Note: The migration may be viewed but not updated. Updating corrupts the file.

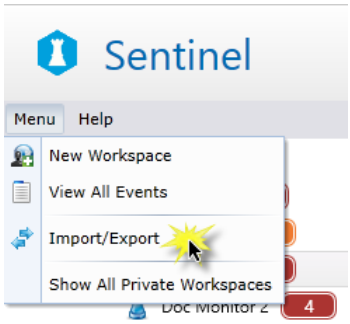
Importing to a P2 Sentinel Environment

Note: The import procedure cannot be reversed. Please ask your System Administrator to make a backup of your Sentinel database before you proceed with the import, in case you need to revert to your pre-import configuration.

You will need a *Sentinel Migration Package* to import. This can either be a zipped (.zip) file, or a plain .xml file, created by an export from another P2 Sentinel environment.

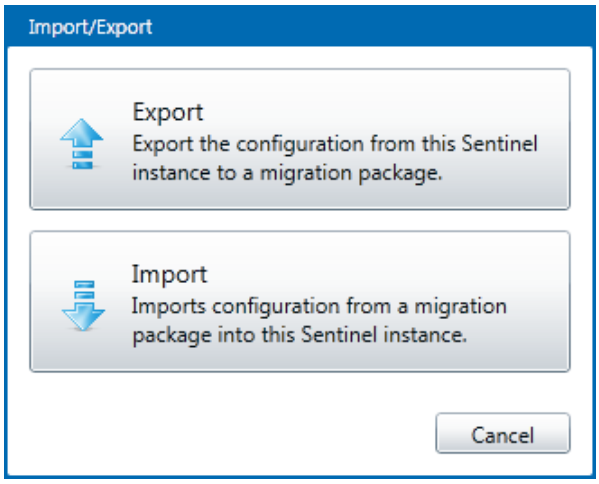
To import to P2 Sentinel:

1. Click the **Menu** button below the Sentinel header.
2. Click **Import/Export**.



Note: This menu option only appears to users who have import or export permissions.

The *Import/Export* window appears.



1. Click the **Import** panel.

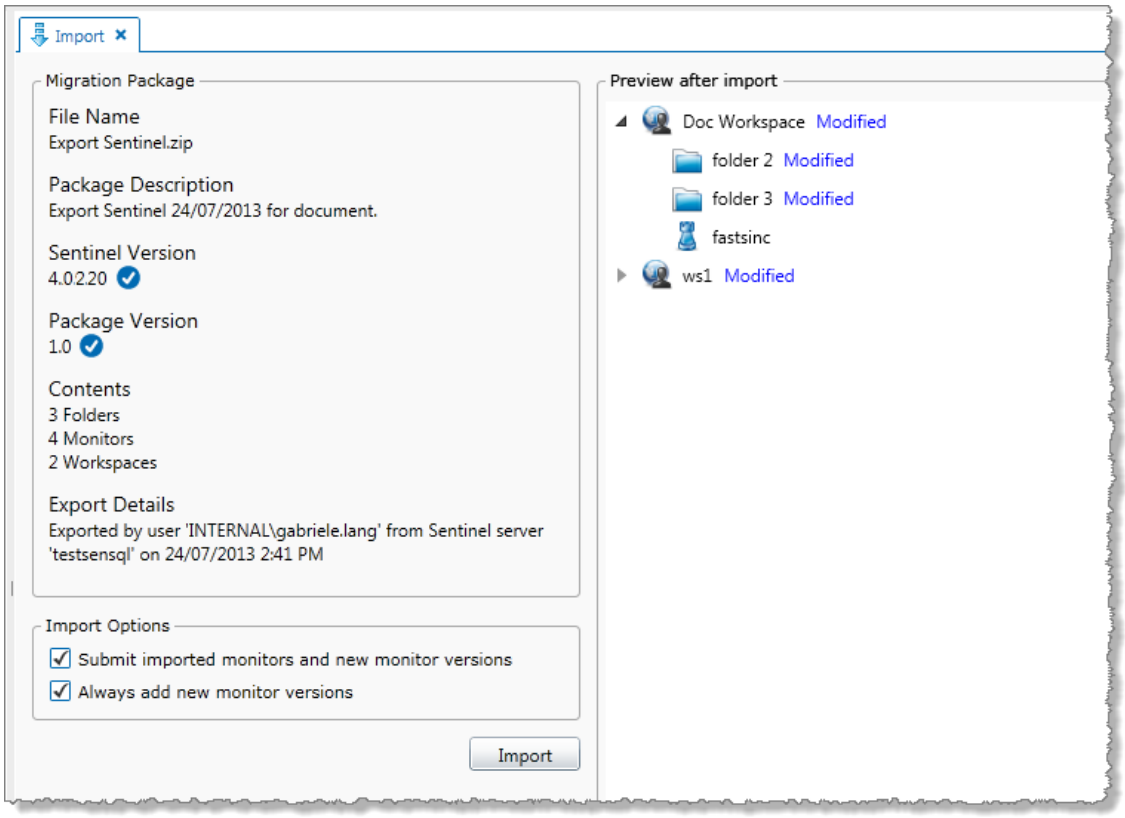
Note: This panel is disabled if you do not have permissions to import to a P2 Sentinel environment.

An **Open** dialog box appears.

2. Navigate to the folder containing the package you want to import.
3. Click on the file, and click **Open**.

Note: If the migration package is corrupt, the **import cannot continue**. An error message window appears. Click **OK** to close the window. The **Import** tab closes.

If this is a valid Sentinel migration package, the **Import** tab opens.



The following information appears on the different panels of the *Import* tab.

Migration Package

This contains the following information relating to the package:

File Name

The file name of the migration package.

Package Description

The description that was supplied at the time that the export package was created (if no package description was added, this header does not appear).

Sentinel Version

The full version number of the migration package Sentinel version (for example 4.0.2.20); this has a tick icon if there are no Sentinel version compatibility issues. If the Sentinel instance that you are importing to has an earlier version number than the migration package version number, the versions are incompatible, and an error icon is displayed along with an error message showing the version number of this Sentinel instance.

Package Version

The full package number of the migration package Sentinel version (for example 1.0); this has a tick icon if there are no package version compatibility issues. If the Sentinel instance that you are importing to has a different package number than the migration package number, the Sentinel version package numbers are incompatible,

and an error icon is displayed along with an error message showing the package number of this Sentinel instance.

Contents
A contents list of the migration package, broken down into separate counts for folders, monitors and workspaces.

Export Details
The user name of the user who performed the export operation, the exporting server name, and the date and time that the migration package was created.

Note: If either the Sentinel version or the Package version number is incompatible, **the import cannot continue**.

Import Options
The default import options are displayed here.

Submit imported monitors and new monitor versions
If this instance of Sentinel is configured to use Change Management, then this option is available, otherwise not.

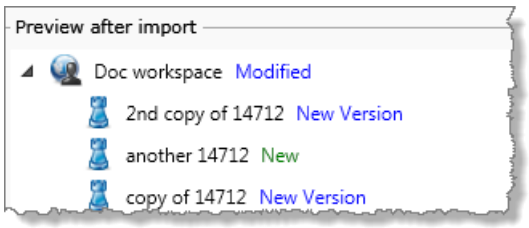
If you select the check box, then imported monitors, or existing monitors with new versions, are automatically submitted for approval if the check box is selected.

Always add new monitor versions
If selected, the system always imports this version of the monitor. If not selected, the system will only import this monitor version if it does not already exist in the instance of Sentinel.

Preview after import
The *Preview after import* panel on the right side of the Import tab shows a preview of what the Workspace panel will contain after the import.

This includes what is currently in the Workspace panel, as well as the newly imported items.

You can navigate through the *Preview after import* panel in the same way that you navigate through the Workspace panel. The following labels are appended to the import item (workspace/folder/monitor) names as applicable.



New
The **New** label indicates that the item to be imported is completely new to this Sentinel instance.

Modified
The **Modified** label indicates that the applicable workspace or folder to be imported contains items that already exist in this instance of Sentinel.

Moved

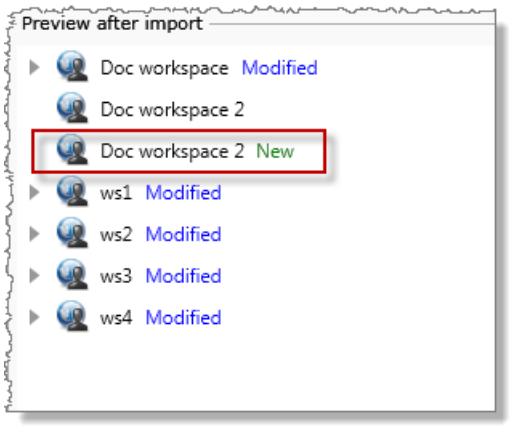
The **Moved** label indicates that the item to be imported already exists in this instance of Sentinel, but is in a different location (folder or workspace). During import, the item is moved to its new location (as it exists in the migration package).

New Version

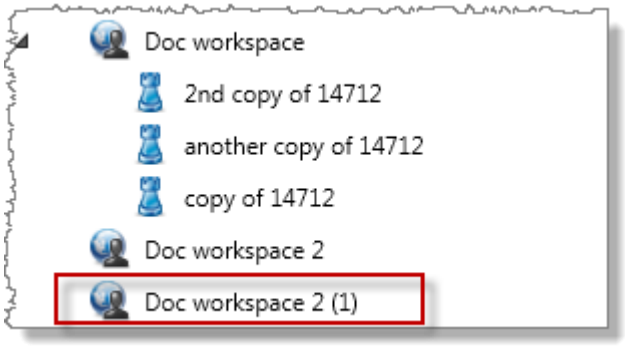
Only monitors will have the **New Version** label. This label appears for monitors that already exist in this Sentinel instance, but where the migration package version is different from the version in this instance of Sentinel.

New items with the same name

If a workspace in the migration package has the same name as an existing workspace, but is not actually the same workspace, then the workspace to be imported will have suffix of "(1)", after the import. For example, "Doc workspace 2" is imported as "Doc workspace 2 (1)". In the preview panel, this suffix does not exist.



Preview of workspace *Doc workspace 2*

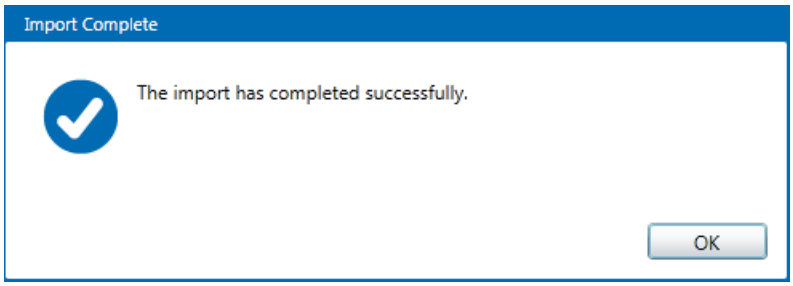


Doc workspace 2 ***after import, now named*** *Doc workspace 2 (1)*

The same behaviour can be observed with different monitors that have the same name, and different folders that have the same name.

4. Change one or both of the import options by selecting or deselecting the relevant check boxes in the **Import Options** panel. The options are: *Submit imported monitors and new monitor versions* and *Always add new monitor versions*.
5. Review the *Preview after import* panel.
6. Click **Import**.
7. Click **Yes** in the *Perform Import* confirmation dialog.

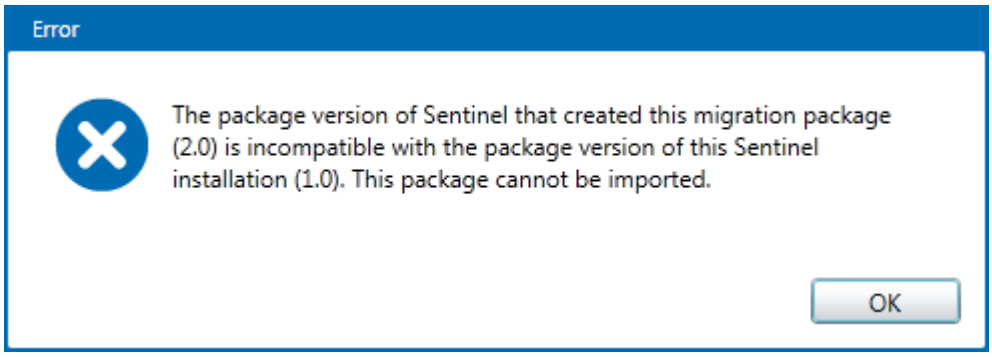
   The import completes, with a message:



Each imported monitor has a version comment, indicating that this version of the monitor was imported, and taking the form: "[comment from exported version] - migrated from [migrating Sentinel server name]".

FOR INCOMPATIBLE PACKAGES OR VERSIONS

If either the Sentinel version or the Package version is incompatible, an error message appears.



- Click **OK** to close the message box.

APPROVE IMPORTED MONITORS

If Change Management has been implemented, you will need to approve the newly imported monitors.

1. Submit new monitors for approval (unless you selected to have automatic submissions as part of the import).
2. Approve or reject the newly imported monitors.

Troubleshooting

This section describes some of the problems that may occur while using P2 Sentinel, and how to resolve them. For a guide on issues that occur while installing P2 Sentinel, refer to "**Troubleshooting**" in the *P2 Sentinel Installation and Administration Guide*.

Footer Status Messages

This section describes some of the messages that may appear in the Status area of the Sentinel Footer, and how to resolve them.

Can't connect to Engine

PROBLEM: THE P2 SENTINEL USER INTERFACE CANNOT CONNECT TO THE P2 SENTINEL ENGINE.

Description: The following message appears in the Status Panel when the P2 Sentinel User Interface cannot connect to the P2 Sentinel Engine:

```
Can't connect to P2 Sentinel Engine - it may not be running
```

Cause: The most probable causes for this message are:

- The P2 Sentinel Engine has stopped.
- There is a network connection issue.

Resolution: The system administrator should check the P2 Sentinel Engine to see if it is running, and restart it if necessary. If the P2 Sentinel Engine is running, then the system administrator should check the network connection and resolve any network problems.

TO RESTART THE P2 SENTINEL ENGINE

1. Go to ***Control Panel > Administration Tools > Services*** on the server that hosts the P2 Sentinel Engine.
2. Locate **P2 Sentinel Processing Engine** in the list.
3. If the status is **stopped,** right-click on **P2 Sentinel Processing Engine**, and select **Start** from the list.

Cannot connect to P2 Sentinel Reporting Engine

PROBLEM: THE P2 SENTINEL USER INTERFACE CANNOT CONNECT TO THE P2 SENTINEL REPORTING ENGINE.

Description: The following message appears in the Status Panel when the P2 Sentinel User Interface cannot connect to the P2 Sentinel Reporting Engine:

```
Can't connect to P2 Sentinel Reporting Engine - it may not be running
```

Cause: The most probable causes for this message are:

- The P2 Sentinel Reporting Engine has stopped.

  Resolution: The system administrator should check the P2 Sentinel Reporting Engine to see if it is running, and restart it if necessary.

- There is a network connection issue.

  Resolution: If the P2 Sentinel Reporting Engine is running, then the system administrator should check the network connection and resolve any network problems.

- There is a mismatch between the ExternalEventSQL setting in the web.config file and the Reporting database.

  Resolution: The Sentinel administrator should compare the ExternalEventSQL setting in the web.config file and make sure it matches what is in the Reporting database.

TO RESTART THE P2 SENTINEL REPORTING ENGINE

1. Go to ***Control Panel > Administration Tools > Services*** on the server that hosts the P2 Sentinel Reporting Engine.
2. Locate **P2 Sentinel Reporting Engine** in the list.
3. If the status is **stopped,** right-click on **P2 Sentinel Reporting Engine**, and select **Start** from the list.

Monitor Status Messages

This section describes some of the messages that may appear in the Monitor Status page, and how to resolve them.

Monitor Restart Warning Message

PROBLEM: A MESSAGE APPEARS ON THE MONITOR STATUS PAGE.

Description: The message is: `Monitor has been requested to run but it is already running. Please refer to the Sentinel documentation for more information`.

Cause: The message appears when the monitor trigger attempts to start the next lot of monitor processing while the monitor is already processing tests.

Resolution: You can take any of the following actions to resolve this issue:

- Adjust the trigger so that the previous processing session always has enough time to complete.
- Reduce the number of monitor entities if there is too much processing in a single monitor test.
- Reduce the number of monitors throughout the installation if processing in general is too slow and is affecting system performance. Refer to "**Performance Considerations**" in the *P2 Sentinel Installation and Administration Guide*.

If you ignore the message, processing will continue. However, this will not necessarily occur at the expected trigger intervals and it is best to address the underlying cause.

No Entities for Processing Warning Message

PROBLEM: A MESSAGE APPEARS ON THE MONITOR STATUS PAGE WHEN A MONITOR TEST SOURCE DOES NOT RETURN ANY ENTITIES FOR PROCESSING.

Description: The message is:

`The source did not return any entities for processing. For further information please consult the Sentinel documentation.`

Cause: When using P2 Server this can be caused by either of the following two cases:

- One of the process inputs has been configured to **Source Entity** but none of the source entities have a data source in P2 Server.
- The process inputs have been configured to a set of attributes or attribute values and the combination of these configurations results in no matches found in P2 Server.

Resolution: Take the following steps to resolve this issue:

1. Open the monitor that is causing the problem.
2. Make the necessary adjustments in the test source and process inputs.
   - Change the test source if this is causing the problem.
   - Change process inputs if these are causing the problem.

Service Error Message

PROBLEM: P2 SENTINEL USER INTERFACE IS NOT CONNECTING TO THE P2 SENTINEL SERVICE.

Description: The following message appears in the Main panel when the P2 Sentinel User Interface cannot connect to the P2 Sentinel Service:

Cause: The most probable causes for this message are:

- The P2 Sentinel Service has stopped.
- There is a network connection issue.
- A firewall is preventing the Sentinel User Interface from connecting to the Sentinel Configuration Service.

Resolution: The system administrator should check the P2 Sentinel Service to see if it is running, and restart it if necessary. If the P2 Sentinel Service is running, then the system administrator should check the network connection and resolve any network problems; this is possibly a firewall problem.

Note: If you hover the mouse over Show Exception, a more detailed message is displayed.

TO RESTART THE P2 SENTINEL SERVICE

1. Go to ***Control Panel > Administration Tools > Services*** on the server that hosts the P2 Sentinel Service.
2. Locate **ISS Sentinel Service** in the list.
3. If the status is **stopped,** right-click on **ISS Sentinel Service**, and select **Start** from the list.

IF THE CONNECTION PROBLEM IS CAUSED BY A FIREWALL

If restarting the P2 Sentinel Service does not resolve the problem, there may be a firewall preventing the Sentinel User Interface from connecting to the P2 Sentinel Service.

You can take either of the following actions to resolve this issue:

- Disable any firewalls that may be preventing the connection between the Sentinel configuration service and the user interface.
- Set a rule to allow inbound traffic.

Missing Process Input Parameters

PROBLEM: DURING PROCESSING, A MONITOR RAISES A WARNING ABOUT MISSING DATA.

Description: The message is:

```
Error fetching data for [ASSET NAME:ATTRIBUTE]: The entity name could not be
properly resolved for one or more historization points. Check that the entity
string is defined for the duration of the request date times.
```

Repeated warnings may ultimately cause the monitor to stop (as determined by the Sentinel configuration **ShutdownMonitorOnWarnings** and **MaxWarningCount** parameters).

Cause: Sometimes an asset that is being monitored is missing attributes or attribute values that should be defining process limits.

> ***For example:***
> The temperature on a set of pumps is defined as an input in a particular Min Max process. The pump's `:MaxTemp` attribute is defined as the **Max** limit for the process, and the pump's `:MinTemp` attribute is defined as the **Min** limit for the process.
>
> In this example, The `:MinTemp` attribute is missing for `PUMP001` (it has not been configured in P2 Server yet). Every time the test runs against the asset `PUMP001`, it fails to test against the missing *MinTemp* attribute, and a warning is raised.

Resolution: Configure the missing attributes or attribute values of assets, in P2 Server, if these are available. The warning message identifies which asset has missing attributes (in respect to the process settings); use this information to find and configure the missing attributes/attribute values.

Alternative Resolution: You can create a new entity in P2 Server that is of data type **String** and which has an expression that is equal to the **UnconfiguredLimitString** parameter in the Sentinel Configuration file (the default value is "unconfigured" - please refer to the *P2 Sentinel Installation and Administration Guide*). You can assign this asset to any known un-configured attributes of entities that are used as limits in Sentinel processes.

During processing, Sentinel recognises that the missing attribute is a declared "unconfigured" attribute, and continues processing without raising any warnings.

Note: This alternative resolution applies to *Min Max* and *Alarm* processes only.

General Troubleshooting

Contact Lookup Taking too Long

PROBLEM: THE CONTACT LIST IS TAKING TOO LONG TO LOAD.

Description: When adding a list of contacts to an email, SMS or SMS via Web Service action, the list of available contacts takes a long time to load.

Cause: P2 Sentinel is searching through the whole of the Active Directory. If this is a very large directory, the search is going through all nodes of the Active Directory server.

Resolution: Update the **ActiveServerDirectory** setting in the P2 Sentinel Configuration file. Refer to "**Update the P2 Sentinel Configuration File**" in the *P2 Sentinel Installation and Administration Guide*. You need to add the node information that is relevant to users. For example, LDAP://adserver/CN=Users,DC=example,DC=com. This will limit the search to the *Users* node in the domain *example.com*.

Events Not Appearing in the Asset Reports

PROBLEM: EVENTS ARE NOT BEING DISPLAYED IN THE ASSET REPORTS.

Description: Some of the events that are visible in the **View Events** page are not being displayed in the asset reports.

Cause: The system clock on the client machine is not synchronised to the system clock on the P2 Sentinel Server.

Resolution: Synchronise the system clock on the client machine to the system clock on the P2 Sentinel Server.

Missing Event Data

PROBLEM: PERIODS OF MISSING DATA IN THE REPORTS FOR CONTINUOUS DATA.

Description: There are patches of missing data where they would normally be expected, for example in reports and in the event log.

Cause: The monitor process that is testing continuous data has periods of missing data. Data is not available in the source over these periods.

Resolution: Check the **NoDataBehavior** setting in the P2 Sentinel Configuration file to see what the configured behaviour has been set to. Refer to "**Update the P2 Sentinel Configuration File**" in the *P2 Sentinel Installation and Administration Guide*.

The table below lists the possible values of **NoDataBehavior** and what the expected outcomes are, when *continuous data* is tested:

Value	Expected Outcomes
Error	A monitor error is raised.
Suppress	A data suppressed event is raised.
Ignore	No event is raised, and no error is raised. The data is simply missing.

If you would like to change the behaviour caused by no data, then update the **NoDataBehavior** setting in the P2 Sentinel configuration file to the appropriate value.

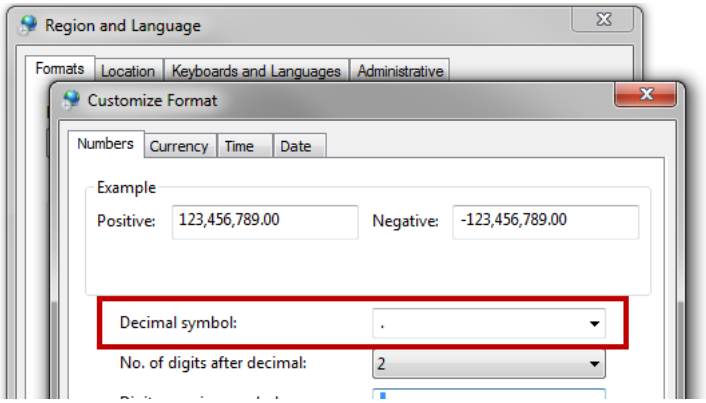
Erroneous Events

PROBLEM: UNEXPECTED EVENTS ARE RAISED IN P2 SENTINEL.

Description: The P2 Sentinel events are unpredictable and appear to be incorrect.

Cause: A likely cause is that the Windows format for the decimal symbol is incorrect; for example, it may be set to a comma (,) instead of a point (.).

Resolution: Ensure that the decimal symbol is set to a point (.) in the Windows formatting on the P2 Sentinel Server. This can be changed in the **Region and Language** settings in the Windows Control Panel (***Start > Control Panel > Region and Language > Additional Settings***).



If the decimal symbol already has the correct format, there may be another cause to this problem. Please contact P2 Customer Support via phone or email for further assistance.

Performance Issue

PROBLEM: P2 SENTINEL IS TOO SLOW.

Description: P2 Sentinel is much slower than usual.

Cause: P2 Sentinel has many tables containing thousands of rows of data. From time to time these tables need to be re-indexed for optimal database performance.

Resolution: The System Administrator should run the optimisation script, either as required or as part of a scheduled maintenance plan. Refer to "**Optimising the Database**" in the *P2 Sentinel Installation and Administration Guide*.

Note: It is strongly recommended that you regularly optimise the P2 Sentinel database. Either routinely submit the re-indexing script, or add the script as a regular database maintenance task.

Alternative resolutions: There are a number of different optimisation possibilities within Sentinel. Refer to "**Optimising P2 Sentinel**" in the *P2 Sentinel Installation and Administration Guide* for more detailed explanations and instructions.

Sentinel Configuration Service Connection Error

PROBLEM: THE SENTINEL CONFIGURATION SERVICE CANNOT BE CONTACTED.

Description: The message is: `The Sentinel configuration service cannot be contacted at address 'https://machinename/Sentinel'. Please check it is running and that the request is not breaking cross-domain policy`.

Cause: A firewall is preventing the Sentinel User Interface from connecting to the Sentinel Configuration Service.

Resolution: You can take either of the following actions to resolve this issue:

- Disable any firewalls that may be preventing the connection between the Sentinel configuration service and the user interface.
- Set a rule to allow inbound traffic.

Emails Not Sending Over SSL

PROBLEM: EMAILS DO NOT SEND AND THE MONITOR PRESENTS A REMOTE CERTIFICATE ERROR.

Description: Emails do not send when P2 Sentinel communicates with the configured mail server using an SSL connection. The full message is: `The remote certificate is invalid according to the validation procedure.`

Cause: P2 Sentinel has been configured to communicate with the mail server using an SSL connection but a trusted certificate issued for the mail server is not installed on the P2 Sentinel server, or the certificate is invalid.

Resolution: The System Administrator should obtain a copy of the relevant SSL certificate for the mail server and install it on the P2 Sentinel server. On Windows Server 2008 R2 certificates can be viewed and installed by clicking the **Start** button, typing **certmgr.msc** into the **Search** box and then pressing ENTER.

If the certificate is installed, the System Administrator should verify that the issuer matches the host name of the mail server and that the certificate has not expired.

Process Values Fetched before Precondition is Processed

PROBLEM: USER EXPECTS THE PRECONDITION TO PREVENT SENTINEL FROM READING NULL VALUES

Description: An error relating to the input data appears, despite the precondition not being met. For example, the following error message appears "Test [*test name*]: Error Fetching Source Data: Datums returned from the fetch for entity [*entity*] were not of a consistent data type. Expected data type 'Double', Value was 'null'". However, the precondition for this particular test should have failed under these data conditions.

Cause: P2 Sentinel reads primary input data before running the precondition. This is by design, and plays an important role in Sentinel's processing optimisation. In the scenario outlined above, the process encountered errors with data before it could even reach the precondition processing.

Resolution: It is helpful to understand the way Sentinel processes data, and in what order, before building tests with effective preconditions. For an overview of monitor processing, read the section Monitor Behaviour, and for a more detailed description, see Appendix K. The Sentinel Engine.

Appendix A. Alarm Process

The Alarm process is used for testing **continuous** data for a monitor item. The sample data is tested against high limits (***High*** and ***High High***), and against low limits (***Low*** and ***Low Low***).

The process can be specified to test against both high and low limits (***High***, ***High High***, ***Low*** and ***Low Low***), just against High limits (***High*** and ***High High***), or just against Low limits (***Low*** and ***Low Low***).

Events

When a new state is reached then a new event is raised. The severity for that state is specified in the state configuration panel of the test.

Values for the Limits

The ***High High***, ***High***, ***Low***, and ***Low Low*** limits can be defined as one of the following:

- A fixed numerical value (Fixed Value)
- A variable input value defined as one of:
  - Attribute (if the test's **Source** is *Entity* or *Hierarchy*)
  - Source Tag (if the test's **Source** is *Tag*)
  - Calculation
  - Tag
  - Entity Attribute

Optional Process Parameters

This feature allows P2 Sentinel to use ***process limits*** of assets with missing attributes.

For instructions on how to utilise this feature by using the **UnconfiguredLimitString** parameter, refer to "**Update the P2 Sentinel Configuration File**" in the *P2 Sentinel Installation and Administration Guide*.

State Transition Rules

The Alarm process has clearly defined state transition logic paths. Transition from one state to another is equally dependant on the current evaluation of data, and on the current state.

State transitions cause events to be raised, allowing for the escalation of actions via the Sentinel framework. Different actions can be assigned to different state outcomes.

In the Alarm process, any state can transition to any other state.

For example, the ***default*** state can transition to the ***high high*** state or the ***high*** state.

Test Outcomes

The following outcomes are possible when the Alarm process is executed:

Outcome	Description
Default State	Data is not in an erroneous state and is within the operating envelope.
High Exceeded State	Data is measured against a high limit. If it exceeds the high limit, a High Exceeded State is reached.
High High Exceeded State	Data is measured against a high high limit. If it exceeds the high high limit, a High High Exceeded State is reached.

Outcome	Description
Low Exceeded State	Data is measured against a low limit. If it is lower than the low limit, a Low Exceeded State is reached.
Low Low Exceeded State	Data is measured against a low low limit. If it is lower than the low low limit, a Low Low Exceeded State is reached.
Suppressed State	The monitor has been suppressed. For example, if the precondition has not been met.

Conditional Logic

The Alarm process provides the following conditional logic.

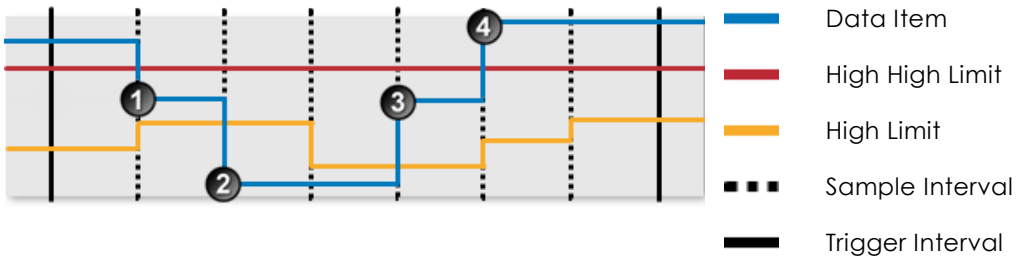
Note: All of the example graphs in the following sections show tests that have used the Last Known Value sample method.

High Limit Monitoring

The monitor item is monitored for upper limits on entities. The monitor item value is checked against the configured high value, and against the configured high high value.

- If the high value is exceeded, then a high exceeded event occurs and a high exceeded state is reached.
- If the high high value is exceeded, then a high high exceeded event occurs and a high high exceeded state is reached.

In the following example, High Limit Monitoring is used to detect when a value rises above a variable high limit, and when it rises above a fixed high high limit.



The following events are depicted in the graph:

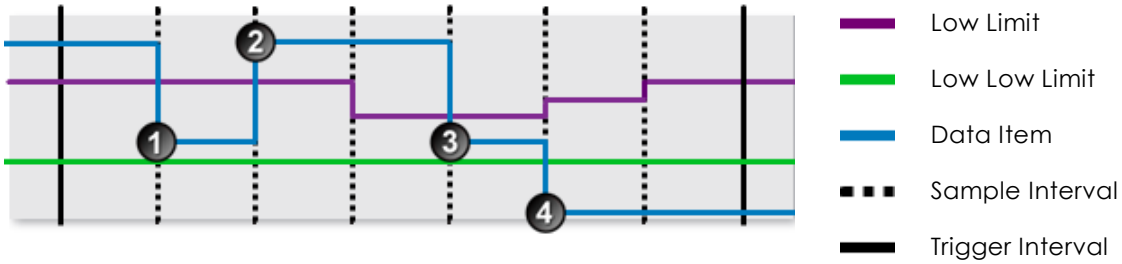
1. The data item value is greater than the high limit. A high exceeded state is reached, and a **high exceeded** event is raised.
2. The data item value is no longer greater than the high limit. A default state is reached, and a **default** event is raised.
3. The data item value is greater than the high limit again. A high exceeded state is reached, and a **high exceeded** event is raised.
4. The data item value is greater than the high high limit. A high high exceeded state is reached, and a **high high exceeded** event is raised.

Low Limit Monitoring

The monitor item is monitored for lower limits on entities. The monitor item value is checked against the configured low value, and against the configured low low value.

- If the data goes below the low value, then a low exceeded event occurs and a low exceeded state is reached.

- If the data goes below the low low value, then a low low exceeded event occurs and a low low exceeded state is reached.



The following events are depicted in the graph:

1. The data item value is lower than the low limit. A low exceeded state is reached, and a **low exceeded** event is raised.
2. The data item value is no longer lower than the low limit. A default state is reached, and a **default** event is raised.
3. The data item value is lower than the low limit again. A low exceeded state is reached, and a **low exceeded** event is raised.
4. The data item value is lower than the low low limit. A low low exceeded state is reached, and a **low low exceeded** event is raised.

High and Low Limit Monitoring

The monitor item is monitored for upper and lower limits on entities. The monitor item value is checked against the defined high value, the high high value, the low value and the low low value.

- If the high value is exceeded, then a high exceeded event occurs and a high exceeded state is reached.
- If the high high value is exceeded, then a high high exceeded event occurs and a high high exceeded state is reached.
- If the data goes below the low value, then a low exceeded event occurs and a low exceeded state is reached.
- If the data goes below the low low value, then a low low exceeded event occurs and a low low exceeded state is reached.

The following events are depicted in the graph:

1. The data item value is lower than the low low limit. A low low state is reached, and a **low low exceeded** event is raised.
2. The data item is between the low limit and the high limit. A default state is reached, and a **default** event is raised.
3. The data item value is higher than the high high limit. A high high exceeded state is reached, and a **high high exceeded** event is raised.
4. The data item value is lower than the low low limit. A low low state is reached, and a **low low exceeded** event is raised.

Adding an Alarm Process

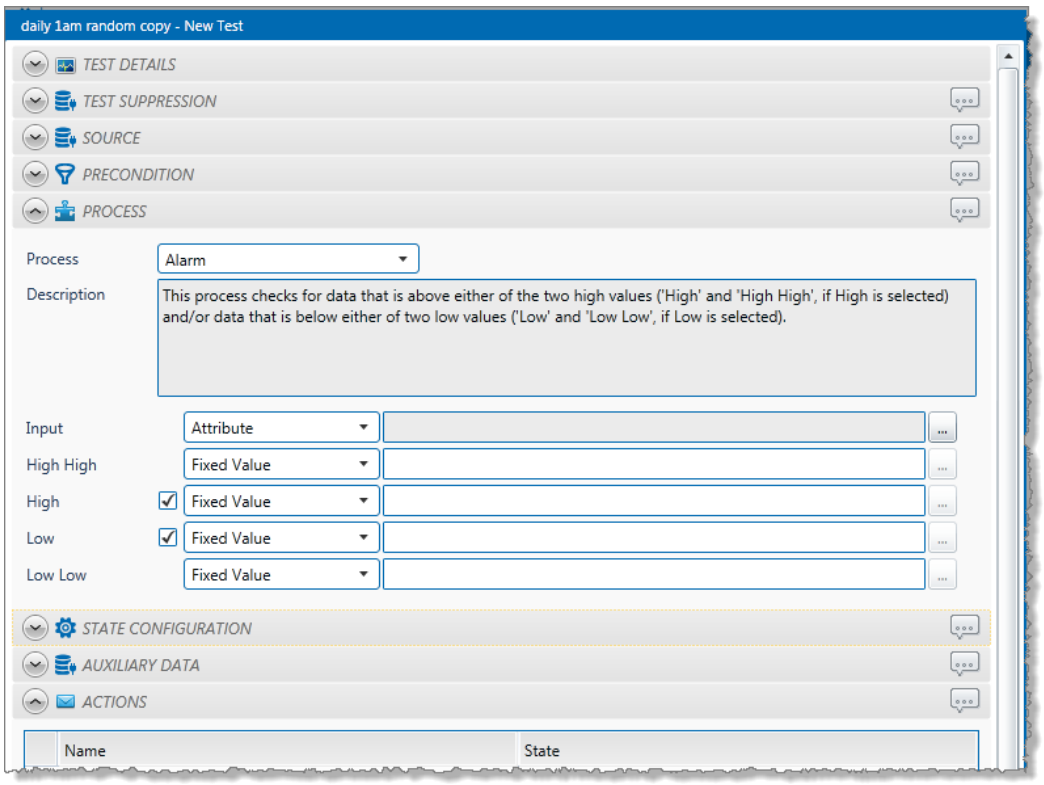
Every test uses a specific type of process, and each process has different limits to define; some of these limits are optional.

The Alarm Process is used for testing continuous values for a monitor item.

In the **Test** page:

1. Expand the **Process** panel.

   The **Process** panel appears as shown in the following screen image:



2. Add the process.

   a. In the **Process** drop-down list, select **Alarm**.

   b. From the **Input** drop-down list, select an input from the following:

      Attribute
      This option is only available if the **Source Type** is **Entity** or **Hierarchy**.

      Click the ellipsis button to select an attribute by using the P2 Server Attribute Picker. You are limited to selecting an attribute of the test source monitor items. This attribute of each of the monitor items is a separate process input.

      Source Tag
      This option is only available if the **Source Type** is **Tag**.

      If you select this option, then each of the tag monitor items is used as separate process input.

Calculation

Click the ellipsis button to open the *Edit Calculation* window. The expression is resolved in the P2 Server calculation engine.

If the Source Type is Entity or Hierarchy:
Type a calculation, prefixed by 'this' as the **Source Entity** token, for example: **{this:THP} + 34**.

If the Source Type is Tag:
Type a calculation, prefixed by 'this' as the **Source Tag** token, for example: **{this} * 2**.

Entity Attribute

Click the ellipsis button to open the *P2 Server Browser* to select an entity. From here, select a P2 Server attribute, or attribute value, by using *the* P2 Server Attribute Picker for the selected entity.

c. With an Alarm process, you can choose to define high values, low values, or both.

To define High values:

i. Select the **High** check box.

ii. Specify the **High** value (see "**Available Low and High Values**" below).

iii. Specify the **High High** value (see "**Available Low and High Values**" below).

To define Low values:

iv. Select the **Low** check box.

v. Specify the **Low** value (see "**Available Low and High Values**" below).

vi. Specify the **Low Low** value (see "**Available Low and High Values**" below).

Note: At least one pair of test limits, High or Low, must be specified for this process.

3. To add comments to the process panel click the comment button, at the top right of the panel.

Available Low and High Values

These are the values that you can specify for Low or High:

Fixed Value
Type in a numerical value.

Attribute
This option is only available if the test's **Source Type** is **Entity** or **Hierarchy**.

Click the ellipsis button to open the P2 Server Attribute Picker, to select an attribute of the source entities.

Source Tag
This option is only available if the **Source Type** is **Tag**.

Calculation
Click the ellipsis button to open the *Edit Calculation* window. The expression is resolved in the P2 Server calculation engine.

If the Source Type is Entity or Hierarchy:
Type a calculation, prefixed by 'this' as the **Source Entity** token, for example: **{this:THP} + 34**.

If the Source Type is Tag:
Type a calculation, prefixed by 'this' as the **Source Tag** token, for example: **{this} * 2**.

Tag

Click the ellipsis button to open the *P2 Server Browser* to select a tag.

Entity Attribute

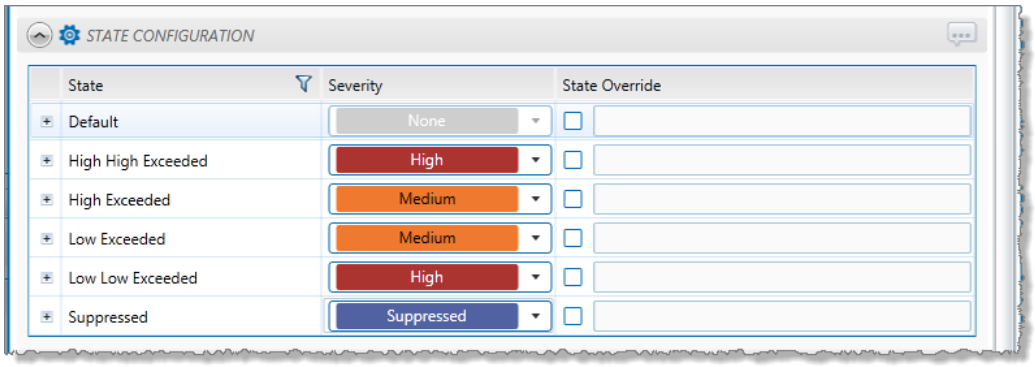
Click the ellipsis button to open the *P2 Server Browser* to select an entity. From here, select a P2 Server attribute, or attribute value, by using the P2 Server Attribute Picker for the selected entity.

Configuring States

For the Alarm process, you can configure the following states, each with an optional state override and comments:

- High High Exceeded
- High Exceeded
- Low Exceeded
- Low Low Exceeded
- Suppressed

You cannot change the severity of the Default state; however, you can add a state override and comments.



Note: Only configure states where you have set a limit.

To configure the state outcomes for a test in the **State Configuration** panel of the test, see 3.6 Configure States. If Case Management is enabled in Sentinel, this is also where you manage cases.

Appendix B. Min Max Process

The Min Max process is used for testing **continuous** data for a monitor item. The sample data is tested against a maximum limit (**Max***)* and a minimum limit (**Min***)*.

The process can be specified to test against both ***Min*** and ***Max*** limits, just against a ***Max*** limit, or just against a ***Min*** limit.

Events

When a new state is reached then a new event is raised. The severity for that state is specified in the state configuration for the test.

Values for the Limits

The *Min* and *Max* limits can be defined as one of the following:

- A fixed numerical value (Fixed Value)
- A variable input value defined as:
  - Attribute (An attribute of the test's source entity; this only applies where the **Source Type** is *Entity* or *Hierarchy*)
  - Source Tag (if the test's **Source** is *Tag*)
  - Calculation
  - Tag
  - Entity Attribute

Optional Process Parameters

This feature allows P2 Sentinel to use *process limits* of assets with missing attributes.

For instructions on how to utilise this feature by using the **UnconfiguredLimitString** parameter, refer to "**Update the P2 Sentinel Configuration File**" in the *P2 Sentinel Installation and Administration Guide*.

State Transition Rules

The Min Max process has clearly defined state transition logic paths. Transition from one state to another is equally dependant on the current evaluation of data, and on the current state.

State transitions cause events to be raised, allowing for the escalation of actions via the Sentinel framework. Different actions can be assigned to different state outcomes.

Default to Other States: A Default State can transition to a Min Exceeded State or a Max Exceeded State.

Min Exceeded to Other States: A Min Exceeded State can transition to a Max Exceeded State, or to a Default State.

Max Exceeded to Other States: A Max Exceeded State can transition to a Min Exceeded State, or to a Default State.

Test Outcomes

A number of outcomes are possible when the Min Max process is executed:

Outcome	Description
Default State	Data is not in an erroneous state (i.e. it is not below the minimum limit or above the maximum limit).
Max Exceeded State	Data is greater than the maximum limit.
Min Exceeded State	Data is less than the minimum limit.
Suppressed State	The monitor has been suppressed. For example, if a precondition has not been met.

Conditional Logic

The Min Max process provides the following conditional logic.

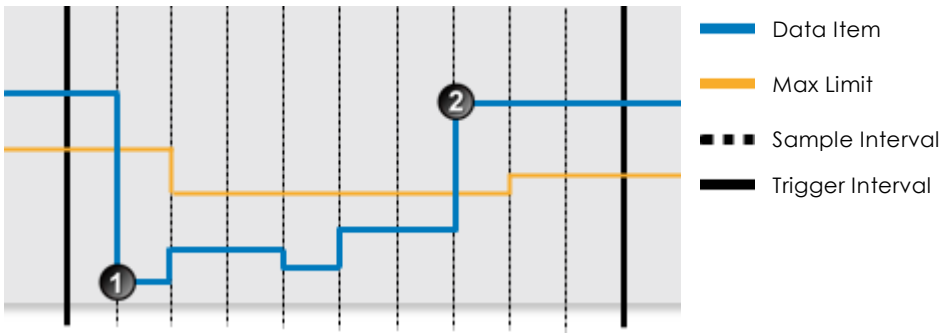
Note: All of the example graphs in the following sections show tests that have used the Last Known Value sample method.

Max Limit Monitoring

The monitor item is monitored for a maximum limit only.

If the item value exceeds the value defined in *Max*, a max exceeded event occurs and a max exceeded state is reached.

The following graph shows a possible scenario for a monitor item using Max Limit Monitoring.



The following events are depicted in the graph:

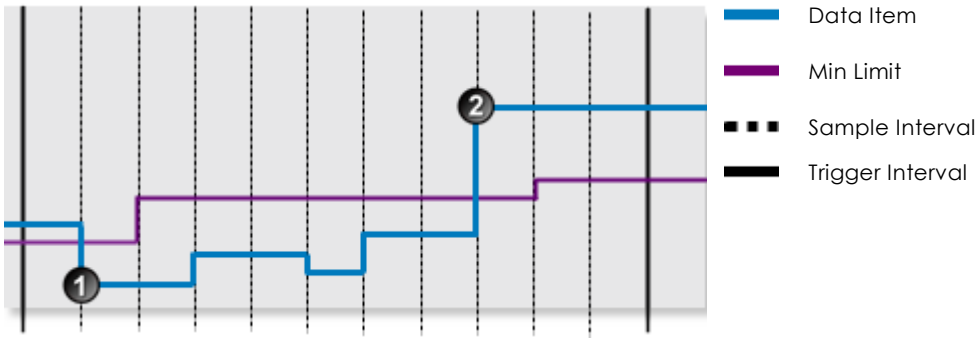
1. Data is below the max limit. A default state is reached, and a **default** event is raised.
2. Data is above the max limit. A max exceeded state is reached, and a **max exceeded** event is raised.

Min Limit Monitoring

The monitor item is monitored for a minimum limit only.

If the item value exceeds the value defined in *Min*, a min exceeded event occurs and a min exceeded state is reached.

The following graph shows a possible scenario for a monitor item using Min Limit Monitoring.



The following events are depicted in the graph:

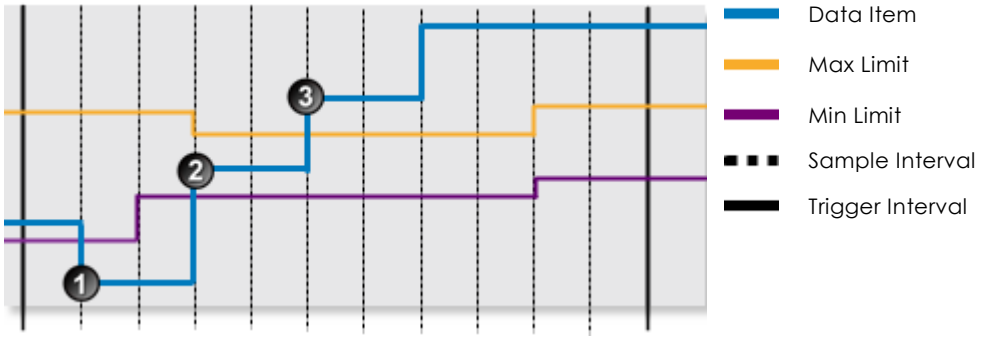
1. Data is below the min limit. A min exceeded state is reached, and a **min exceeded** event is raised.
2. Data is above the min limit. A default state is reached, and a **default** event is raised.

Min and Max Limit Monitoring

Here the item is monitored for minimum and for maximum limits on entities.

If the item value exceeds *Max*, then a max exceeded state is reached. If the value is lower than *Min*, then a min exceeded state is reached.

The following graph shows a possible scenario for a monitor item using Min and Max Limit Monitoring.



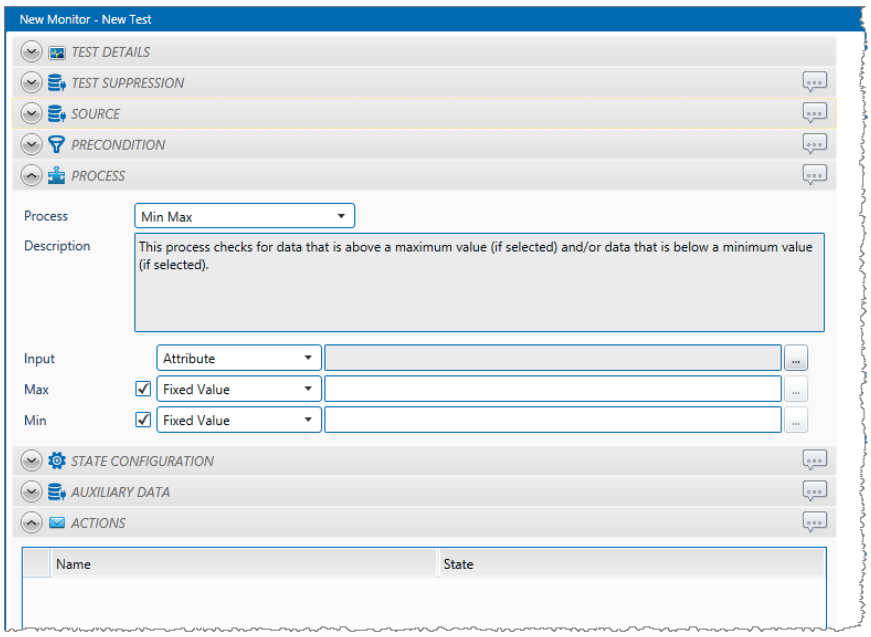
The following events are depicted in the graph:

1. Data is below the min limit. A min exceeded state is reached, and a **min exceeded** event is raised.
2. Data is above the min limit, but below the max limit. A default state is reached, and a **default** event is raised.
3. Data is above the max limit. A max exceeded state is reached, and a **max exceeded** event is raised.

Adding a Min Max Process

Every test uses a specific type of process, and each process has different limits to define; some of these limits are optional.

The Min Max Process is used for testing continuous data for a monitor item.



1. In the **Process** drop-down list, select **Min Max**.

2. From the **Input** drop-down list, select an input from the following:

   Attribute
   This option is only available if the **Source Type** is **Entity** or **Hierarchy**.

   Click the ellipsis button to select an attribute by using the P2 Server Attribute Picker. You are limited to selecting an attribute of the test source monitor items. This attribute of each of the monitor items is a separate process input.

   Source Tag
   This option is only available if the **Source Type** is **Tag**.

   If you select this option, then each of the tag monitor items is used as separate process input.

   Calculation
   Click the ellipsis button to open the *Edit Calculation* window. The expression is resolved in the P2 Server calculation engine.

   If the Source Type is Entity or Hierarchy:
   Type a calculation, prefixed by 'this' as the **Source Entity** token, for example: **{this:THP} + 34**.

   If the Source Type is Tag:
   Type a calculation, prefixed by 'this' as the **Source Tag** token, for example: **{this} * 2**.

Entity Attribute

Click the ellipsis  button to open the *P2 Server Browser* to select an entity. From here, select a P2 Server attribute, or attribute value, by using *the* P2 Server Attribute Picker for the selected entity.

3. With a *Min Max* process, you can choose to define a maximum limit, a minimum limit, or both.

   To define a Maximum limit:

   i. Select the **Max** check box.

   ii. Specify the **Max** value (see "**Available Min and Max Values**" below).

   To define a Minimum limit:

   iii. Select the **Min** check box.

   iv. Specify the **Min** value (see "**Available Min and Max Values**" below).

Note: At least one test limit, Min or Max, must be specified for this process.

4. To add comments to the process panel click the comment  button, at the top right of the panel.

Available Min and Max Values

These are the values that you can specify for Min or Max:

Fixed Value

Type in a numerical value.

Attribute

This option is only available if the test's **Source Type** is **Entity** or **Hierarchy**.

Click the ellipsis  button to open the P2 Server Attribute Picker, to select an attribute of the source entities.

Source Tag

This option is only available if the **Source Type** is **Tag**.

Calculation

Click the ellipsis  button to open the *Edit Calculation* window. The expression is resolved in the P2 Server calculation engine.

If the Source Type is Entity or Hierarchy:

Type a calculation, prefixed by 'this' as the **Source Entity** token, for example: **{this:THP} + 34**.

If the Source Type is Tag:

Type a calculation, prefixed by 'this' as the **Source Tag** token, for example: **{this} * 2**.

Tag

Click the ellipsis  button to open the *P2 Server Browser* to select a tag.

Entity Attribute

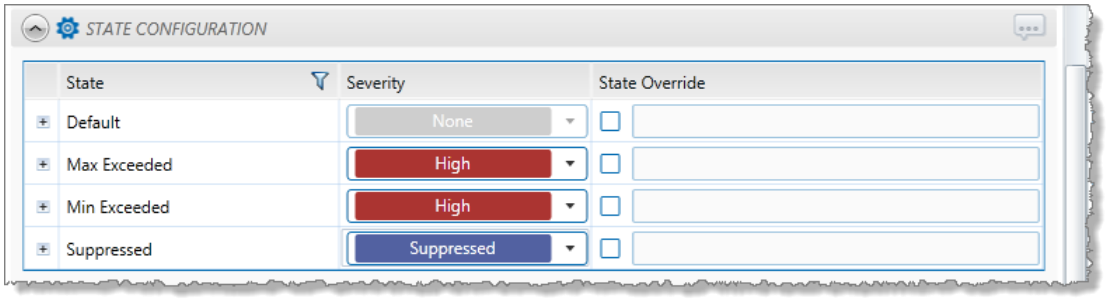
Click the ellipsis  button to open the *P2 Server Browser* to select an entity. From here, select a P2 Server attribute, or attribute value, by using the P2 Server Attribute Picker for the selected entity.

Configuring States

For the Min Max process, you can configure the following states, each with an optional state override and comments:

- Max Exceeded
- Min Exceeded
- Suppressed

You cannot change the severity of the Default state; however, you can add a state override and comments.



Note: Only configure states where you have set a limit.

To configure the state outcomes for a test in the **State Configuration** panel of the test, see 3.6 Configure States. If Case Management is enabled in Sentinel, this is also where you manage cases.

Appendix C. Digital State Process

The Digital State process is for evaluating different state pairs of the monitor item. The monitor item that is being tested will be in either one of two states. If it is in a ***Default Entity*** state, a default state is maintained. If it is in a ***Primary Limit Entity*** state, a primary state is reached.

There are several state pairs to choose from. By default these are:

Primary Limit Entity State	Default Entity State
Off	On
Shutdown	Running
One	Zero
0	1
1	0

These pairs are defined in the system configuration. You can define additional state pairs in the configuration file. For further information, refer to "**Update the P2 Sentinel Configuration File**" in the *P2 Sentinel Installation and Administration Guide*.

If the monitor item cannot be evaluated against the selected state pair, then an *Unknown* event is raised.

State Transition Rules

The Digital State process has clearly defined state transition logic paths. Transition from one state to another is equally dependant on the current evaluation of data, and on the current state.

State transitions cause events to be raised, allowing for the escalation of actions via the Sentinel framework. Different actions can be assigned to different state outcomes.

Default to Primary: A default state can only transition to the primary state or the unknown state.

Primary to Secondary: If the primary state endures for the specified secondary duration, a secondary state is reached.

Secondary to Tertiary: If the secondary state endures for the specified tertiary duration, a tertiary state is reached.

Unknown: Any state can transition to the unknown State. This state occurs as soon as the state pair cannot be evaluated.

Test Outcomes

A number of outcomes are possible when the Digital State Process is executed:

Outcome	Description
Default State	Data is in the *default entity state*, as defined in the state pair.
Primary State	Data is in the *primary entity state*, as defined in the state pair.
Secondary State	Data remains in the *primary entity state* for a specified duration (secondary duration).
Tertiary State	Data remains in the *secondary state* for a specified duration (tertiary duration).
Unknown State	If the monitor item cannot be evaluated against the selected state pair, then an Unknown event is raised.
Suppressed State	The monitor has been suppressed. For example, if a precondition has not been met.

Conditional Logic

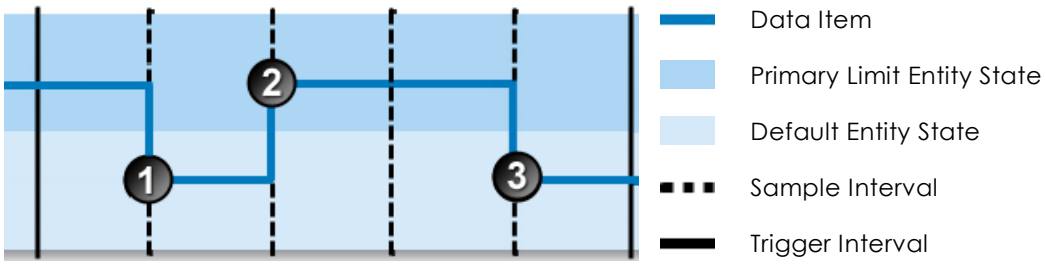
The Digital State process provides the following conditional logic.

Note: All of the example graphs in the following sections show tests that have used the Last Known Value sample method.

Primary Limit

During the test, the entity state is evaluated against the state pair.

If the monitor item is in the default entity state of the selected state pair, then a default event is raised, and a default state is reached. If the monitor item is in the primary entity state as defined by the selected state pair, then a primary event occurs and a primary state is reached.

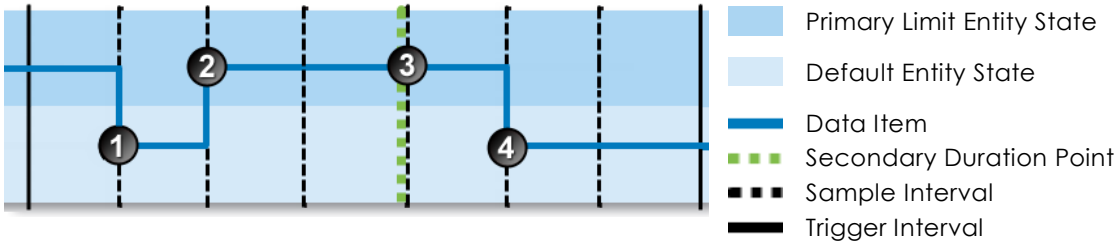


The following events are depicted in the graph:

1. The monitor item is in the default entity state of the state pair. A default state is reached, and a **default** event is raised.
2. The monitor item is in the primary limit entity state of the state pair. A primary state is reached, and a **primary** event is raised.
3. The monitor item has returned to the default entity state of the state pair. A default state is reached, and a **default** event is raised.

Secondary Duration

The duration of the primary state is measured against the secondary duration time period, defined in days, hours, minutes, and seconds. If a primary event lasts for the secondary duration, then a secondary event occurs and a secondary state is reached.



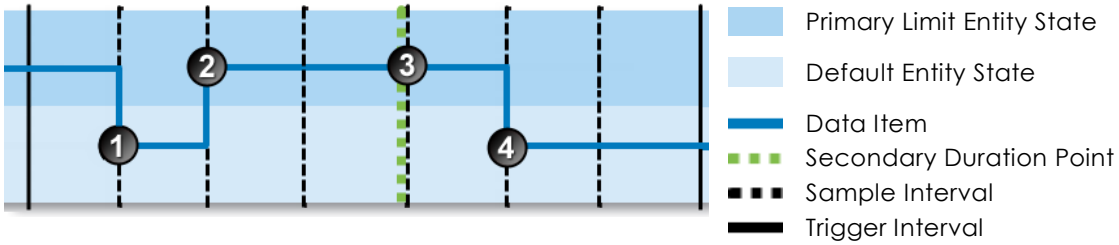
The following events are depicted in the graph:

1. The monitor item is in the default entity state of the state pair. A default state is reached, and a **default** event is raised.

2. The monitor item is in the primary limit entity state of the state pair. A primary state is reached, and a **primary** event is raised.
3. At the next sample interval the data is still in the primary limit entity state. The primary state has endured for the secondary duration. A secondary state is reached, and a **secondary** event is raised.
4. The monitor item has returned to the default entity state of the state pair. A default state is reached, and a **default** event is raised.

Tertiary Duration

The duration of the secondary state is measured against the tertiary duration period, defined in days, hours, minutes, and seconds. If a secondary state lasts for the tertiary duration, then a tertiary event occurs and a tertiary state is reached.



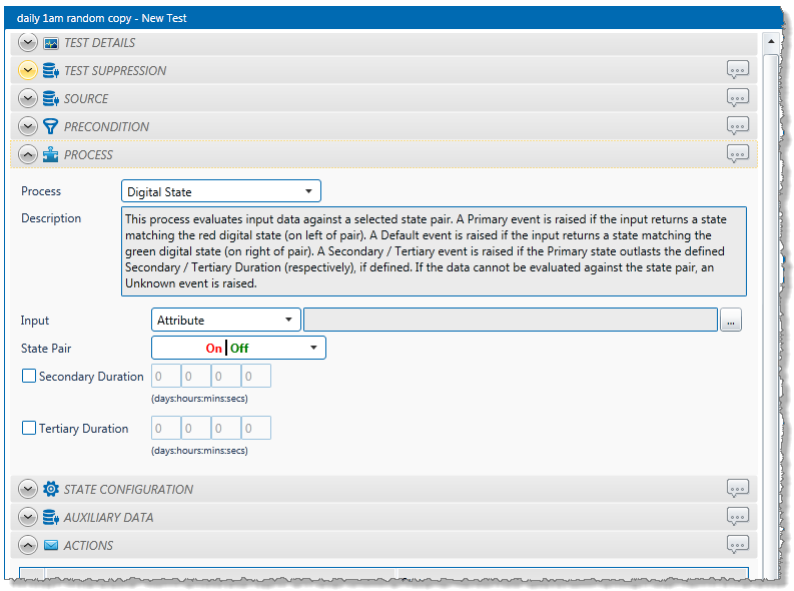
The following events are depicted in the graph:

1. The monitor item is in the default entity state of the state pair. A default state is reached, and a **default** event is raised.
2. The monitor item is in the primary limit entity state of the state pair. A primary state is reached, and a **primary** event is raised.
3. At the next sample interval the data is still in the primary limit entity state. The primary state has endured for the secondary duration. A secondary state is reached, and a **secondary** event is raised.
4. The monitor item has returned to the default entity state of the state pair. A default state is reached, and a **default** event is raised.

Adding a Digital State Process

Every test uses a specific type of process, and each process has different limits to define; some of these limits are optional.

The Digital State Process is used for evaluating state pairs (such as On | Off) of the monitor item.



1. In the **Process** drop-down list, select **Digital State**.
2. From the **Input** drop-down list, select an input from the following:

   Attribute
   This option is only available if the **Source Type** is **Entity** or **Hierarchy**.

   Click the ellipsis button to select an attribute by using the P2 Server Attribute Picker. You are limited to selecting an attribute of the test source monitor items. This attribute of each of the monitor items is a separate process input.

   Source Tag
   This option is only available if the **Source Type** is **Tag**.

   If you select this option, then each of the tag monitor items is used as separate process input.

   Calculation
   Click the ellipsis button to open the *Edit Calculation* window. The expression is resolved in the P2 Server calculation engine.

   If the Source Type is Entity or Hierarchy:
   Type a calculation, prefixed by 'this' as the **Source Entity** token, for example: **{this:THP} + 34**.

   If the Source Type is Tag:
   Type a calculation, prefixed by 'this' as the **Source Tag** token, for example: **{this} * 2**.

   Entity Attribute
   Click the ellipsis button to open the *P2 Server Browser* to select an entity. From here, select a P2 Server attribute, or attribute value, by using *the* P2 Server Attribute Picker for the selected entity.

3. Select a state pair from the **State Pair** drop-down list, to define the limit.

4. Define a secondary duration (optional).
    a. Select the **Secondary Duration** check box.
    b. Type integer values in the **Days**, **Hours**, **Minutes (Mins)**, and **Seconds (Secs)** boxes to define a duration period. The default value is zero.
5. Define a tertiary duration (optional).
    a. Select the **Tertiary Duration** check box.
    b. Type integer values in the **Days**, **Hours**, **Minutes (Mins)**, and **Seconds (Secs)** boxes to define a duration period. The default value is zero.

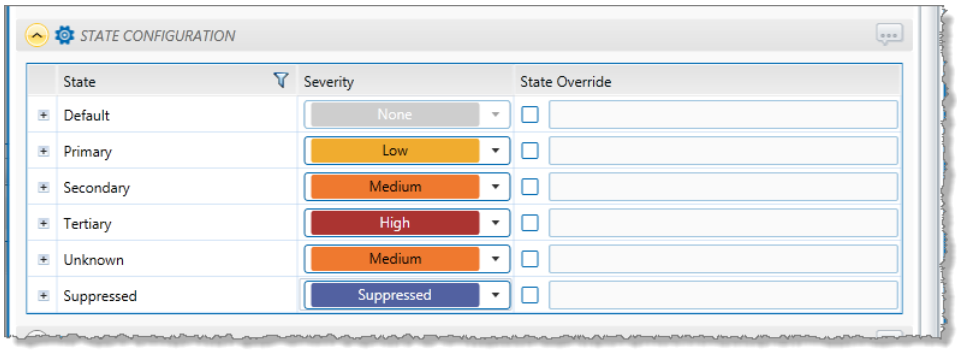
To add comments to the process panel click the comment button, at the top right of the panel.

Configuring States

For the Digital State process, you can configure the following states, each with an optional state override and comments:

- Primary
- Secondary
- Tertiary
- Unknown
- Suppressed

You cannot change the severity of the Default state; however, you can add a state override and comments.



Note: Only configure states where you have set a limit.

To configure the state outcomes for a test in the **State Configuration** panel of the test, see 3.6 Configure States. If Case Management is enabled in Sentinel, this is also where you manage cases.

Appendix D. Discrete Min Max Process

This process is used for testing discrete data for a monitor item. The sample data is tested against a maximum limit, ***Max***, and a minimum limit, ***Min***.

The process can be specified to test against ***Max*** and ***Min*** limits, just against a ***Max*** limit, or just against a ***Min*** limit. Any periods where no data is found will cause a ***No Data*** event.

State Transition Rules

The Discrete Min Max process has clearly defined state transition logic paths. Transition from one state to another is equally dependant on the current evaluation of data, and on the current state.

State transitions cause events to be raised, allowing for the escalation of actions via the Sentinel framework. Different actions can be assigned to different state outcomes.

Default to Other States: A Default State can transition to a Min Exceeded State or a Max Exceeded State. If no data is found, the Default State will transition to the No Data State.

Min Exceeded to Other States: A Min Exceeded State can transition to a Max Exceeded State, or to a Default State. If no data is found, the Min Exceeded State will transition to the No Data State.

Max Exceeded to Other States: A Max Exceeded State can transition to a Min Exceeded State, or to a Default State. If no data is found, the Max Exceeded State will transition to the No Data State.

No Data to Other States: As soon as data is found again, the No Data State will transition to another state: this could be Default State, Min Exceeded State or Max Exceeded State.

Test Outcomes

A number of outcomes are possible when the Discrete Min Max process is executed:

Outcome	Description
Default State	Data is not in an erroneous state (i.e. the data item is between the minimum and maximum limits).
No Data State	No data found in the trigger interval.
Max Exceeded State	Data is greater than the maximum limit.
Min Exceeded State	Data is less than the minimum limit.
Suppressed State	The monitor has been suppressed. For example, if the precondition has not been met.

Conditional Logic

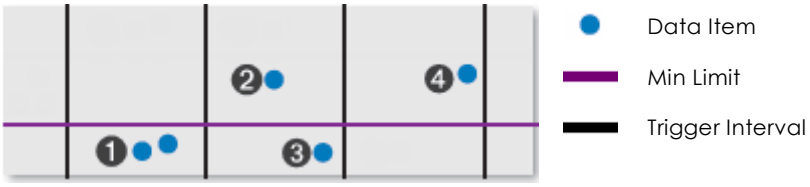
The Discrete Min Max process provides the following conditional logic.

Min Limit Monitoring

The monitor item is monitored for a minimum limit only.

If the item value exceeds the value defined in Min, a min exceeded event occurs and a min exceeded state is reached.

The Min limit must be defined as a fixed numerical value.



The following events are depicted in the graph:

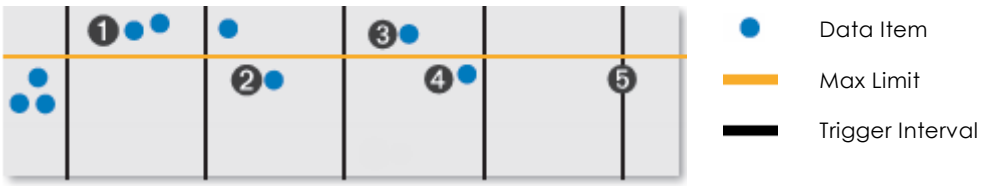
1. The data value is now below the min limit and a min exceeded state is reached. A **min exceeded** event is raised.
2. At the next trigger interval, the data is no longer lower than the min limit. It has returned to the default state. A new **default** event is raised.
3. In the same trigger interval, the data item value is lower than the min limit again. A min exceeded state is reached, and a **min exceeded** event is raised.
4. In the next trigger interval, the data value is no longer lower than the min limit. A default state is reached, and a **default** event is raised.

Max Limit Monitoring

The monitor item is monitored for a maximum limit only.

If the item value exceeds the value defined in Max, a max exceeded event occurs and a max exceeded state is reached.

The Max limit must be defined as a fixed numerical value.



The following events are depicted in the graph:

1. In this interval, the data item value is greater than the max limit. A max exceeded state is reached, and a **max exceeded** event is raised.
2. In the next interval, the data item value is no longer greater than the max limit. A default state is reached, and a **default** event is raised.
3. In the next interval, the data item value is greater than the max limit. A max exceeded state is reached, and a **max exceeded** event is raised.
4. In the same trigger interval, the data value is no longer lower than the min limit. A default state is reached, and a **default** event is raised.
5. No data found in the trigger interval. A **no data** event is raised.

Min and Max Limit Monitoring

Here the item is monitored for minimum and for maximum limits on entities.

If the item value exceeds Max, then a max exceeded state is reached. If the value is lower than min, then a min exceeded state is reached.

In the following example, Discrete Minimum and Maximum Monitoring is used to detect when a discrete value is greater than the maximum limit, and when a discrete value is less than the minimum limit.

The Min and Max limits must be defined as fixed numerical values.

The following events are depicted in the graph:

1. In this interval, the data item value is greater than the max limit. A max exceeded state is reached, and a **max exceeded** event is raised.
2. In the next interval, the data item value is no longer greater than the max limit. A default state is reached, and a d**efault** event is raised.
3. In the next interval, the data item value is less than the min limit. A min exceeded state is reached, and a **min exceeded** event is raised.
4. In the same trigger interval, the data value is no longer lower than the min limit. A default state is reached, and a **default** event is raised.
5. No data found in the trigger interval. A **no data** event is raised.

No Data Events

The Discrete Min Max process tests discrete data. Sometimes there is no data at all during a trigger interval. This causes a **No Data** event.

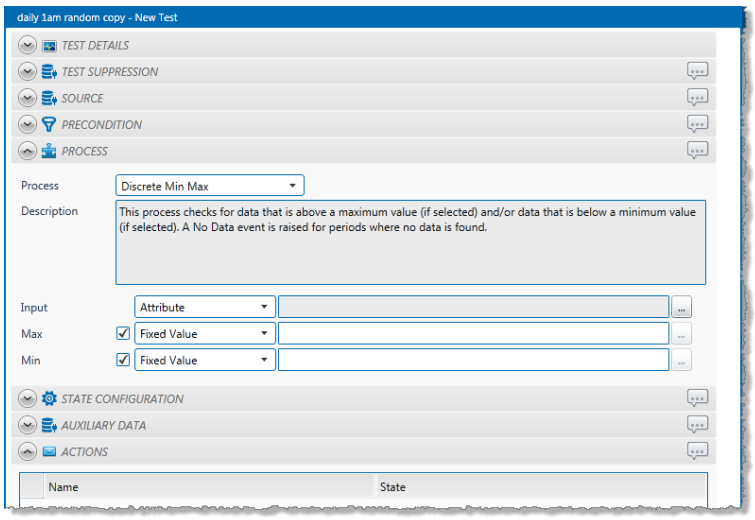
In this example, the data is monitored for a maximum limit only.

The following events are depicted in the graph:

1. In this interval, the data item value is greater than the max limit. A max exceeded state is reached, and a **max exceeded** event is raised.
2. In the next interval, the data item value is no longer greater than the max limit. A default state is reached, and a **default** event is raised.
3. No data found in the trigger interval. A **no data** event is raised.

Adding a Discrete Min Max Process

The Discrete Min Max Process is used for testing discrete data for a monitor item.



1. In the **Process** drop-down list, select **Discrete Min Max.**

2. From the **Input** drop-down list, select an input from the following:

   Attribute
   This option is only available if the **Source Type** is **Entity** or **Hierarchy**.

   Click the ellipsis button to select an attribute by using the P2 Server Attribute Picker. You are limited to selecting an attribute of the test source monitor items. This attribute of each of the monitor items is a separate process input.

   Source Tag
   This option is only available if the **Source Type** is **Tag**.

   If you select this option, then each of the tag monitor items is used as separate process input.

   Calculation
   Click the ellipsis button to open the *Edit Calculation* window. The expression is resolved in the P2 Server calculation engine.

   If the Source Type is Entity or Hierarchy:
   Type a calculation, prefixed by 'this' as the **Source Entity** token, for example: **{this:THP} + 34**.

   If the Source Type is Tag:
   Type a calculation, prefixed by 'this' as the **Source Tag** token, for example: **{this} * 2**.

   Entity Attribute
   Click the ellipsis button to open the *P2 Server Browser* to select an entity. From here, select a P2 Server attribute, or attribute value, by using *the* P2 Server Attribute Picker for the selected entity.

3. With a Discrete Min Max process, you can choose to define a maximum limit, a minimum limit, or both.

   To define a Maximum limit:

   i. Select the **Max** check box.

ii. Specify the **Max** value (see "**Available Min and Max Values**" below).

To define a Minimum limit:

iii. Select the **Minimum** check box.

iv. Specify the **Min** value (see "**Available Min and Max Values**" below).

Note: At least one test limit, Min or Max, must be specified for this process.

Available Min and Max Values

These are the values that you can specify for **Min** or **Max**:

Fixed Value

Type in a numerical value.

Attribute

This option is only available if the test's **Source Type** is **Entity** or **Hierarchy**.

Click the ellipsis button to open the P2 Server Attribute Picker, to select an attribute of the source entities.

Source Tag

This option is only available if the **Source Type** is **Tag**.

Calculation

Click the ellipsis button to open the *Edit Calculation* window. The expression is resolved in the P2 Server calculation engine.

If the Source Type is Entity or Hierarchy:
Type a calculation, prefixed by 'this' as the **Source Entity** token, for example: **{this:THP} + 34**.

If the Source Type is Tag:
Type a calculation, prefixed by 'this' as the **Source Tag** token, for example: **{this} * 2**.

Tag

Click the ellipsis button to open the *P2 Server Browser* to select a tag.

Entity Attribute

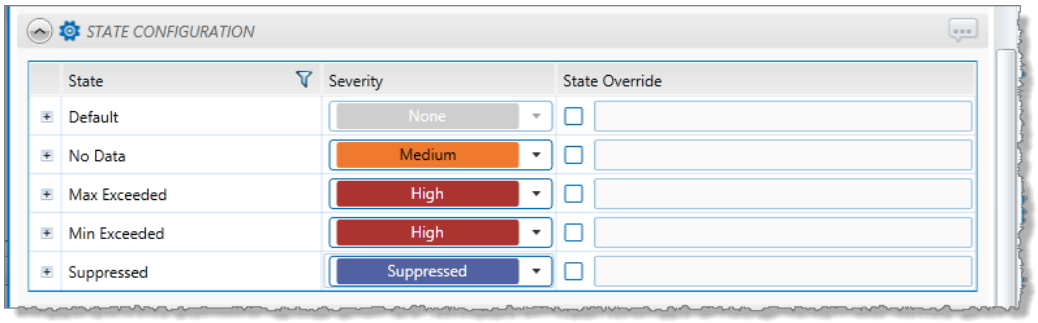
Click the ellipsis button to open the *P2 Server Browser* to select an entity. From here, select a P2 Server attribute, or attribute value, by using the P2 Server Attribute Picker for the selected entity.

Configuring States

For the Discrete Min Max process, you can configure the following states, each with an optional state override and comments:

- No Data
- Max Exceeded
- Min Exceeded
- Suppressed

You cannot change the severity of the Default state; however, you can add a state override and comments.

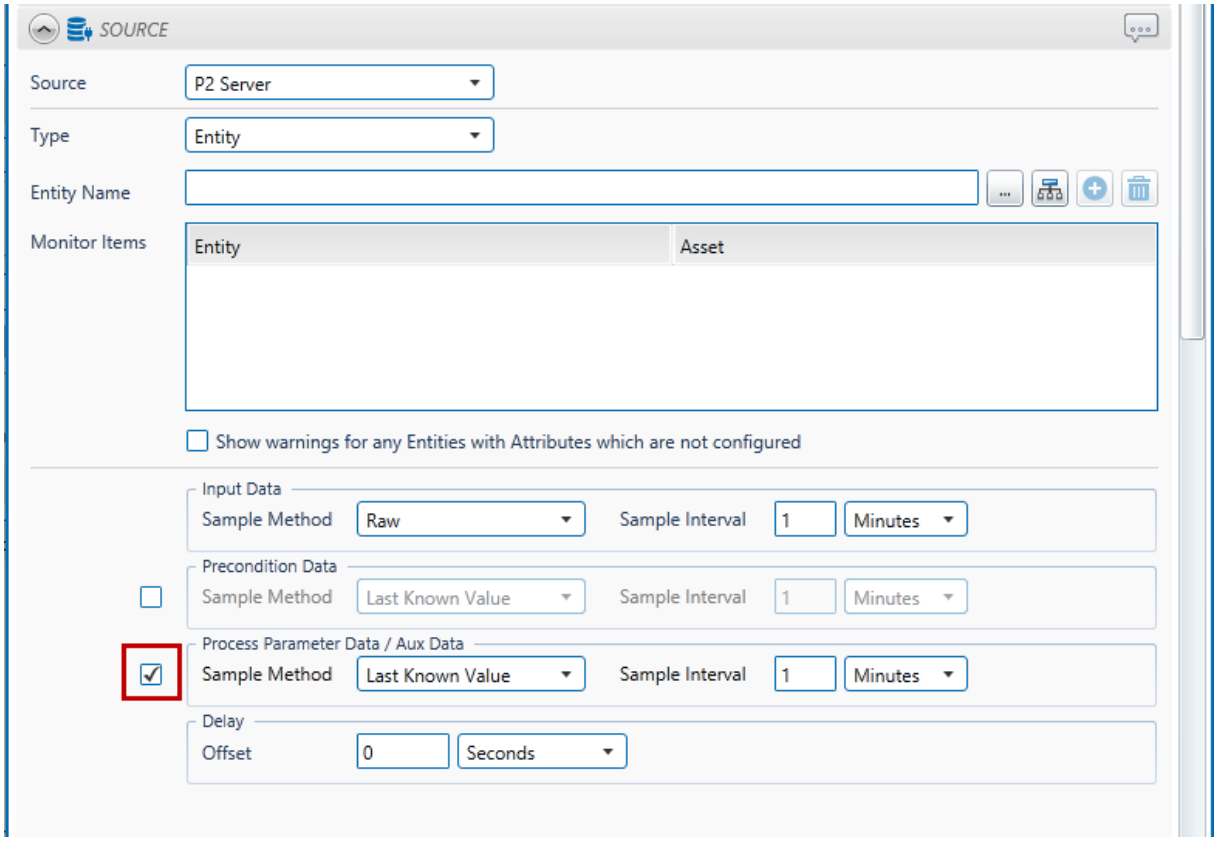


Note: Only configure states where you have set a limit.

To configure the state outcomes for a test in the **State Configuration** panel of the test, see 3.6 Configure States. If Case Management is enabled in Sentinel, this is also where you manage cases.

Auxiliary Data

If the test source includes auxiliary data, you need to select the **Process Parameter Data / Aux Data** check box and choose from the *Last Known Value, Average, or Linear Interpolate* sample methods, otherwise Sentinel will unsuccessfully attempt to collect the data using the *Raw* sample method.



Appendix E. Process Variable Surveillance Process

The Process Variable Surveillance process compares process variable data against defined limits and conditions.

Process Variable Surveillance is a complex process capable of concurrently monitoring multiple conditions such as transgression of limits, state duration, and movement between states.

State Transition Rules

The Process Variable Surveillance process has clearly defined state transition logic paths. Transition from one state to another is equally dependant on the current evaluation of data, and on the current state.

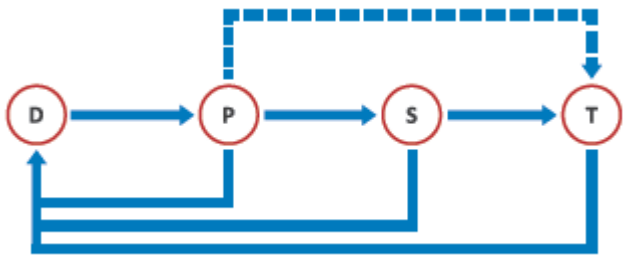
State transitions cause events to be raised, allowing for the escalation of actions via the Sentinel framework. Different actions can be assigned to different state outcomes.

The following table outlines the allowable state transitions of the Process Variable Surveillance process.

This state can transition to		This state
Default	→	Primary
Primary	→	Secondary
	⇢	Tertiary*
	→	Default
Secondary	→	Tertiary
	→	Default
Tertiary	→	Default

***Note**: Primary State can only transition to Tertiary State if the Tertiary Limit is breached, and not for any other conditions.

The following diagram outlines the state transition logic of the Process Variable Surveillance process.



D Default

P Primary

S Secondary

T Tertiary

Test Outcomes

A number of outcomes are possible when the Process Variable Surveillance process is executed:

DEFAULT STATE

Data is not in an erroneous state and is within the operating envelope.

PRIMARY STATE

Data is measured against a primary limit (fixed or variable). If it exceeds the primary limit (for a Maximum Operating Envelope), or if it is lower than the primary limit (for a Minimum Operating Envelope), a Primary State is reached.

SECONDARY STATE

A number of possible conditions can cause a secondary state. These are explained in more detail in the Secondary State section.

TERTIARY STATE

As with the secondary state, a number of conditions can cause a tertiary state. These are explained in more detail in the Tertiary State section.

SUPPRESSED STATE

The monitor has been suppressed. For example, if the precondition has not been met.

Output Status Tag

For tertiary and secondary states, you can set an output status tag.

This tag is a P2 Server entity attribute, or a tag, either as it is, or as part of a calculation. If a secondary output status tag is set, the tag will show a status of one within P2 Explorer when a secondary state is reached, and zero for any other state. Similar behaviour applies to the tertiary output status tag (one for tertiary state, zero for any other state). Within P2 Explorer, the status tag can be observed, for example altering a shape's appearance to indicate whether the monitor's data item is in a secondary / tertiary state or not.

Conditional Logic

The Process Variable Surveillance process provides the following conditional logic.

Note: All of the example graphs in the following sections show tests that have used the Last Known Value sample method.

Rolling Sum Period

A secondary state rolling sum period can be defined for evaluating some of the secondary state conditions; likewise, a tertiary state rolling sum period can be defined for evaluating some of the tertiary state conditions.

The rolling sum period is a defined period (specified in days and hours). At every sample interval, the rolling sum period is that period preceding the sample interval. So, for example, if the secondary state rolling sum period is set at 1 day 2 hours then at 3pm on Friday 3 August, the secondary state rolling sum period is from 1pm on Thursday 2 August (covering the last 1 day and 2 hours). Any evaluations relating to that sample interval's secondary state rolling sum period conditions must fall within that time.

Operating Envelope

Defines whether the maximum or minimum operation envelope is used for all conditions of the process.

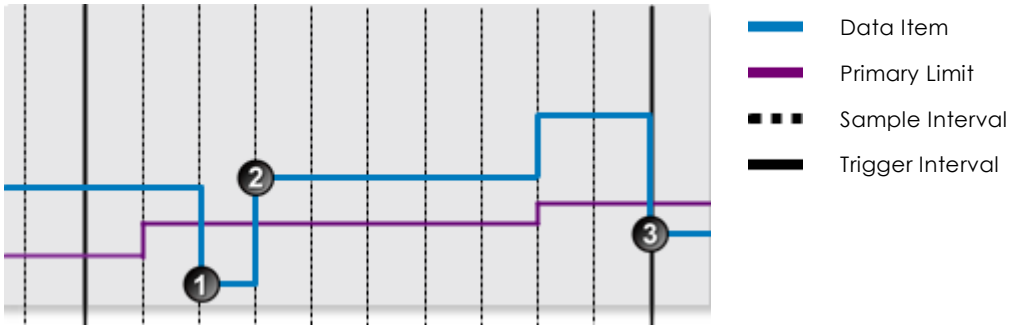
- If a ***minimum*** operating envelope is used, then excursions occur when values drop below a defined limit.
- If a ***maximum*** operating envelope is used, excursions occur when values exceed the defined limits.

Primary State Limit

The primary limit must be set for the process to work.

If the configured primary state limit is breached, a primary event occurs, and a primary state is reached.

The following chart demonstrates a breach of the primary limit, causing a primary event to occur. The operating envelope is set to minimum.



The following events are depicted in the graph:

1. Data is below the primary limit. A default state is reached, and a **default** event is raised.
2. Data is above the primary limit. A primary state is reached, and a **primary** event is raised.
3. Data is below the primary limit. A default state is reached, and a **default** event is raised.

Secondary State

There are several ways to reach the secondary state outcome, in the Process Variable Surveillance process:

- Secondary State Limit
- Secondary State Duration
- Secondary State Integration
- Secondary State Rolling Sum Total Duration
- Secondary State Rolling Sum Total Integration
- Secondary State Rolling Sum Total Breach Occurrences

You can choose to set one or more conditions to set the secondary state.

For example, a test may have a variable secondary limit defined, as well as configured variables for determining secondary state rolling sum breach occurrences.

Secondary State Limit

If the configured secondary limit is breached, a secondary event occurs, and a secondary state is reached.

The graph demonstrates a breach of the secondary limit (with an Operating Envelope of Maximum), causing a secondary event to occur.

The following events are depicted in the graph:

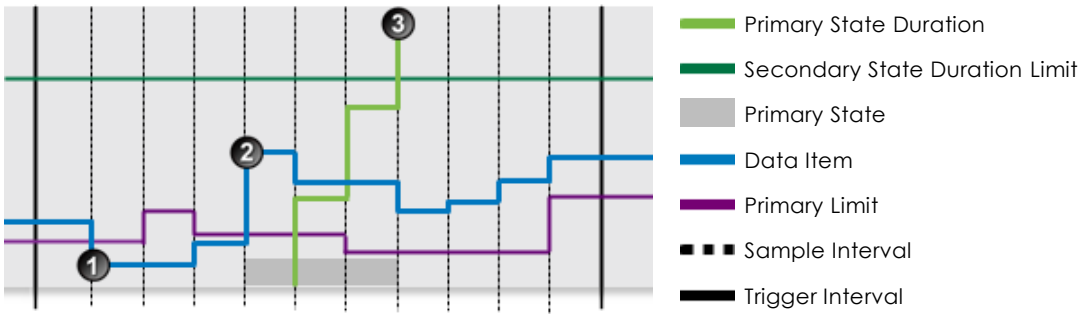
1. Data is below the primary limit. A default state is reached, and a **default** event is raised.
2. Data is above the primary limit. A primary state is reached, and a **primary** event is raised.
3. Data is above the secondary limit. A secondary state is reached, and a **secondary** event is raised.

Secondary State Duration

Monitor for a specified continuous duration of the primary state.

If the primary state endures for longer than specified in the secondary state duration limit, a secondary event occurs, and a secondary state is reached.

The graph demonstrates how the duration of the primary limit causes a secondary event to occur:



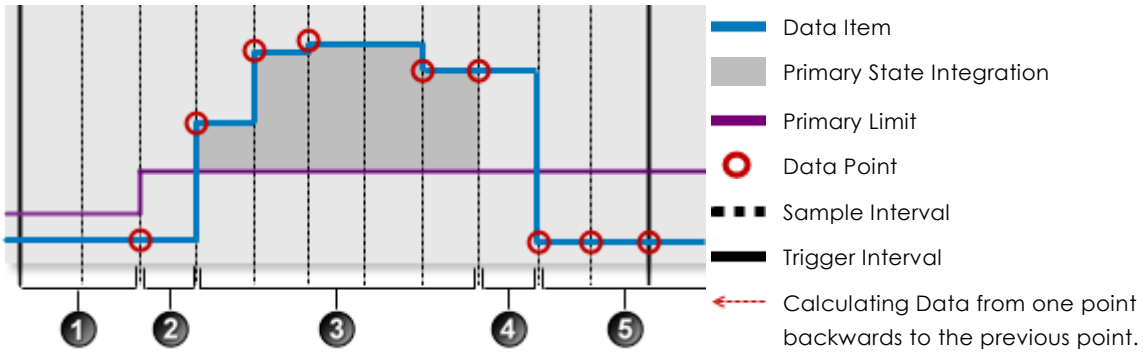
The following events are depicted in the graph:

1. Data is below the primary limit. A default state is reached, and a **default** event is raised.
2. Data is above the primary limit. A primary state is reached, and a **primary** event is raised.
3. The continuous primary state duration exceeds the secondary state duration limit. A secondary state is reached, and a **secondary** event is raised.

Secondary State Integration

Monitor the data integral (from the primary limit as a base) while data is continuously in the primary state, for transgression against a configured limit.

The integral is calculated as the area under the data line, between a data point and its preceding data point if both data points are above the primary limit, as shown in the diagram below:

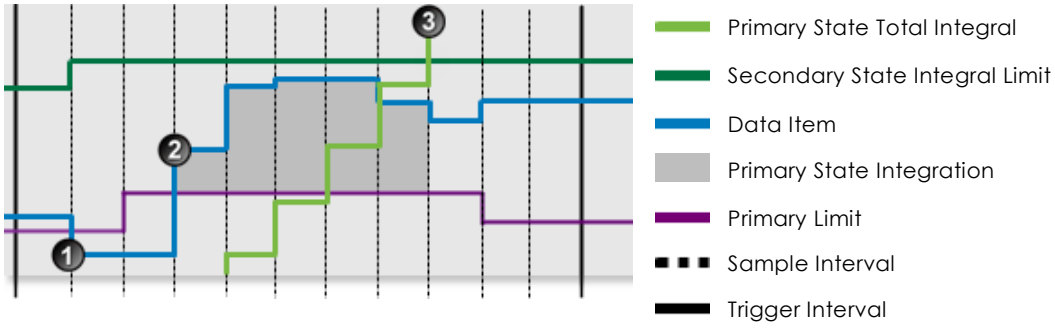


An explanation of whether or not the different segments are used in integration.

1. Data points in this segment fall below the primary limit, therefore there is no integration.
2. The first data point in this segment falls below the primary limit, therefore there is no integration.
3. In this segment, data points and their respective preceding data points are above the primary limit, therefore there is integration.
4. For this segment, the data point is below the primary limit, even though its preceding data point is above the limit, therefore there is no integration.
5. All data points in this segment fall below the primary limit, therefore there is no integration.

If the integral exceeds the configured secondary state integration value, a secondary event occurs, and a secondary state is reached.

The following graph demonstrates the ***data integral exceeding the secondary state integral limit***.



The following events are depicted in the graph:

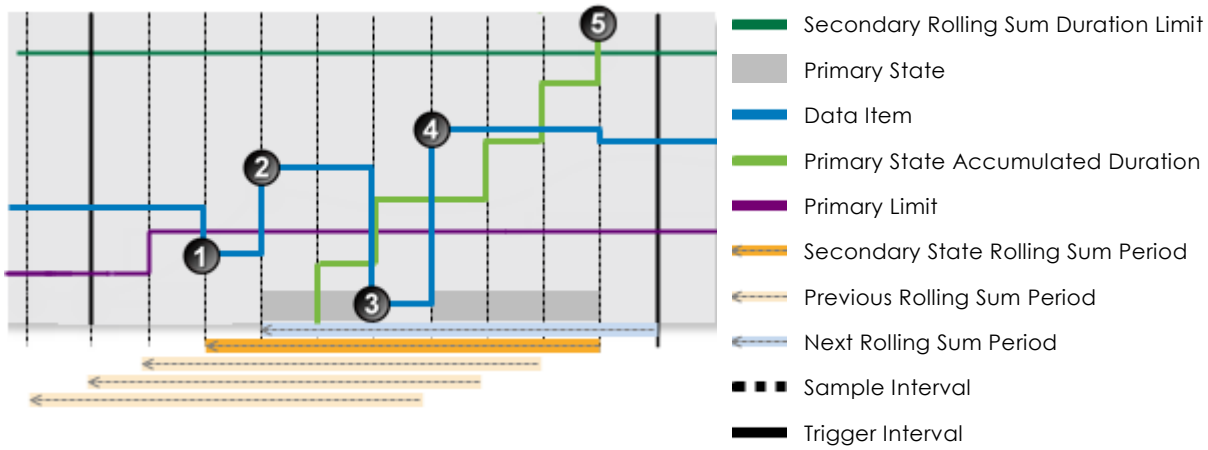
1. Data is below the primary limit. A default state is reached, and a **default** event is raised.
2. Data is above the primary limit. A primary state is reached, and a **primary** event is raised.
3. The total primary state integral exceeds the secondary state integration limit. A secondary state is reached, and a **secondary** event is raised.

Secondary State Rolling Sum Total Duration

Monitor for a specified accumulated duration of all periods of primary state within the preceding specified secondary state rolling sum period.

If the accumulated duration of all primary states within the rolling sum period is longer than the specified secondary state rolling sum total duration, a secondary event occurs, and a secondary state is reached. Note how each sample interval has its own rolling sum period.

The following chart demonstrates how a secondary state can be reached by secondary state rolling sum duration.



The following events are depicted in the graph:

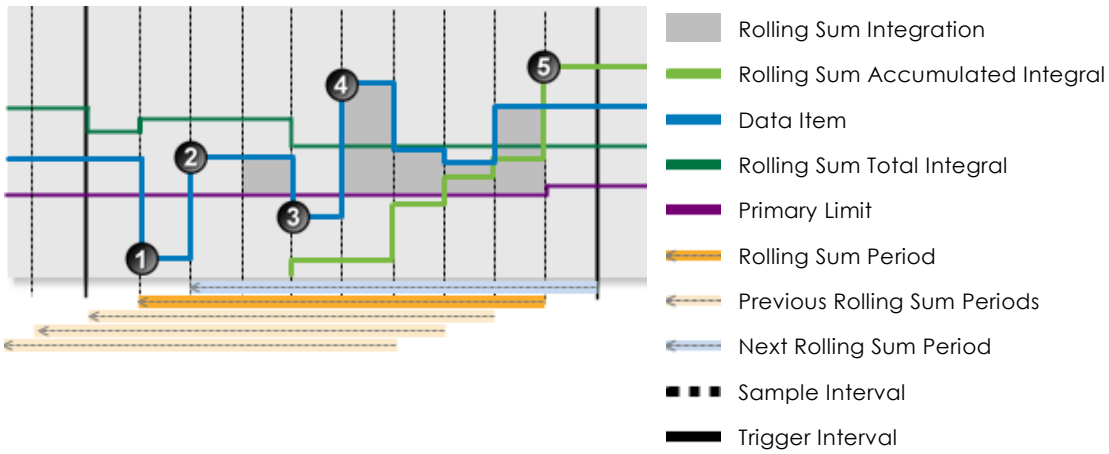
1. Data falls below the primary limit. A default state is reached, and a **default** event is raised.
2. The primary limit is exceeded. A primary state is reached, and a **primary** event is raised.
3. Data falls below the primary limit. A default state is reached, and a **default** event is raised.
4. The primary limit is exceeded. A primary state is reached, and a **primary** event is raised.
5. The rolling sum accumulated duration over this sample interval's preceding rolling sum period exceeds the rolling sum duration limit. A secondary state is reached, and a s**econdary** event is raised.

Secondary State Rolling Sum Total Integration

Monitor for a specified accumulated integration of all periods of primary state within the preceding specified secondary state rolling sum period.

The integral is calculated as the area under the data curve, where both data points are above the primary limit.

If the integral exceeds the configured secondary state rolling sum total integration value, a secondary event occurs, and a secondary state is reached.



The following events are depicted in the graph:

1. Data is below the primary limit. A default state is reached, and a **default** event is raised.
2. Data is above the primary limit. A primary state is reached, and a **primary** event is raised.
3. Data is below the primary limit. A default state is reached, and a **default** event is raised.
4. Data is above the primary limit. A primary state is reached, and a **primary** event is raised.
5. In the preceding secondary state rolling sum period, the secondary rolling sum accumulated integral exceeds the secondary state rolling sum total integral limit. A secondary state is reached, and a **secondary** event is raised.

Secondary State Rolling Sum Breach Occurrences

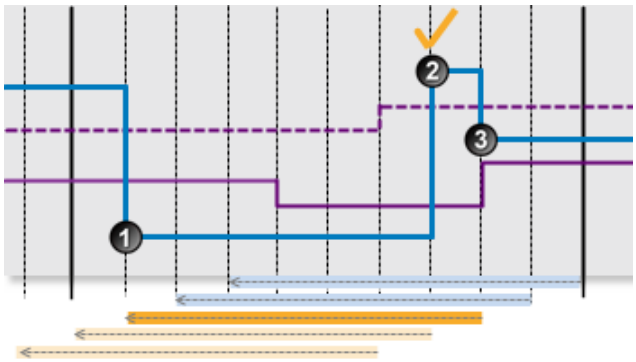
Monitor whether a set number of values has traversed the configured breach limit, during the preceding specified secondary state rolling sum period.

The process counts the number of times that the secondary state rolling sum breach limit is breached within a secondary state rolling sum period. If this number is equal to the secondary state rolling sum breach occurrences number, and if the current state is primary, a secondary event occurs, and a secondary state is reached.

The following events are depicted in the graph:

1. Data is below the primary limit. A default state is reached, and a **default** event is raised.
2. Data is above the primary limit. A primary state is reached, and a **primary** event is raised.
3. Data has traversed the breach limit three times during the preceding rolling sum period. In this example, the secondary state breach occurrences is set to 3. Thus, a secondary state is reached, and a **secondary** event is raised.

The following scenario demonstrates how the current value of the data item does not need to be over the secondary state breach limit in order for the secondary state to be triggered.



- Breach Occurrences Counter
- Data Item
- Secondary State Breach limit
- Primary Limit
- Rolling Sum Period
- Previous Rolling Sum Periods
- Next Rolling Sum Periods
- Sample Interval
- Trigger Interval

The following events are depicted in the graph:

1. Data is below the primary limit. A default State is reached, and a **default** event is raised.
2. Data is above the secondary state breach limit. In this example, secondary state breach occurrences is set to 1. Because the current state is default and the data is over the primary limit, a primary state is reached, and a **primary** event is raised. This follows the State Transition Rules, whereby the state cannot transition from default to secondary.
3. Data has traversed the breach limit once during the preceding rolling sum period. In this example, secondary state breach occurrences is set to 1.

   Thus, a secondary state is reached, and a **secondary** event is raised, even though the data is currently below the secondary state breach limit. The transition from primary state to secondary state is allowable according to the state transition rules.

Tertiary State

There are several ways to reach the tertiary state outcome, in the Process Variable Surveillance process:

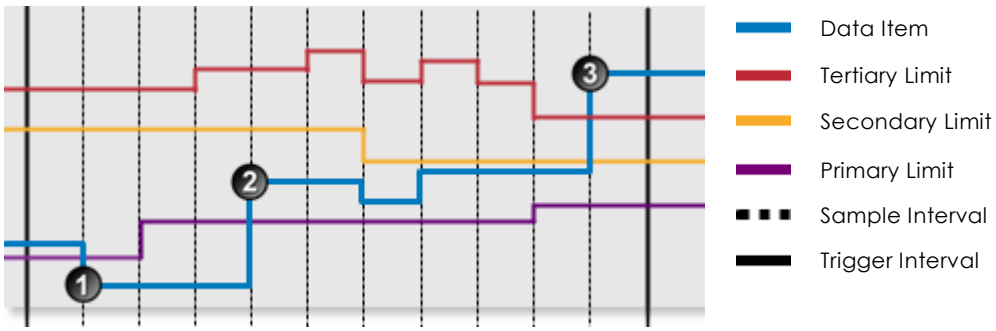
- Tertiary State Limit
- Tertiary State Duration
- Tertiary State Integration
- Tertiary State Rolling Sum Total Duration
- Tertiary State Rolling Sum Total Integration
- Tertiary State Rolling Sum Total Breach Occurrences

Depending on the complexity required, you can set one or more conditions to set the tertiary state. For example, a test may have a variable tertiary limit defined, as well as configured variables for determining tertiary state rolling sum breach occurrences.

Tertiary State Limit

If the configured tertiary limit is breached, a tertiary event occurs, and a tertiary state is reached.

The following chart demonstrates a breach of the tertiary limit (with an Operating Envelope of Maximum), causing a tertiary event to occur:



The following events are depicted in the graph:

1. Data is below the primary limit. A default state is reached, and a **default** event is raised.
2. Data is above the primary limit. A primary state is reached, and a **primary** event is raised.
3. Data is above the tertiary limit. A tertiary state is reached, and a **tertiary** event is raised.

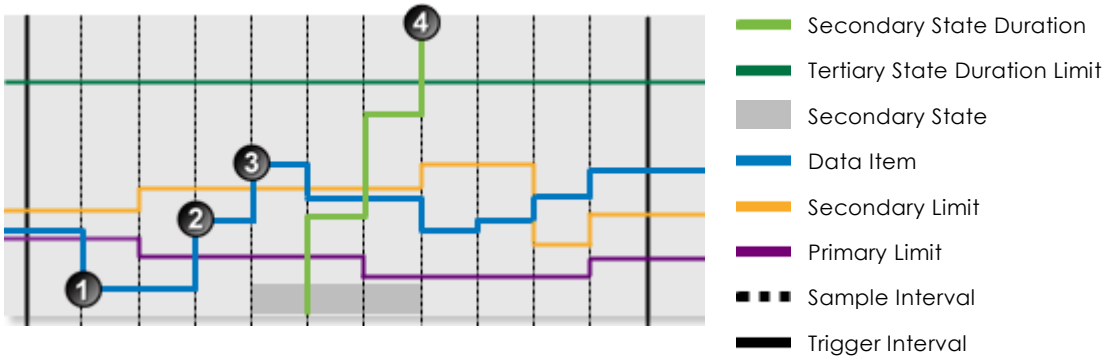
Note: In this example, the state has transitioned from primary to tertiary. This transition is allowed when the tertiary limit has been breached, according to the State Transition Rules.

Tertiary State Duration

Monitor for a specified continuous duration of the secondary state.

If the secondary state endures for longer than specified in the tertiary state duration limit, a tertiary event occurs and a tertiary state is reached.

The following graph demonstrates how the duration of the secondary state causes a tertiary event to occur:



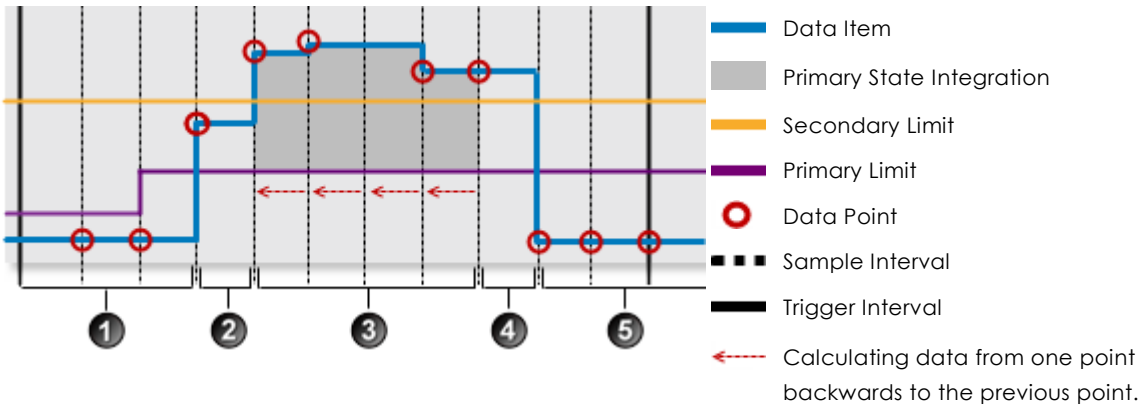
The following events are depicted in the graph:

1. Data is below the primary limit. A default state is reached, and a **default** event is raised.
2. Data is above the primary limit. A primary state is reached, and a **primary** event is raised.
3. Data is above the secondary limit. A secondary state is reached, and a **secondary** event is raised.
4. The continuous secondary state duration exceeds the tertiary state duration limit. A tertiary state is reached, and a **tertiary** event is raised.

Tertiary State Integration

Monitor the data integral (from the primary limit as a base) while data is continuously in the secondary state, for transgression against a configured limit.

The integral is calculated as the area under the data line, only if both data points are in a secondary state, as shown in the diagram below:

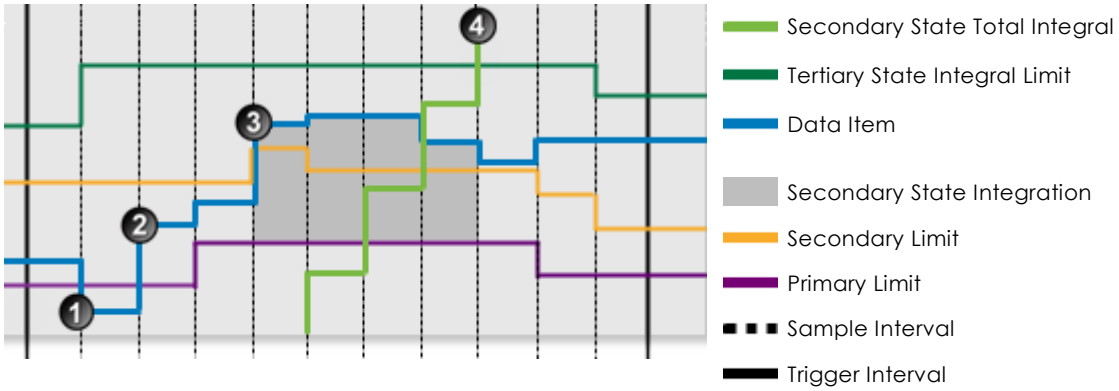


An explanation of whether or not the different segment are used in integration.

1. Data points in this segment fall below the secondary limit, therefore there is no integration.
2. The first data point in this segment falls below the secondary limit, therefore there is no integration.
3. In this segment, data points and their respective preceding data points are above the secondary limit, therefore there is integration (calculated from the primary limit as a base).
4. For this segment, the data point is below the primary limit, even though its preceding data point is above the limit, therefore there is no integration.
5. All data points in this segment fall below the primary limit, therefore there is no integration.

If the integral exceeds the configured tertiary state integration value, a tertiary event occurs and a tertiary state is reached.

The following graph demonstrates the data integral exceeding the tertiary state integral limit.



The following events are depicted in the graph:

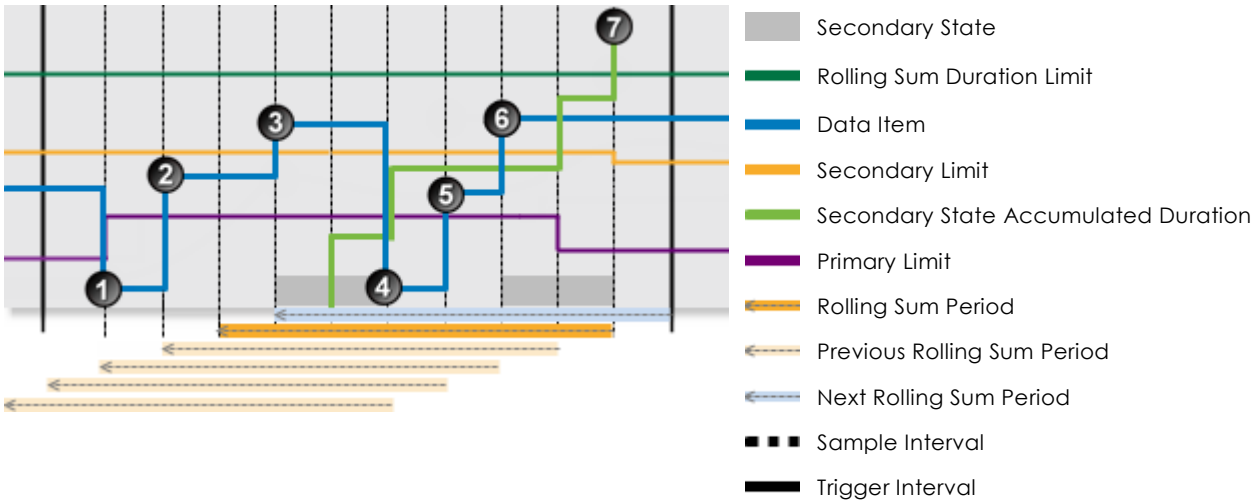
1. Data is below the primary limit. A default state is reached, and a **default** event is raised.
2. Data is above the primary limit. A primary state is reached, and a **primary** event is raised.
3. Data is above the secondary limit. A secondary state is reached, and a **secondary** event is raised.
4. The total secondary state integral exceeds the secondary state integration limit. A tertiary state is reached, and a **tertiary** event is raised.

Tertiary State Rolling Sum Total Duration

Monitor for a specified accumulated duration of all periods of secondary state within the preceding specified tertiary state rolling sum period.

If the accumulated duration of all secondary states within the rolling sum period is longer than specified in the tertiary state rolling sum total duration, a tertiary event occurs and a tertiary state is reached. Note how each sample interval has its own rolling sum period.

The following graph demonstrates how a tertiary state can be reached by tertiary state rolling sum duration.



The following events are depicted in the graph:

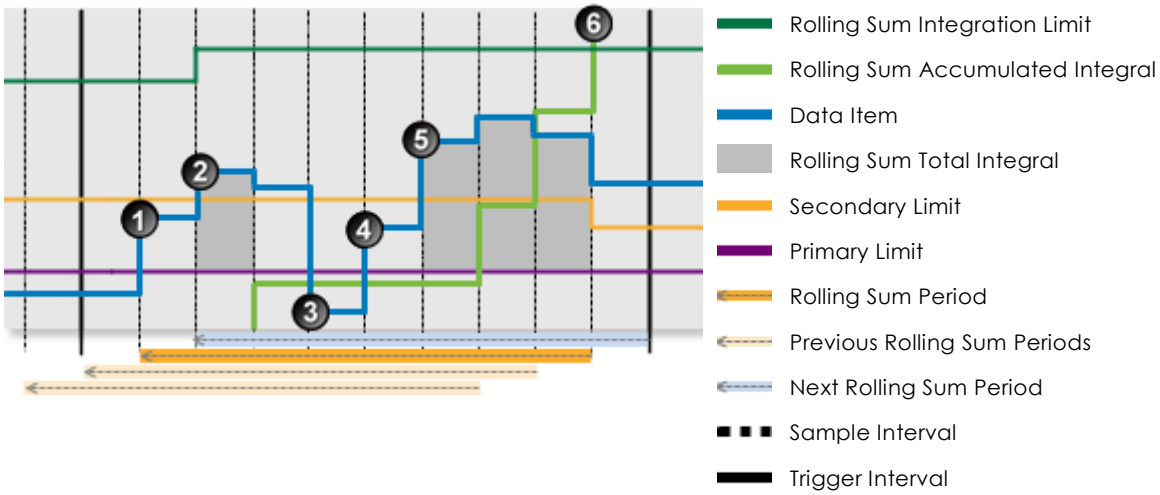
1. Data is below the primary limit. A default state is reached, and a **default** event is raised.
2. The primary limit is exceeded. A primary state is reached, and a **primary** event is raised.
3. The secondary limit is exceeded. A secondary state is reached, and a **secondary** event is raised.
4. Data is below the primary limit. A default state is reached, and a **default** event is raised.
5. The primary limit is exceeded. A primary state is reached, and a **primary** event is raised.
6. The secondary limit is exceeded. A secondary state is reached, and a **secondary** event is raised.
7. The rolling sum accumulated duration over this sample interval's preceding rolling sum period exceeds the rolling sum duration limit. A tertiary State is reached, and a **tertiary** event is raised.

Tertiary State Rolling Sum Total Integration

Monitor for a specified accumulated integration of all periods of secondary state within the preceding specified secondary state rolling sum period.

The integral is calculated as the area under the data curve, for periods of secondary state.

If the integral exceeds the configured tertiary state rolling sum total integration value, a tertiary event occurs and a tertiary state is reached.



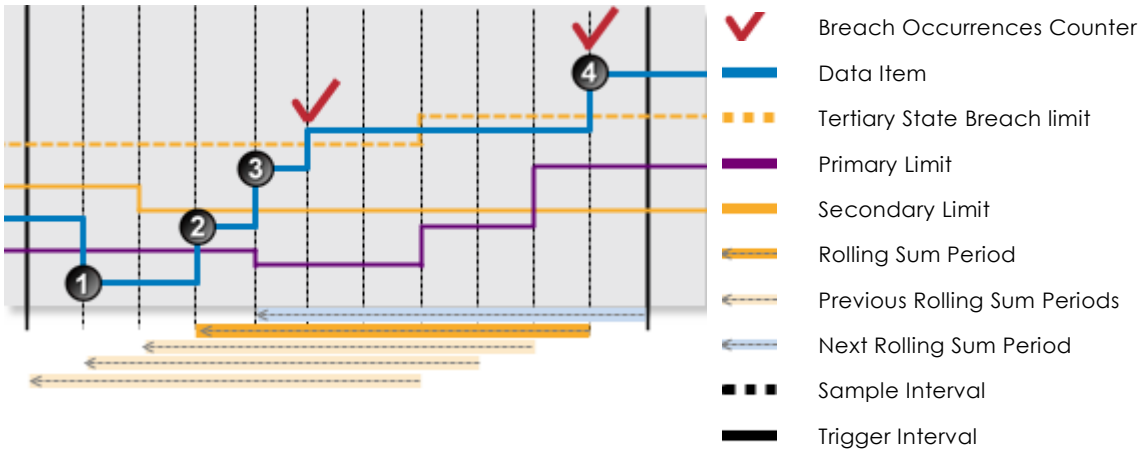
The following events are depicted in the graph:

1. Data is above the primary limit. A primary state is reached, and a **primary** event is raised.
2. Data is above the secondary limit. A secondary state is reached, and a **secondary** event is raised. The integral is calculated from this point, until the state changes again.
3. Data is below the primary limit. A default state is reached, and a default event is raised.
4. Data is above the primary limit. A primary state is reached, and a **primary** event is raised.
5. Data is above the secondary limit. A secondary state is reached, and a **secondary** event is raised. The integral is calculated from this point, until the state changes again.
6. In the preceding tertiary state rolling sum period, the tertiary rolling sum accumulated integral exceeds the tertiary state rolling sum total integral limit. A tertiary state is reached, and a **tertiary** event is raised.

Tertiary State Rolling Sum Breach Occurrences

Monitor whether a set number of values has traversed the configured breach limit, during the preceding specified tertiary state rolling sum period.

Counts the number of times that the tertiary state rolling sum breach limit is breached within a tertiary state rolling sum period. If this number is equal to the tertiary state rolling sum breach occurrences number, and if the current state is secondary, a tertiary event occurs and a tertiary state is reached.



The following events are depicted in the graph:

1. Data is below the primary limit. A default state is reached, and a **default** event is raised.
2. Data is above the primary limit. A primary state is reached, and a **primary** event is raised.
3. Data is above the secondary limit. A secondary state is reached, and a **secondary** event is raised.
4. Data has traversed the breach limit twice during the preceding rolling sum period. In this example, the tertiary state breach occurrences is set to 2. Thus, a tertiary state is reached, and a **tertiary** event is raised.

Additional Scenarios

This section describes scenarios that are more complex than the ones previously shown. The Process Variable Surveillance process is capable of assessing multiple conditions, whilst still following the state transition rules.

Multiple Ways to Reach a State

This example demonstrates how a secondary state is reached in 3 different ways:

- Secondary State Limit
- Secondary State Duration
- Secondary State Rolling Sum Breach Occurrences

The conditions are configured as follows:

PRIMARY STATE

Operating Envelope

Maximum is selected.

Primary State Limit

A fixed limit, set at 35.

SECONDARY STATE

Secondary State Limit

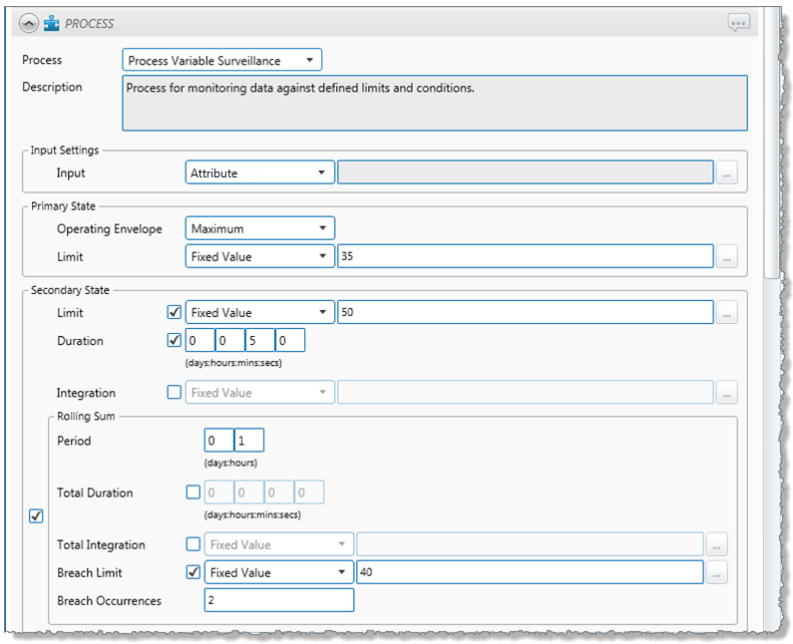
A fixed secondary state limit is set at 50.

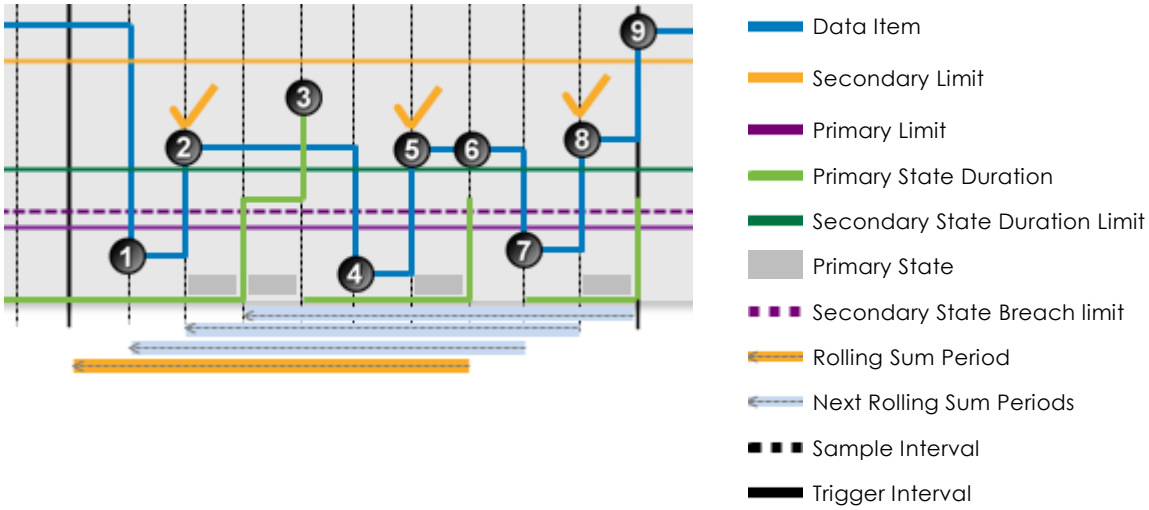
Secondary State Duration

A fixed secondary state duration limit is set at 5 minutes.

Secondary State Rolling Sum Breach Occurrences

- Rolling Sum Period is set at 1 hour.
- A fixed breach limit is set at 40.
- Breach occurrences is set to 2.



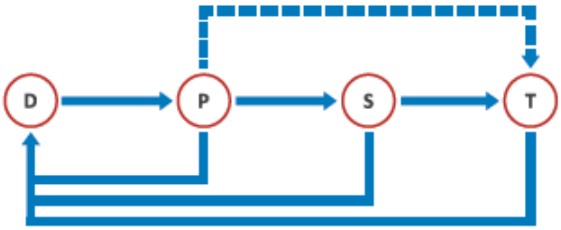


The following events are depicted in the graph:

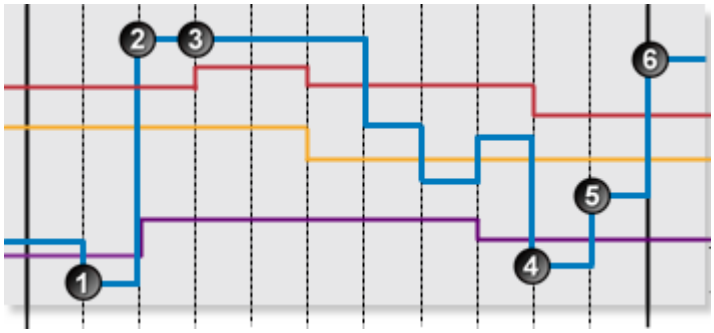
1. Data is below the primary limit. A default state is reached, and a **default** event is raised.
2. Data is above the primary limit. A primary state is reached, and a **primary** event is raised.
3. The continuous primary state duration exceeds the secondary state duration limit. A secondary state is reached, and a **secondary** event is raised.
4. Data is below the primary limit. A default state is reached, and a **default** event is raised.
5. Data is above the primary limit. A primary state is reached, and a **primary** event is raised.
6. Data has traversed the breach limit twice during the preceding rolling sum period. In this example, the Secondary State Breach Occurrences value is set to 2. Thus, a secondary state is reached, and a **secondary** event is raised.
7. Data is below the primary limit. A default state is reached, and a **default** event is raised.
8. Data is above the primary limit. A primary state is reached, and a **primary** event is raised.
9. Data is above the secondary limit. A secondary state is reached, and a **secondary** event is raised.

Demonstrating Allowable State Changes

The following graph shows how states cannot change unless the State Transition Rules are followed.



The graph demonstrates a breach of the secondary limit (with an Operating Envelope of Maximum), causing a secondary event to occur:



Data Item
Tertiary Limit
Secondary Limit
Primary Limit
Sample Interval
Trigger Interval

The following events are depicted in the graph:	State transition rule affecting state outcome:
1 Data is below the primary limit. A default state is reached, and a **default** event is raised.	Any state can move to the default state.
2 Data is above the tertiary limit. A primary state is reached, and a **primary** event is raised.	Default to tertiary is not allowed. Default can transition to the primary state.
3 Data is above the tertiary limit. A tertiary state is reached, and a **tertiary** event is raised. Note that the data has not changed, but a new state is reached at this interval.	Transition from primary state to tertiary state is allowed where the tertiary limit is in breach (and for no other conditions).
At the next few sample intervals, there are no events, and the tertiary state persists.	A state cannot move to a lower state, unless it moves to a default state.
4 Data is below the primary limit. A default state is reached, and a **default** event is raised.	Any state can transition to the default state.
5 Data is above the primary limit. A primary state is reached, and a **primary** event is raised.	Transition from default state to primary state is allowed.
6 Data is above the tertiary limit. A tertiary state is reached, and a **tertiary** event is raised.	Transition from primary state to tertiary state is allowed where the tertiary limit is in breach (and for no other conditions).

Adding a Process Variable Surveillance Process

The Process Variable Surveillance Process compares process variable data against defined limits and conditions. If a limit or condition is breached when the process is executed, a new state is reached and an event is raised.

Setting Process Limits

Part of setting up the Process Variable Surveillance process involves selecting limits, such as the primary limit, secondary state limit, tertiary limit, breach limits and so on. Limits can either be fixed values, or they can be variable data taken from P2 Server entities.

The following limits are available. Select a limit type from the drop-down list, then type in or select a limit.

Fixed Value
Type in a numerical value.

Source Tag
This option is only available if the **Source Type** is **Tag**.

Attribute
This option is only available if the test's **Source Type** is **Entity** or **Hierarchy**.

Click the ellipsis button to open the P2 Server Attribute Picker, to select an attribute of the source entities.

Calculation
Click the ellipsis button to open the *Edit Calculation* window. The expression is resolved in the P2 Server calculation engine.

If the Source Type is Entity or Hierarchy:
Type a calculation, prefixed by 'this' as the **Source Entity** token, for example: **{this:THP} + 34**.

If the Source Type is Tag:
Type a calculation, prefixed by 'this' as the **Source Tag** token, for example: **{this} * 2**.

Tag
Click the ellipsis button to open the *P2 Server Browser* to select a tag.

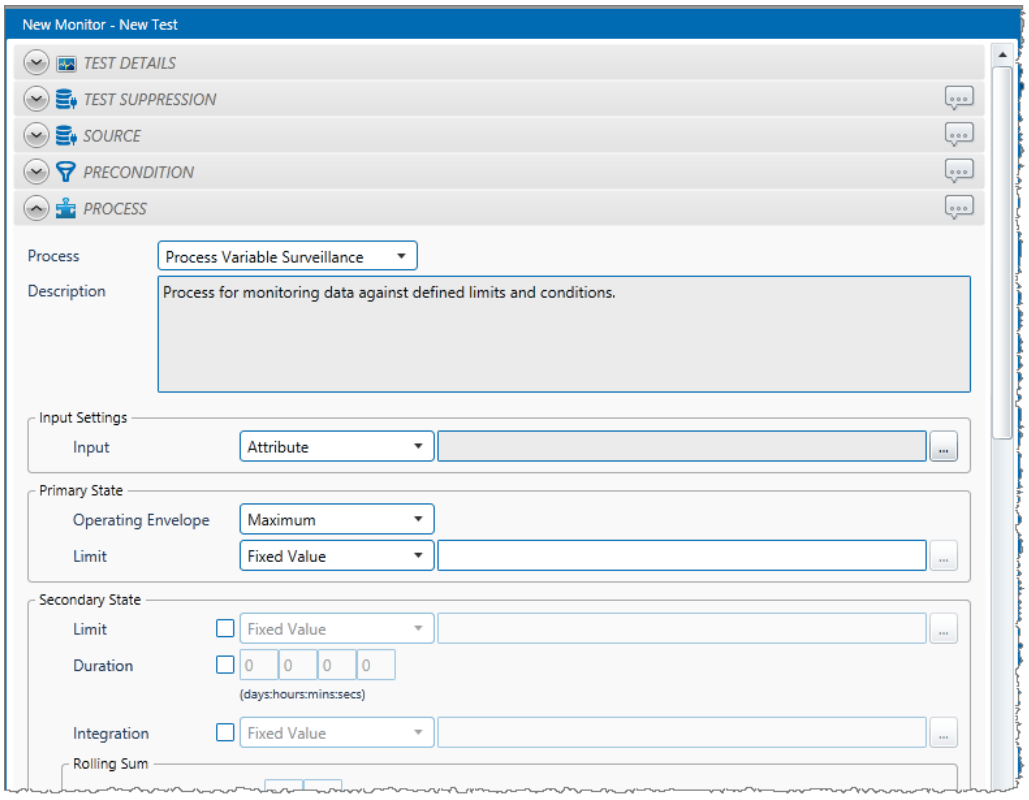
Entity Attribute
Click the ellipsis button to open the *P2 Server Browser* to select an entity. From here, select a P2 Server attribute, or attribute value, by using the P2 Server Attribute Picker for the selected entity.

Adding the Process

In the Sentinel **Test** page:

1. Expand the **Process** panel.

2. Select **Process Variable Surveillance** from the drop-down list.



3. From the **Input** drop-down list, select an input from the following:

Attribute
This option is only available if the **Source Type** is **Entity** or **Hierarchy**.

Click the ellipsis button to select an attribute by using the P2 Server Attribute Picker. You are limited to selecting an attribute of the test source monitor items. This attribute of each of the monitor items is a separate process input.

Source Tag
This option is only available if the **Source Type** is **Tag**.

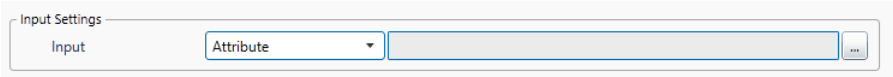
If you select this option, then each of the tag monitor items is used as separate process input.

Calculation
Click the ellipsis button to open the *Edit Calculation* window. The expression is resolved in the P2 Server calculation engine.

If the Source Type is Entity or Hierarchy:
Type a calculation, prefixed by 'this' as the **Source Entity** token, for example: **{this:THP} + 34**.

If the Source Type is Tag:
Type a calculation, prefixed by 'this' as the **Source Tag** token, for example: **{this} * 2**.

Entity Attribute
Click the ellipsis button to open the *P2 Server Browser* to select an entity. From here, select a P2 Server attribute, or attribute value, by using *the* P2 Server Attribute Picker for the selected entity.



4. Define the *Primary State* limits and conditions.

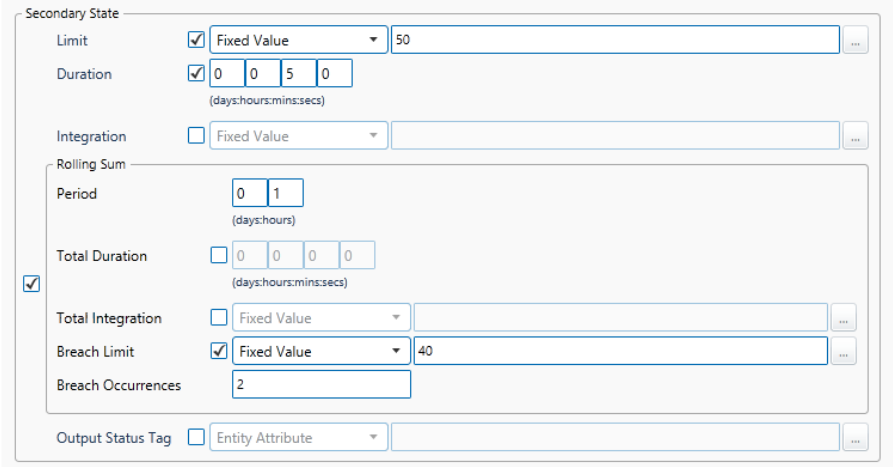
a. Select an Operating Envelope (Maximum or Minimum) from the drop-down list.

b. Specify a Limit in the drop-down list and the text box (see "**Setting Process Limits**", above).

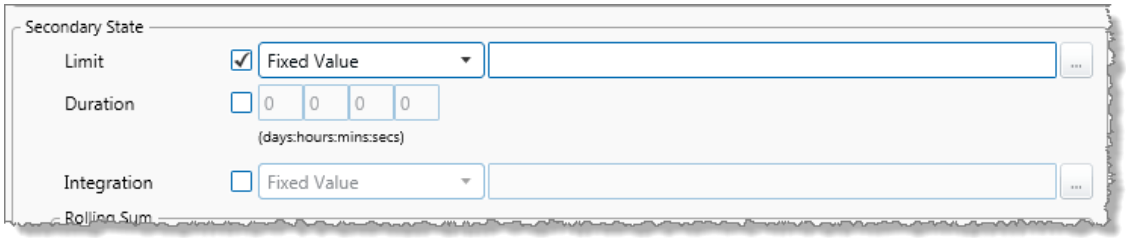
5. Define the Secondary State limits and conditions, in the **Secondary State** panel of the process.

Secondary State Limits and Conditions that can be set:

- Secondary State Limit
- Secondary State Duration
- Secondary State Integration
- Secondary State Rolling Sum Period
- Secondary State Rolling Sum Total Duration
- Secondary State Rolling Sum Total Integration
- Secondary State Rolling Sum Breach Occurrences



To select a Secondary State Limit:



a. Select the **Limit** check box.

b. Specify the **Limit** in the drop-down list and the text box (see "**Setting Process Limits**", above).

To set a Secondary State Duration:

1.1 Select the **Duration** check box.

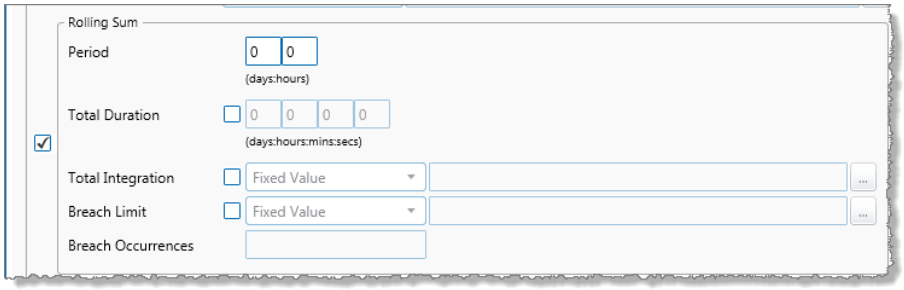
c. Type integer values in the **days**, **hours**, **mins** (minutes), and **secs** (seconds) **Duration** boxes to define a duration period. The default value is zero.

To set a Secondary State Integration:

1.2 Select the **Integration** check box.

d. Specify the **Integration** limit in the drop-down list and the text box (see "**Setting Process Limits**", above).

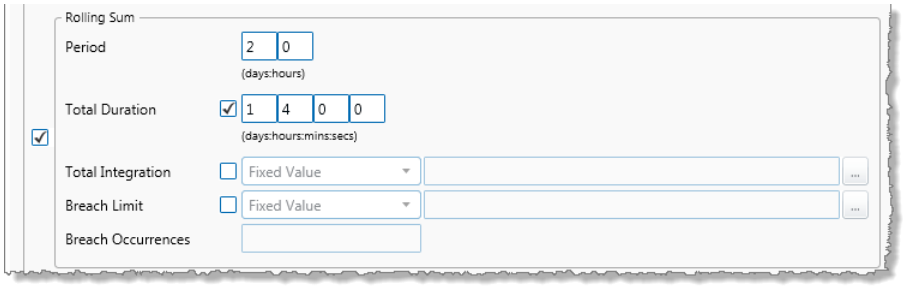
To set Secondary State Rolling Sum conditions:



e. Select the **Rolling Sum** check box (to the left of the *Rolling Sum* panel).

f. Type integer values in the **days** and **hours** boxes to define the secondary state Rolling Sum **Period**.

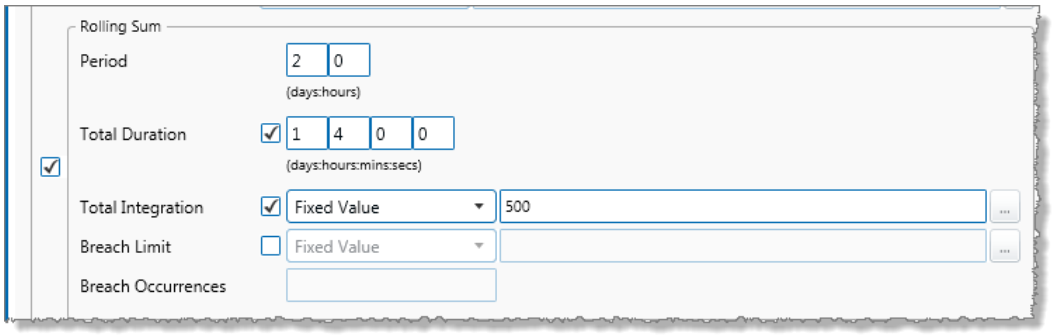
To set a Secondary State Rolling Sum Total Duration:



1.2.1 Select the **Total Duration** check box.

i. Type integer values in the **days**, **hours**, **mins** (minutes), and **secs** (seconds) in the **Total Duration** boxes to define the *total duration* period. The default value is zero.

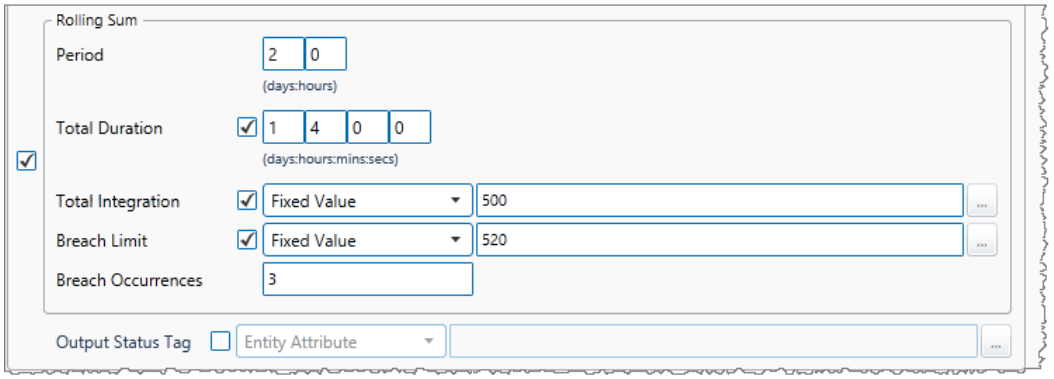
To set a Secondary State Rolling Sum Total Integration:



1.2.2 Select the **Total Integration** check box.

ii. Specify the **Total Integration** limit in the drop-down list and the text box (see "**Setting Process Limits**", above).

To configure Secondary State Rolling Sum Breach Occurrences:

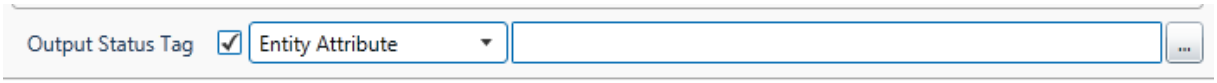


1.2.3 Select the **Breach Limit** check box.

iii. Specify the Breach Limit in the drop-down list and the text box.

iv. In the **Breach Occurrences** text box, type the number of breach occurrences.

To set the Secondary State Output Status Tag:



g. Select the **Output Status Tag** check box.

h. From the drop-down list, select the output from the following:

Attribute
This option is only available if the test's **Source Type** is **Entity** or **Hierarchy**.

Click the ellipsis [...] button to open the P2 Server Attribute Picker, to select an attribute of the source entities.

Tag
Click the ellipsis [...] button to open the *P2 Server Browser* to select a tag.

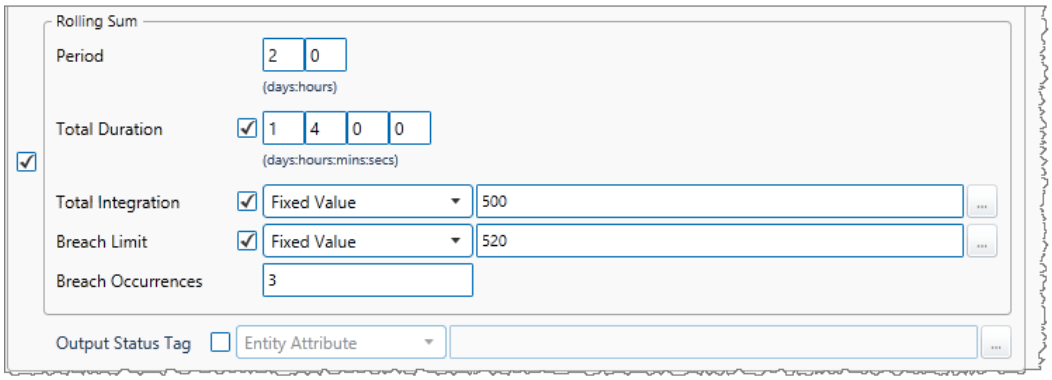
Entity Attribute

Click the ellipsis button to open the *P2 Server Browser* to select an entity. From here, select a P2 Server attribute, or attribute value, by using the P2 Server Attribute Picker for the selected entity.

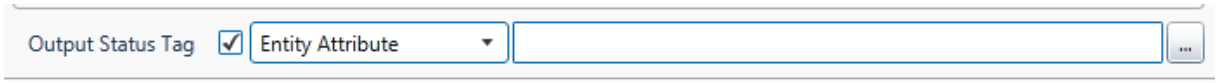
6. Define the Tertiary State limits and conditions, in the **Tertiary State** panel of the process. The limits and conditions can be added in the same way as for Secondary state.

   Tertiary State Limits and Conditions that can be set:

   - Tertiary State Limit
   - Tertiary State Duration
   - Tertiary State Integration
   - Tertiary State Rolling Sum Total Duration
   - Tertiary State Rolling Sum Total Integration
   - Tertiary State Rolling Sum Breach Occurrences



To set the Tertiary State Output Status Tag:



   a. Select the **Output Status Tag** check box.

   b. From the drop-down list, select the output from the following:

Attribute

This option is only available if the test's **Source Type** is **Entity** or **Hierarchy**.

Click the ellipsis button to open the P2 Server Attribute Picker, to select an attribute of the source entities.

Tag

Click the ellipsis button to open the *P2 Server Browser* to select a tag.

Entity Attribute

Click the ellipsis button to open the *P2 Server Browser* to select an entity. From here, select a P2 Server attribute, or attribute value, by using the P2 Server Attribute Picker for the selected entity.

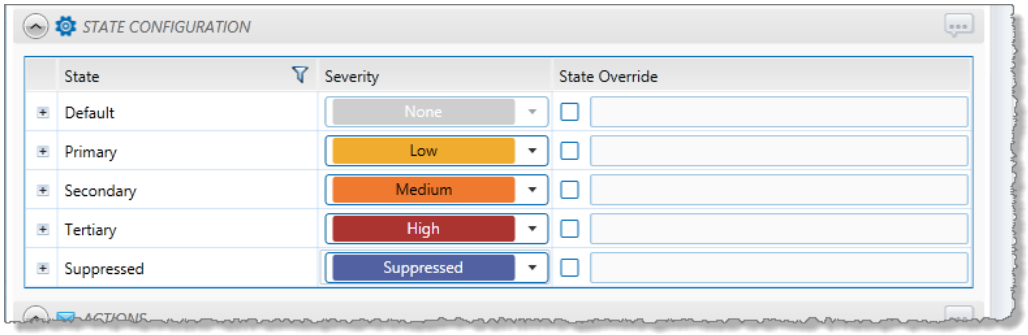
7. To add comments to the process panel click the comment button, at the top right of the panel.

Configuring States

For the Process Variable Surveillance process, you can configure the following states, each with an optional state override and comments:

- Primary
- Secondary
- Tertiary
- Suppressed

You cannot change the severity of the Default state; however, you can add a state override and comments.



Note: Only configure states where you have set a limit.

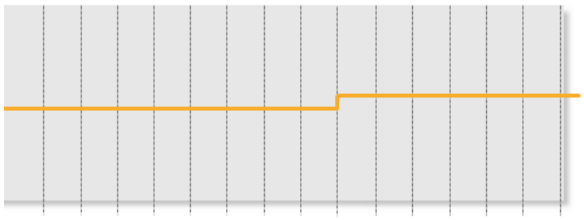
To configure the state outcomes for a test in the **State Configuration** panel of the test, see 3.6 Configure States. If Case Management is enabled in Sentinel, this is also where you manage cases.

Appendix F. Drift Detection Process

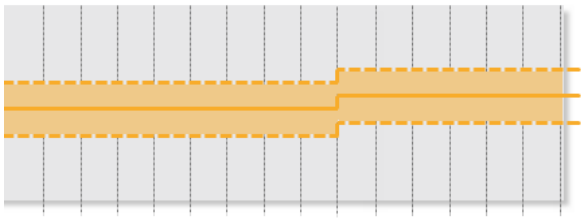
The Drift Detection Process monitors the deviation between process variable data (inputs) and a reference input. The reference input can either be a fixed value, or it can be a dynamic value such as a P2 Server entity.

A primary deviation limit is applied to the reference input, as either a percentage value or an absolute value. This limit can be an upper limit, a lower limit, or both, forming a deviation band. In the same way, secondary and tertiary limits may be applied to the reference input, to raise secondary or tertiary states, respectively.

Upper and Lower Primary deviation Limits are Created

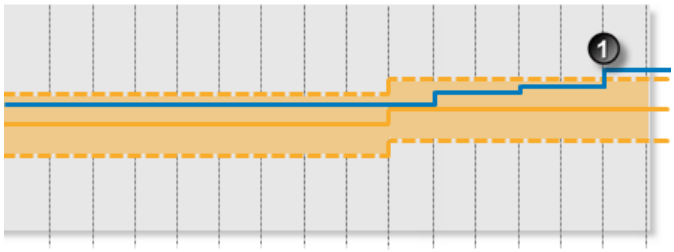


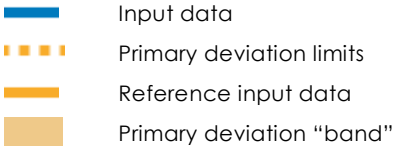
The reference input data shown over several sample intervals ■ ■ ■ .



Using an ***Absolute Value*** deviation mode, a primary deviation "band" is created. ***Upper*** and ***Lower*** deviations are used in this example.

Input Data is Evaluated against Upper and Lower Primary deviation Limits





Input data is evaluated against the primary deviation limits at every sample interval.

1 A **primary** event is raised when data exceeds the limit.

As well as detecting data that breaches the primary, secondary and tertiary deviation limits (raising a primary, secondary or tertiary state, respectively), the drift detection process has a variety of option methods for raising a secondary or tertiary event.

The Drift Detection process can measure duration above the primary limit, and also the number of data points above the primary limit. These measurements can be taken consecutively, or they can be summed in total over the preceding rolling sum period.

The Drift Detection process is used for monitoring the deviation between a reference input and the test input. Unacceptable deviations may signify equipment failure or calibration errors.

Drift Detection is a complex process capable of concurrently monitoring multiple conditions such as transgression of limits, state duration, and movement between states.

State Transition Rules

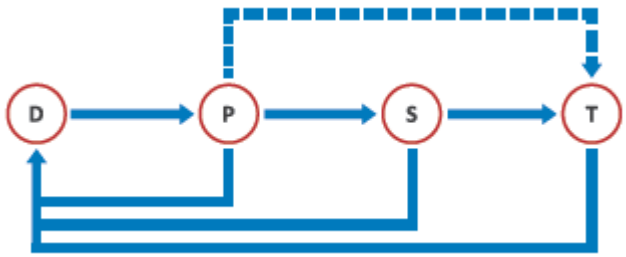
The Drift Detection process has clearly defined state transition logic paths. Transition from one state to another is equally dependant on the current evaluation of data, and on the current state.

State transitions cause events to be raised, allowing for the escalation of actions via the Sentinel framework. Different actions can be assigned to different state outcomes.

The following table outlines the allowable state transitions of the Drift Detection process.

This state can transition	To this state	Under these conditions
Default	Primary	Data has transgressed the primary state upper or lower deviation limits.
Primary	Secondary	Any one of the secondary state conditions have been met.
	Tertiary	Only if the tertiary deviation limit is breached.
	Default	Data is not erroneous, and is within the deviation limits of the curve.
Secondary	Tertiary	Any one of the tertiary state conditions has been met.
	Default	Data is not erroneous, and is within the deviation limits of the curve.
Tertiary	Default	Data is not erroneous, and is within the deviation limits of the curve.

The following diagram outlines the state transition logic of the Drift Detection process.



D Default

P Primary

S Secondary

T Tertiary

Test Outcomes

A number of outcomes are possible when the Drift Detection process is executed:

Default State

Data is not in an erroneous state and is within the primary deviation limits.

Primary State

Data is measured against the defined fixed or variable primary deviation limit (upper and/or lower). If it breaches a primary deviation limit, a primary state is reached, and a primary event is raised.

Secondary State

A number of possible conditions can cause a secondary event, leading to a secondary state. These are explained in more detail in the Secondary State section.

TERTIARY STATE

As with the secondary state, a number of conditions can cause a tertiary event. These are explained in more detail in the Tertiary State section.

SUPPRESSED STATE

The monitor has been suppressed. For example, if the precondition has not been met.

Conditional Logic

The Drift Detection process provides the following conditional logic.

Note: All of the example graphs in the following sections show tests that have used the Last Known Value sample method.

Input Settings

The input and the reference input are defined in this section.

Input

The input is the data that is monitored. Input data is defined as an attribute of the source entity, either as it is, or as part of a calculation.

Reference Input

The fixed or variable *reference input* is used to create deviation limits for the input data.

The process will calculate limits around the reference input based on the deviation mode and the deviation limit settings, and then compare the input data stream to this model in order to determine drift.

Mode Settings

Define whether the deviation mode is a percentage or an absolute value, to establish how primary, secondary and tertiary deviation limits are calculated. Also select whether to set upper or lower deviation limits, or both.

Deviation Limit Settings

The primary state deviation limit must be set for the process to work. If the calculated primary state deviation limit is breached, a primary event occurs, and a primary state is reached. Optionally, a secondary state deviation limit and a tertiary state deviation limit may be set for the process.

The Rolling Sum Period

A secondary state rolling sum period can be defined for evaluating some of the secondary state conditions; likewise, a tertiary state rolling sum period can be defined for evaluating some of the tertiary state conditions.

The rolling sum period is a defined period (specified in days and hours). At every sample interval, the rolling sum period is that period preceding the sample interval. So, for example, if the secondary state rolling sum period is set at 1 day 2 hours then at 3pm on Tuesday 15 January 2013, the secondary state rolling sum period is from 1pm on Monday 14 January (covering the last 1 day

and 2 hours). Any evaluations relating to that sample interval's secondary state rolling sum period conditions must fall within that time.

Primary State Deviation Limit

The primary state deviation limit must be set for the process to work.

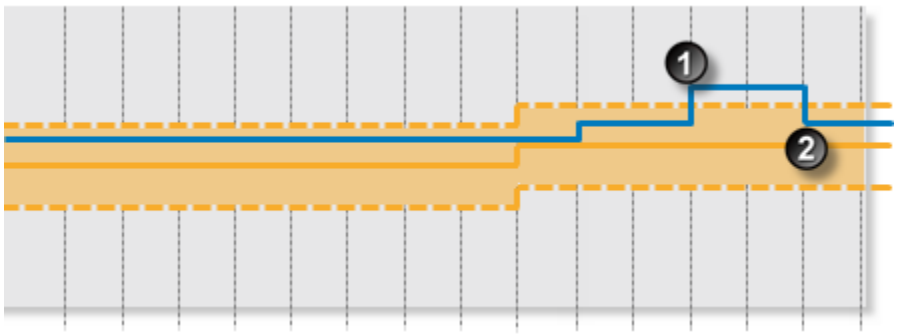
If the configured primary state deviation limit is breached, a primary event occurs, and a primary state is reached.

Example of Primary State Deviation Limit

In this example, a primary event is raised when the input data breaches the upper primary deviation limit.

- *The sample interval is one hour*.

Data item
Upper and lower primary deviation limits
Sample interval



1 At **5:00am**, the input data exceeds the upper primary deviation limit. A primary state is reached, and a **primary** event is raised.

2 At **7:00am**, the input data drops below the upper primary deviation limit. A default state is reached, and a **default** event is raised.

Secondary State

There are several possible ways to reach the secondary state outcome in the Drift Detection process:

- Secondary State Deviation Limit
- Secondary State Duration Limit
- Secondary State Sustained Value Limit
- Secondary State Rolling Sum Total Duration Limit
- Secondary State Rolling Sum Breach Occurrences Limit

You can choose to set one or more conditions to trigger the secondary state. For example, a test may have a secondary deviation limit defined, as well as configured variables for determining secondary state rolling sum breach occurrences.

Secondary State Deviation Limit

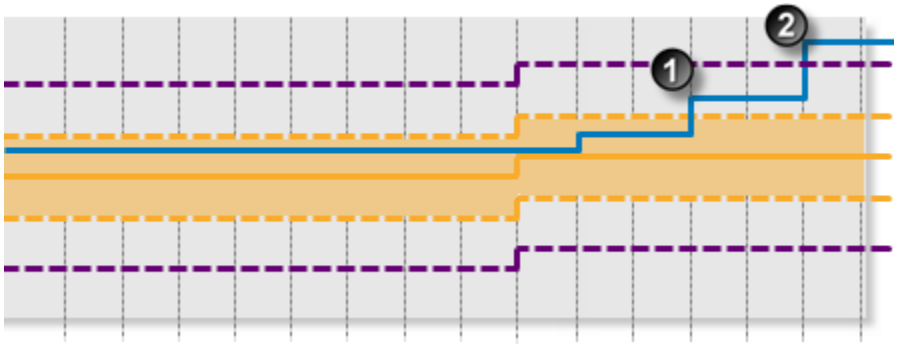
If the configured secondary deviation limit is breached, a secondary event occurs, and a secondary state is reached.

Example of Secondary State Deviation Limit

In this example, a secondary event is raised when the input data breaches the upper secondary deviation limit.

- *The sample interval is one hour.*

Data item
Sample interval
Upper and lower primary deviation limits
Upper and lower secondary deviation limits



1 At **5:00am**, the input data exceeds the upper primary deviation limit. A primary state is reached, and a **primary** event is raised.

2 At **7:00am**, the input data exceeds the upper secondary deviation limit. A secondary state is reached, and a **secondary** event is raised.

Secondary State Duration Limit

Monitor for data that continuously exceeds the primary deviation limit, for longer than the secondary state duration limit.

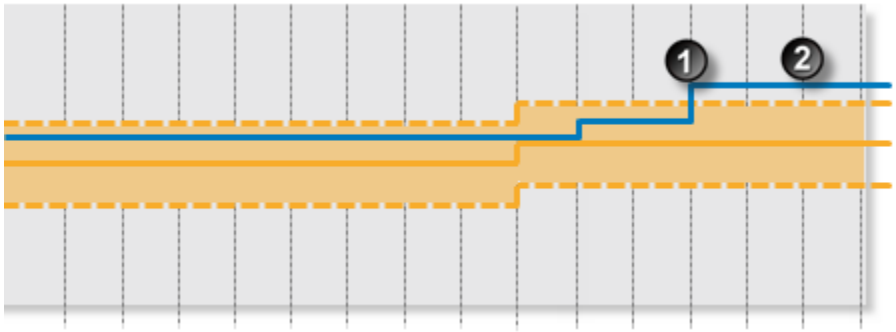
If data that continuously exceeds the primary deviation limit for longer than specified in the secondary state duration limit, a secondary event occurs, and a secondary state is reached.

Example of Secondary State Duration Limit

In this example, a secondary event is raised when the input data has exceeded the upper primary deviation limit for a period of 2 hours, exceeding the primary state duration limit of 1.5 hours.

- Secondary state duration limit is 1.5 hours.
- *The sample interval is one hour.*

Data item
Upper and lower primary deviation limits
Sample interval



1 At **5:00am**, the input data exceeds the upper primary deviation limit. A primary state is reached, and a **primary** event is raised.

2 At **7:00am**, the input data is still above the upper deviation limit. The duration of data above the upper deviation limits is 2 hours, exceeding the 1.5 hour secondary duration limit. A secondary state is reached, and a **secondary** event is raised.

Secondary State Sustained Value Limit

Monitor for when data exceeds the primary deviation limit for more than a specified number of times (secondary state, sustained value limit), consecutively. When this happens, a secondary event occurs, and a secondary state is reached.

Example of Secondary State Sustained Value Limit

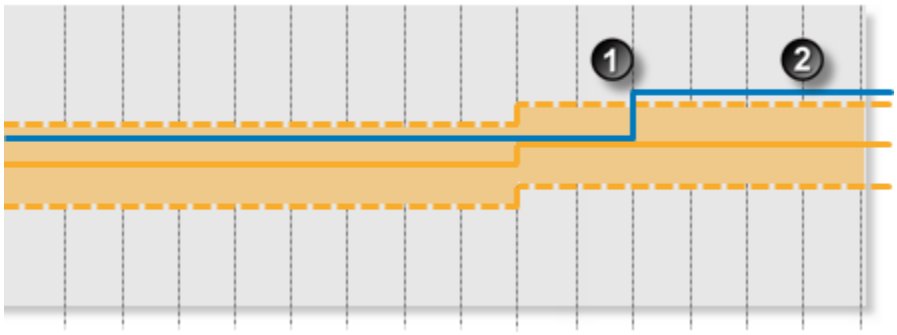
In this example, a secondary event is raised when the input data has exceeded the upper deviation limit, consecutively, for four sample intervals, exceeding the secondary state sustained value limit of three.

- Secondary state sustained value limit is 3.
- *The sample interval is one hour.*

Data item

Upper and lower primary deviation limits

Sample interval



1 At **5:00am**, the input data exceeds the upper primary deviation limit. A primary state is reached, and a **primary** event is raised.

2 At **8:00am**, the input data has exceeded the upper deviation limit for four sample intervals, consecutively, exceeding the secondary state sustained value limit of three. A secondary state is reached, and a **secondary** event is raised.

Secondary State Rolling Sum Total Duration Limit

Monitor for a specified accumulated duration of all periods where data is in breach of the primary deviation limit, within the preceding specified secondary state rolling sum period.

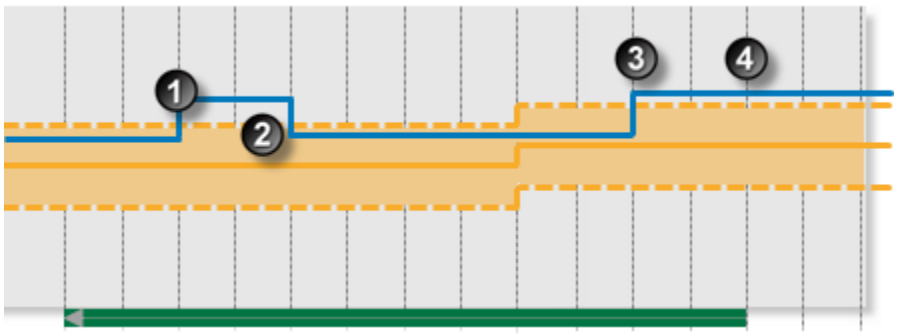
If the total combined primary state duration is longer than the specified secondary state rolling sum duration limit, a secondary event occurs, and a secondary state is reached.

Example of Secondary State Rolling Sum Total Duration Limit

In this example, a secondary event is raised when the input data is above the primary deviation limit for a total of four hours during the current secondary state rolling sum period, exceeding the secondary state rolling sum duration limit of 3.5 hours.

- Secondary state rolling sum total duration is 3.5 hours.
- Secondary state rolling sum period is 12 hours.
- *The sample interval is one hour.*

Data Item	Upper and lower primary deviation limits
Sample Interval	Current secondary state rolling sum period.



1 At **2:00am**, the input data exceeds the upper primary deviation limit. A primary state is reached, and a **primary** event is raised.

2 At **4:00am**, the input data drops below the upper primary deviation limit. A default state is reached, and a **default** event is raised.

The total duration of primary state for the current rolling sum period is 2 hours (two sample intervals). Timing stops while in the default state.

3 At **10:00am**, the input data exceeds the upper primary deviation limit. A primary state is reached, and a **primary** event is raised. Timing resumes.

4 At **12:00pm**, the combined total duration of primary state for the current rolling sum period is now 4 hours, exceeding the secondary state rolling sum duration limit. A secondary state is reached, and a **secondary** event is raised.

Secondary State Rolling Sum Breach Occurrences Limit

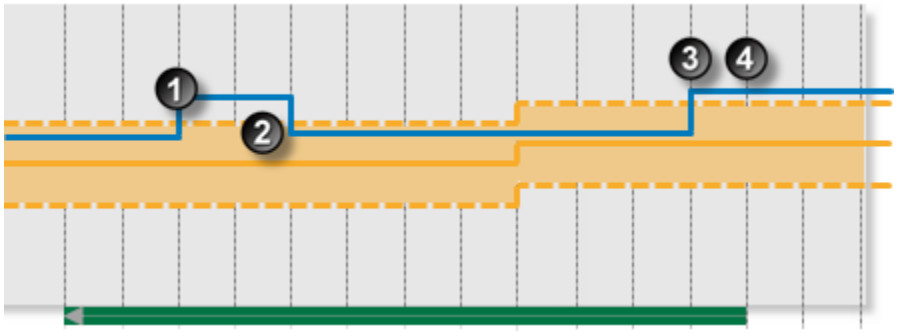
Monitor for when a set number of values (secondary state breach occurrences limit) has breached the primary deviation limit, during the preceding specified secondary rolling sum period.

Example of Secondary State Rolling Sum Breach Occurrences Limit

In this example, a secondary event is raised when the input data has breached the primary deviation limit three times in the current secondary state rolling sum period, reaching the secondary state rolling sum breach occurrences limit of three.

- Secondary state breach occurrences limit is 3.
- Secondary state rolling sum period is 12 hours.
- *The sample interval is one hour*.

Data item
Sample interval
Occurrence Counter
Upper and lower primary deviation limits
Current secondary state rolling sum period.



1 At **2:00am**, the input data exceeds the upper primary deviation limit. A primary state is reached, and a **primary** event is raised.

1 At **2:00am**, the breach occurrences counter is one.

2 At **4:00am**, the input data drops below the upper primary deviation limit. A default state is reached, and a **default** event is raised.

1 At **4:00am**, the breach occurrences counter remains at one.

3 At **11:00am**, the input data exceeds the upper primary deviation limit. A primary state is reached, and a **primary** event is raised.

2 At **11:00am**, the breach occurrences counter is two.

3 4 At **12:00pm**, the primary deviation limit has been breached three times in the current rolling period, reaching the secondary state rolling sum breach occurrences limit. A secondary state is reached, and a **secondary** event is raised.

Tertiary State

There are several ways to reach the tertiary state outcome in the Drift Detection process:

- Tertiary State Deviation Limit
- Tertiary State Duration Limit
- Tertiary State Sustained Value Limit
- Tertiary State Rolling Sum Total Duration Limit
- Tertiary State Rolling Sum Breach Occurrences Limit

You can choose to set one or more conditions to trigger the tertiary state. For example, a test may have a tertiary deviation limit defined, as well as configured variables for determining tertiary state rolling sum breach occurrences.

Tertiary State Deviation Limit

If the configured tertiary deviation limit is breached, a tertiary event occurs, and a tertiary state is reached.

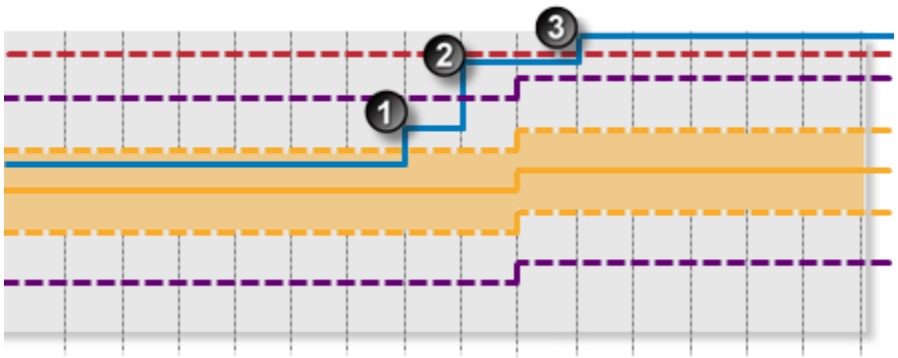
The graph demonstrates a breach of the tertiary deviation limit, causing a tertiary event to occur.

Example of Tertiary State Deviation Limit

In this example, a tertiary event is raised when the input data breaches the upper tertiary deviation limit.

- *The sample interval is one hour.*

Data item
Sample interval
Upper and lower primary deviation limits
Upper and lower secondary deviation limits
Upper and lower tertiary deviation limits



1 At **5:00am**, the input data exceeds the upper primary deviation limit. A primary state is reached, and a **primary** event is raised.

2 At **6:00am**, the input data exceeds the upper secondary deviation limit. A secondary state is reached, and a **secondary** event is raised.

3 At **8:00am**, the input data exceeds the upper tertiary deviation limit. A tertiary state is reached, and a **tertiary** event is raised.

Tertiary State Duration Limit

Monitor for data that continuously exceeds the primary deviation limit, for longer than the tertiary state duration limit.

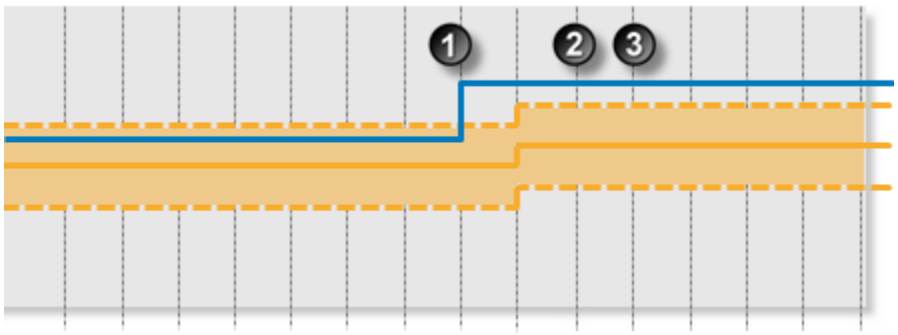
If data that continuously exceeds the primary deviation limit for longer than specified in the tertiary state duration limit, a tertiary event occurs, and a tertiary state is reached.

Example of Tertiary State Duration Limit

In this example, a tertiary event is raised when the input data has exceeded the upper primary deviation limit consecutively for a period of 3 hours, exceeding the tertiary state duration limit of 2.5 hours.

- Secondary state duration limit is 1.5 hours.
- Tertiary state duration limit is 2.5 hours.
- *The sample interval is one hour*.

Data item
Upper and lower primary deviation limits
Sample interval



1 At **5:00am**, the input data exceeds the upper primary deviation limit. A primary state is reached, and a **primary** event is raised.

2 At **7:00am**, the input data is still above the upper primary deviation limit. The duration of data above the primary limit is now 2 hours, exceeding the 1.5 hour secondary duration limit. A secondary state is reached, and a **secondary** event is raised.

3 At **8:00am**, the input data is still above the upper primary deviation limit. The duration of data above the primary limit is now 3 hours exceeding the 2.5 hour tertiary duration limit. A tertiary state is reached, and a **tertiary** event is raised.

Tertiary State Sustained Value Limit

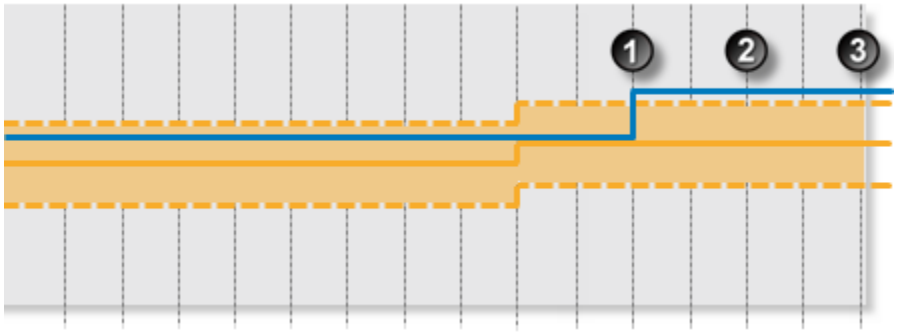
Monitor for when data exceeds the primary deviation limit for more than a specified number of times (tertiary state sustained value limit), consecutively. If this is the case, a tertiary event occurs, and a tertiary state is reached.

Example of Tertiary State Sustained Value Limit

In this example, a tertiary event is raised when the input data has exceeded the upper deviation limit for five sample intervals, consecutively, exceeding the tertiary state sustained value limit of four.

- Secondary state sustained value limit is 2.
- Tertiary state sustained value limit is 4.
- *The sample interval is one hour*.

Data item
Upper and lower primary deviation limits
Sample interval



1 At **5:00am**, the input data exceeds the upper primary deviation limit. A primary state is reached, and a **primary** event is raised.

2 At **7:00am**, the input data has exceeded the upper primary deviation limit for three sample intervals, exceeding the secondary state sustained value limit of two. A secondary state is reached, and a **secondary** event is raised.

3 At **9:00am**, the input data has exceeded the upper deviation limit for five sample intervals, exceeding the tertiary state sustained value limit of four. A tertiary state is reached, and a **tertiary** event is raised.

Tertiary State Rolling Sum Total Duration Limit

Monitor for a specified accumulated duration of all periods where data is in breach of the primary deviation limit, within the preceding specified tertiary state rolling sum period.

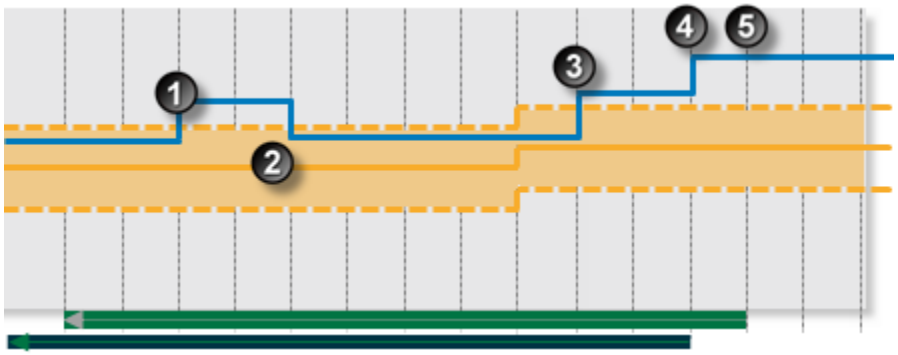
If the total combined primary state duration is longer than the specified tertiary state rolling sum duration limit, a tertiary event occurs, and a tertiary state is reached.

Example of Tertiary State Rolling Sum Total Duration Limit

In this example, the tertiary state rolling sum duration limit is exceeded, causing a tertiary event.

- Tertiary state rolling sum total duration is 3.5 hours.
- *The sample interval is one hour*.
- *Tertiary rolling sum period is 12*.

Data Item
Upper and lower primary deviation limits
Sample Interval
Current tertiary state rolling sum period
Previous sample interval's tertiary state rolling sum period



1 At **2:00am**, the input data exceeds the upper primary deviation limit. A primary state is reached, and a **primary** event is raised.

2 At **4:00am**, the input data drops below the upper primary deviation limit. A default state is reached, and a **default** event is raised.

The total duration of primary state for the current rolling sum period is 2 hours. Timing is paused.

3 At **9:00am**, the input data exceeds the upper primary deviation limit. A primary state is reached, and a **primary** event is raised. Timing resumes.

4 At **11:00am**, the combined total duration of data above the primary limit for the current rolling sum period is now 4 hours, exceeding the tertiary state rolling sum duration limit of 3.5 hours. A secondary state is reached, and a **secondary** event is raised. Note: The test outcome cannot go from primary state to tertiary state unless a tertiary deviation limit has been breached.

5 At **12:00pm**, the combined total duration of data above the primary limit for the current rolling sum period is now 5 hours, exceeding the tertiary state rolling sum duration limit of 3.5 hours. A tertiary state is reached, and a **tertiary** event is raised.

Tertiary State Rolling Sum Breach Occurrences Limit

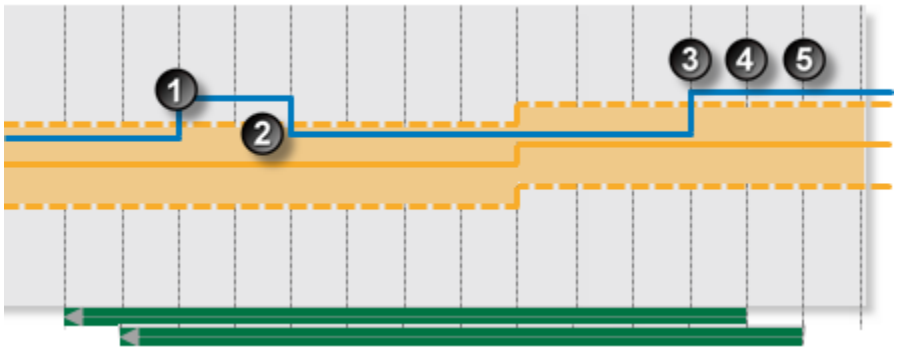
Monitor whether a set number of values (tertiary state breach occurrences limit) has breached the primary deviation limit, during the preceding specified tertiary rolling sum period.

Example of Tertiary State Rolling Sum Breach Occurrences Limit

In the following example, the tertiary state rolling sum breach occurrences limit is exceeded, causing a tertiary event. Note that a secondary state must be reached first.

- Tertiary state breach occurrences limit is three.
- *The sample interval is one hour.*
- *Tertiary rolling sum period is 12 hours.*

Data item	Upper and lower primary deviation limits
Sample interval	Tertiary state rolling sum period (12 hours).
Occurrence Counter	



2:00am	1 At **2:00am**, the input data exceeds the upper primary deviation limit. A primary state is reached, and a **primary** event is raised. 1 At **2:00am**, the breach occurrences counter is one.
4:00am	2 At **4:00am**, the input data drops below the upper primary deviation limit. A default state is reached, and a **default** event is raised. 1 At **4:00am**, the breach occurrences counter remains at one.
11:00am	3 At **11:00am**, the input data exceeds the upper primary deviation limit. A primary state is reached, and a **primary** event is raised. 2 At **11:00am**, the breach occurrences counter is two.
12:00pm	3 4 At **12:00pm**, the primary deviation limit has been breached three times in the current rolling sum period, reaching the tertiary state rolling sum breach occurrences limit. A secondary state is reached, and a **secondary** event is raised. Note: The test outcome cannot go from primary state to tertiary state unless a tertiary deviation limit has been breached.
1:00pm	4 5 At **1:00pm,** the primary deviation limit has been breached four times in the current rolling sum period, exceeding the tertiary state rolling sum breach occurrences limit. A tertiary state is reached, and a **tertiary** event is raised.

Adding a Drift Detection Process

The Drift Detection Process monitors the deviation between process variable data (inputs) and a reference input. If a limit or condition is breached when the process is executed, a new state is reached and an event is raised.

Setting Process Values and Limits

Part of setting up the Drift Detection process involves selecting limits, such as the primary state deviation limit, secondary state deviation limit, tertiary state deviation limit, breach occurrences limits and so on. Limits can either be fixed values, or they can be variable data taken from P2 Server entities.

The following limits are available. Select a limit type from the drop-down list, then type in or select a limit.

Fixed Value

Type in a numerical value.

Attribute

This option is only available if the test's **Source Type** is **Entity** or **Hierarchy**.

Click the ellipsis  button to open the P2 Server Attribute Picker, to select an attribute of the source entities.

Source Tag

This option is only available if the **Source Type** is **Tag**.

Calculation

Click the ellipsis  button to open the *Edit Calculation* window. The expression is resolved in the P2 Server calculation engine.

If the Source Type is Entity or Hierarchy:
Type a calculation, prefixed by 'this' as the **Source Entity** token, for example: **{this:THP} + 34**.

If the Source Type is Tag:
Type a calculation, prefixed by 'this' as the **Source Tag** token, for example: **{this} * 2**.

Tag

Click the ellipsis  button to open the *P2 Server Browser* to select a tag.

Entity Attribute

Click the ellipsis  button to open the *P2 Server Browser* to select an entity. From here, select a P2 Server attribute, or attribute value, by using the P2 Server Attribute Picker for the selected entity.

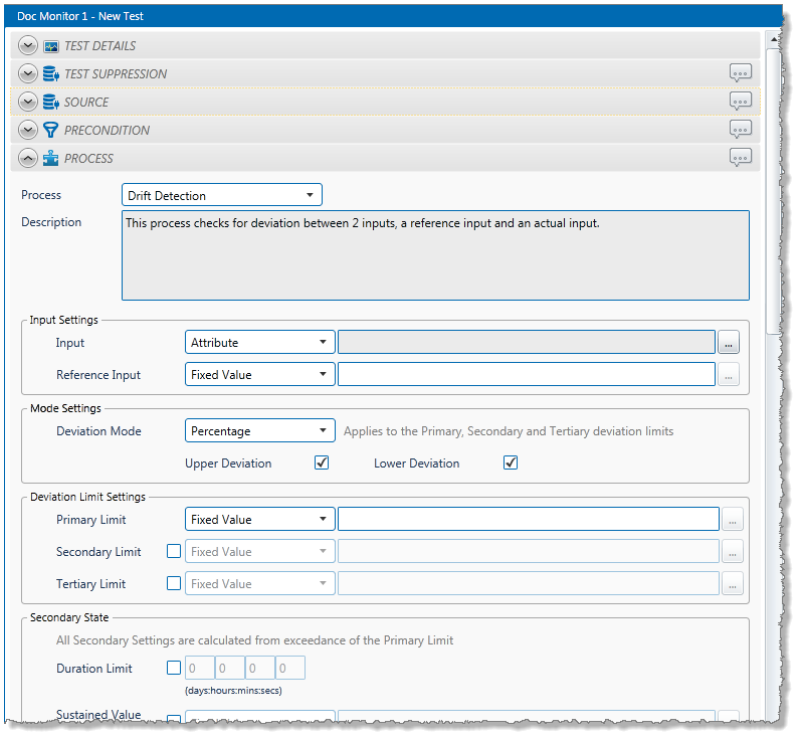
Adding the Process

As with all P2 Sentinel processes, the Drift Detection Process is defined within a Sentinel **Test** page.

Drift Detection Process

In the Sentinel **Test** page:

1. Expand the **Process** panel.
2. Select **Drift Detection** from the drop-down list.



Select Input Settings

1. From the **Input** drop-down list, select an input from the following:

Attribute
This option is only available if the **Source Type** is **Entity** or **Hierarchy**.

Click the ellipsis button to select an attribute by using the P2 Server Attribute Picker. You are limited to selecting an attribute of the test source monitor items. This attribute of each of the monitor items is a separate process input.

Source Tag
This option is only available if the **Source Type** is **Tag**.

Calculation
Click the ellipsis button to open the *Edit Calculation* window. The expression is resolved in the P2 Server calculation engine.

If the Source Type is Entity or Hierarchy:
Type a calculation, prefixed by 'this' as the **Source Entity** token, for example: **{this:THP} + 34**.

If the Source Type is Tag:
Type a calculation, prefixed by 'this' as the **Source Tag** token, for example: **{this} * 2**.

Entity Attribute

Click the ellipsis  button to open the *P2 Server Browser* to select an entity. From here, select a P2 Server attribute, or attribute value, by using *the* P2 Server Attribute Picker for the selected entity.

2. **From the Reference Input** drop-down list, select one of the following; then type in or select a corresponding value:

   - Fixed Value
   - Attribute (only available of the **Source** type is *Entity* or *Hierarchy*)
   - Source Tag (only available of the **Source** type is *Tag*)
   - Calculation
   - Tag
   - Entity Attribute

These different options are outlined above, in the section: "**Setting Process Values and Limits**", above.

Define the Mode Settings

Define whether the deviation mode is a percentage or an absolute value, to establish how primary, secondary and tertiary deviation limits are calculated. Also select whether to set upper or lower deviation limits, or both.

Note: The mode settings apply to primary, secondary and tertiary deviation limits.

1. From the **Deviation Mode** drop-down list, select *Percentage* or *Absolute Value*. The deviation mode determines how the deviation limits will be calculated.
2. Select the **Upper Deviation** check box to set an upper deviation limit.
3. Select the **Lower Deviation** check box to set a lower deviation limit.

Select Deviation Limit Settings

Note: The Primary Deviation Limit is mandatory for the Drift Detection Process.

1. From the **Primary Limit** drop-down list, select one of the following and then type in or select a corresponding value:

   - Fixed Value
   - Attribute (only available of the **Source** type is *Entity* or *Hierarchy*)
   - Source Tag (only available of the **Source** type is *Tag*)
   - Calculation
   - Tag
   - Entity Attribute

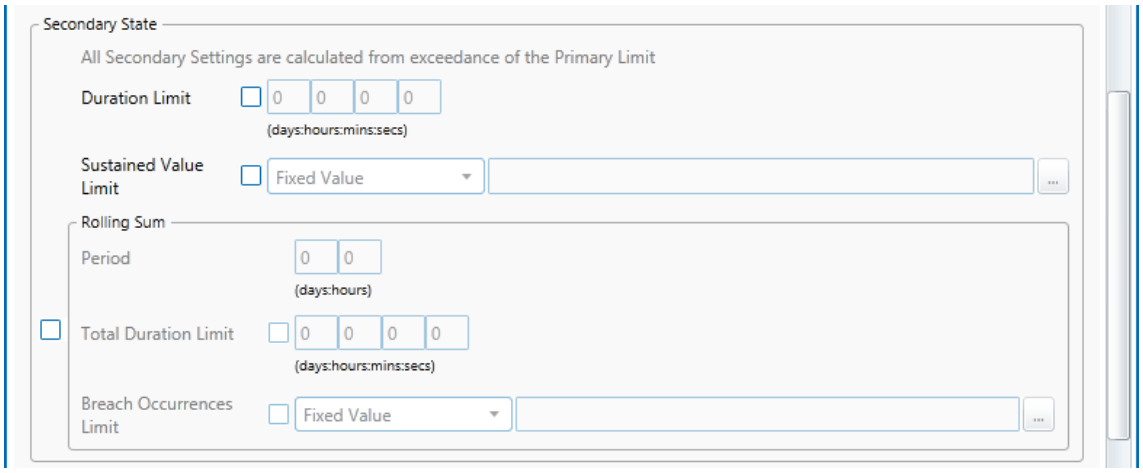
   These different options are outlined above, in the section: "**Setting Process Values and Limits**", above.

2. Optionally define secondary limits in the same way (first select the **Secondary Limit** check box).
3. Optionally define tertiary limits in the same way (first select the **Tertiary Limit** check box).

Select Secondary State Settings

Note: All Secondary State settings are calculated from the primary deviation limit.

All secondary state settings are captured or selected in the **Secondary State** section of the process, with the exception of the Secondary Deviation Limit, which is set in the **Deviation Limit Settings** section of the process.



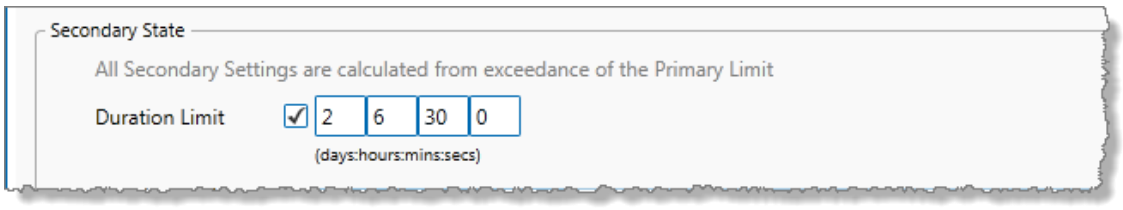
The Secondary State Section of the Process

Setting a Secondary State Duration Limit

The Secondary State Duration Limit is used for monitoring where data is continuously beyond the primary deviation limit, for longer than the specified secondary duration limit.

In the **Secondary State** section:

1. Select the **Duration Limit** check box.
2. Type integer values in the **days**, **hours**, **mins** (minutes), and **secs** (seconds) **Duration Limit** boxes to define a duration period. The default value is zero.



A Secondary State Duration of 2 Days, 6 Hours and 30 Minutes

Setting a Secondary State Sustained Value Limit

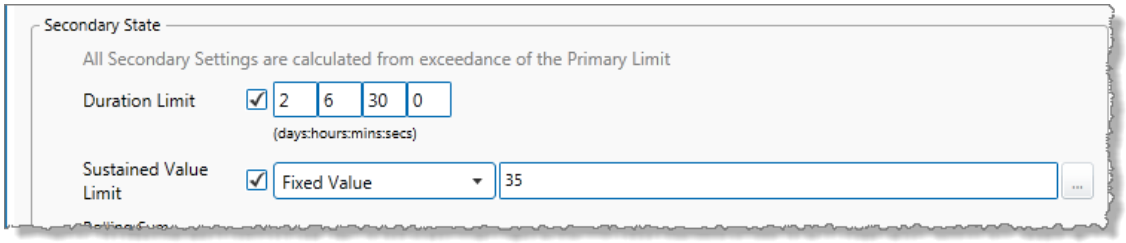
The Secondary State Sustained Value Limit is used for monitoring where data is beyond the primary deviation limit for more than a specified number of times (secondary state sustained value limit), consecutively.

In the **Secondary State** section:

1. Select the **Sustained Value Limit** check box.
2. From the **Sustained Value Limit** drop-down list, select one of the following and then type in or select a corresponding value:

- Fixed Value
- Attribute (only available of the **Source** type is *Entity* or *Hierarchy*)
- Source Tag (only available of the **Source** type is *Tag*)
- Calculation
- Tag
- Entity Attribute

These different options are outlined above, in the section: "**Setting Process Values and Limits**", above.



A Sustained Value Limit of 35 (Fixed Value)

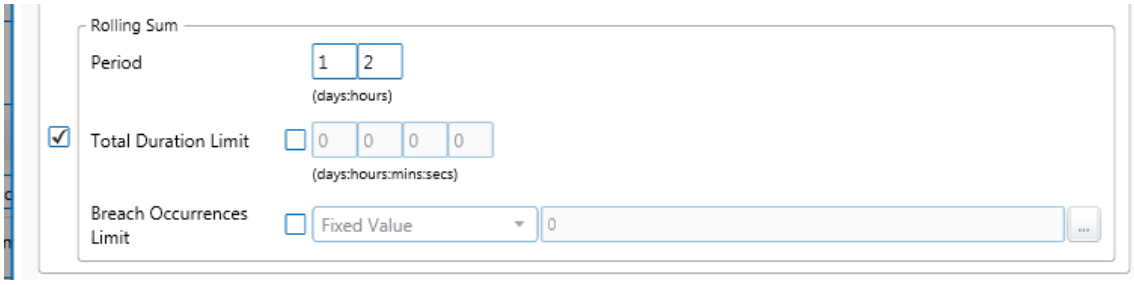
Setting a Secondary State Rolling Sum Period

The rolling sum period is a defined period (specified in days and hours). At every sample interval, the rolling sum period applies to that period preceding the sample interval.

Set a secondary state rolling sum period if you are going to define a Secondary State Total Duration Limit or a Secondary State Breach Occurrences Limit.

In the **Secondary State** section:

1. Select the check box to the left of the **Rolling Sum** section.
2. Type integer values in the **days** and **hours** *Period* boxes to define the rolling sum period.



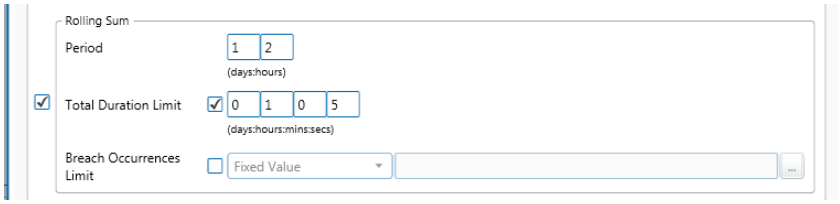
A Secondary State Rolling Sum Period of 1 Day and 2 Hours

Setting a Secondary State Rolling Sum Total Duration Limit

The Secondary State Rolling Sum Total Duration Limit is used to monitor for a specified accumulated duration of all periods where data is in breach of the primary deviation limit, within the preceding specified secondary state rolling sum period.

In the **Rolling Sum** section, within the **Secondary State** section:

1. Select the **Total Duration Limit** check box.
2. Type integer values in the **days**, **hours**, **mins** (minutes), and **secs** (seconds) **Total Duration Limit** boxes to define a total duration limit period. The default value is zero.



A Total Duration Limit of 1 Hour and 5 Seconds

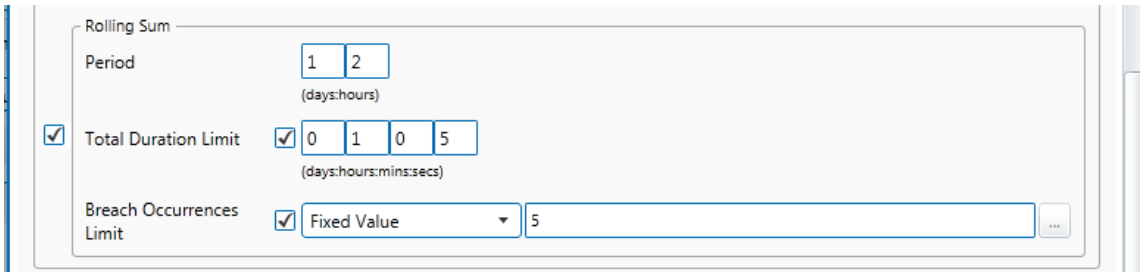
Setting a Secondary State Rolling Sum Breach Occurrences Limit

The Secondary State Rolling Sum Breach Occurrences Limit is used to monitor for when a set number of values (secondary state breach occurrences limit) has breached the primary deviation limit, during the preceding specified secondary state rolling sum period.

In the **Rolling Sum** section, within the **Secondary State** section:

1. Select the **Breach Occurrences Limit** check box.
2. From the **Breach Occurrences Limit** drop-down list, select one of the following and then type in or select a corresponding value:
   - Fixed Value
   - Attribute (only available of the **Source** type is *Entity* or *Hierarchy*)
   - Source Tag (only available of the **Source** type is *Tag*)
   - Calculation
   - Tag
   - Entity Attribute

   These different options are outlined above, in the section "**Setting Process Values and Limits**", above.

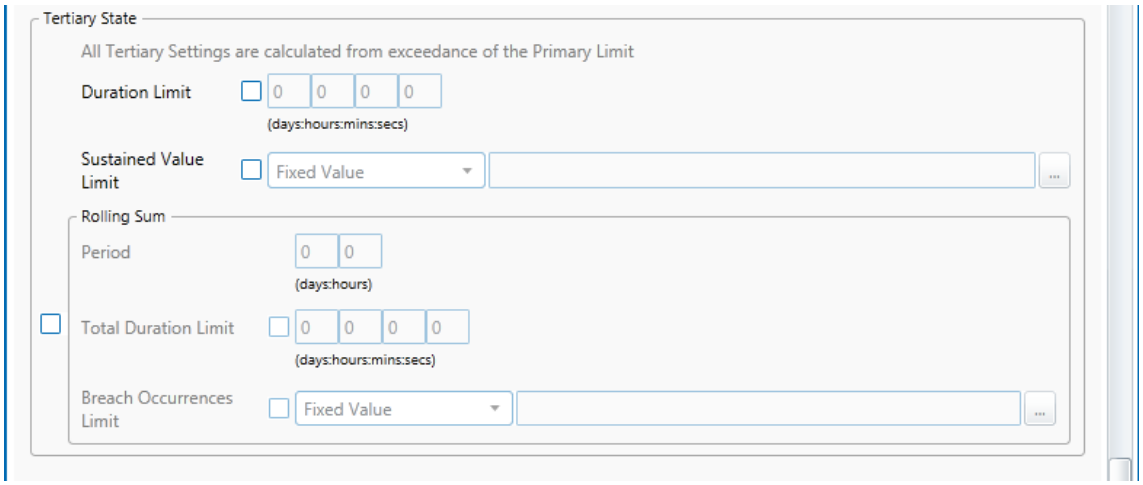


A Breach Occurrences Limit of 5 (Fixed Value)

Select Tertiary State Settings

Note: All Tertiary State settings are calculated from the primary deviation limit.

All tertiary state settings are captured or selected in the **Tertiary State** section of the process, with the exception of the Tertiary Deviation Limit which is set in the **Deviation Limit Settings** section of the process.



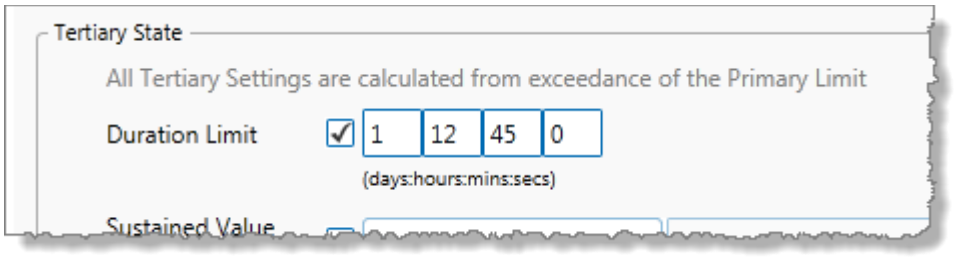
The Tertiary State Section of the Process

To Set a Tertiary State Duration Limit

The tertiary state duration limit is used for monitoring where data is continuously beyond the primary deviation limit, for longer than the specified tertiary duration limit.

In the **Tertiary State** section:

1. Select the **Duration Limit** check box.
2. Type integer values in the **days**, **hours**, **mins** (minutes), and **secs** (seconds) **Duration Limit** boxes to define a duration period. The default value is zero.



A Tertiary State Duration of 1 Day, 12 Hours and 45 Minutes

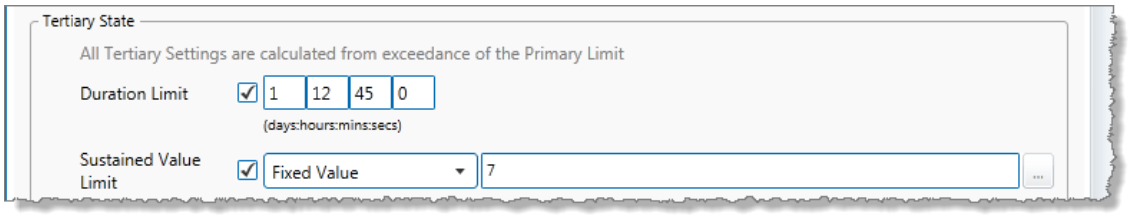
To Set a Tertiary State Sustained Value Limit

The Tertiary Sustained Value Limit is used for monitoring where data is beyond the primary deviation limit for more than a specified number of times (tertiary state sustained value limit), consecutively.

In the **Tertiary State** section:

1. Select the **Sustained Value Limit** check box.
2. From the **Sustained Value Limit** drop-down list, select one of the following and then type in or select a corresponding value:
   - Fixed Value
   - Attribute (only available of the **Source** type is *Entity* or *Hierarchy*)
   - Source Tag (only available of the **Source** type is *Tag*)
   - Calculation
   - Tag
   - Entity Attribute

   These different options are outlined above, in the section "**Setting Process Values and Limits**", above.



A Sustained Value Limit of 7 (Fixed Value)

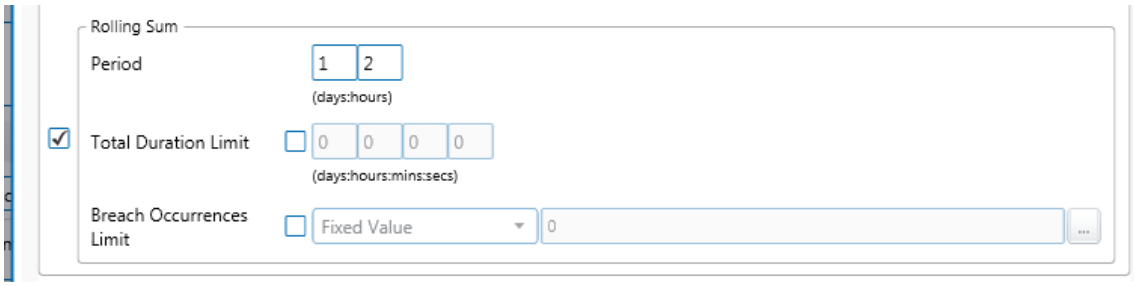
To Set a Tertiary State Rolling Sum Period

The rolling sum period is a defined period (specified in days and hours). At every sample interval, the rolling sum period applies to that period preceding the sample interval.

Set a tertiary state rolling sum period if you are going to define a Tertiary State Total Duration Limit or a Tertiary State Breach Occurrences Limit.

In the **Tertiary State** section:

1. Select the check box to the left of the Rolling Sum section.
2. Type integer values in the **days** and **hours** *Period* boxes to define the rolling sum period. The default value is zero.



A Tertiary State Rolling Sum Period of 1 Day and 2 Hours

To Set a Tertiary State Rolling Sum Total Duration Limit

The Tertiary State Rolling Sum Total Duration Limit is used to monitor for a specified accumulated duration of all periods where data is in breach of the primary deviation limit, within the preceding specified tertiary state rolling sum period.

In the **Rolling Sum** section, within the **Tertiary State** section:

1. Select the **Total Duration Limit** check box.
2. Type integer values in the **days**, **hours**, **mins** (minutes), and **secs** (seconds) **Total Duration Limit** boxes to define a total duration limit period. The default value is zero.

A Total Duration Limit of 3 Hours and 45 Minutes

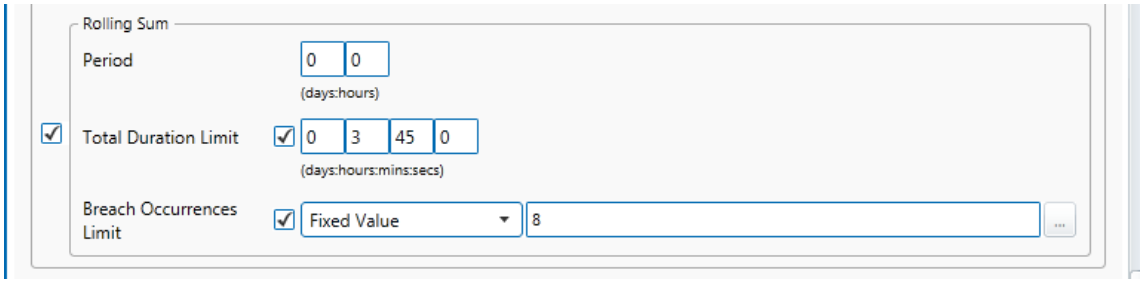
To Set a Tertiary State Rolling Sum Breach Occurrences Limit

The Tertiary State Rolling Sum Breach Occurrences Limit is used to monitor for when a set number of values (tertiary state breach occurrences limit) has breached the primary deviation limit, during the preceding specified tertiary rolling sum period.

In the **Rolling Sum** section, within the **Tertiary State** section:

1. Select the Breach Occurrences Limit check box.
2. From the **Breach Occurrences Limit** drop-down list, select one of the following and then type in or select a corresponding value:
   - Fixed Value
   - Attribute (only available of the **Source** type is *Entity* or *Hierarchy*)
   - Source Tag (only available of the **Source** type is *Tag*)
   - Calculation
   - Tag
   - Entity Attribute

   These different options are outlined above, in the section "**Setting Process Values and Limits**", above.



A Breach Occurrences Limit of 8 (Fixed Value)

Adding Comments to the Process Panel

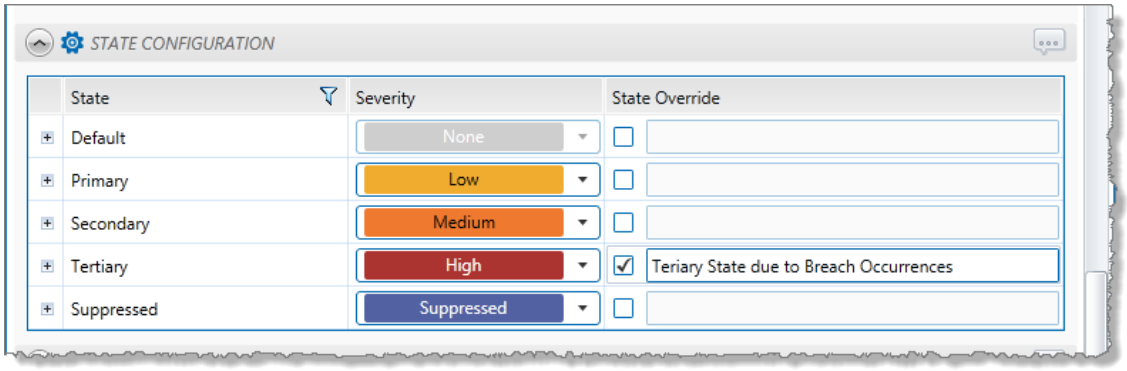
- To add comments to the process panel click the comment button, at the top right of the panel.

Configuring States

For the Drift Detection process, you can configure the following states, each with an optional state override and comments:

- Primary
- Secondary
- Tertiary
- Suppressed

You cannot change the severity of the Default state; however, you can add a state override and comments.



Note: Only configure states where you have set a limit.

To configure the state outcomes for a test in the **State Configuration** panel of the test, see 3.6 Configure States. If Case Management is enabled in Sentinel, this is also where you manage cases.

Appendix G. Stuck Value Process

The Stuck Value process determines whether test data remains the same for longer than a specified duration. If the data maintains a single value for longer than the duration limit, a *Stuck Value* state is reached and a ***Stuck Value*** event is raised.

State Transition Rules

The Stuck Value process follows state transition logic paths. Transition from one state to another is equally dependant on the current evaluation of data, and on the current state.

State transitions cause events to be raised, allowing for the escalation of actions via the Sentinel framework. Different actions can be assigned to different state outcomes.

There are only three possible state outcomes for a test using the Stuck Value process:

- Default
- Stuck Value
- Suppressed

The standard state transition logic for the Stuck Value process outcomes is to move between the default state and the stuck value state, based on data evaluation. Either of these states can also move to a suppressed state.

When defining the process for a test, you can set state transition logic such that the suppressed state can only transition to the default state. If this is not set, then the state will revert to whatever it was before the suppressed state.

The following table outlines the allowable state transitions of the Stuck Value process.

This state can transition to...	this state
Default	Stuck Value Suppressed
Stuck Value	Default Suppressed
Suppressed	Default Stuck Value*

***Note:** The transition from Suppressed to Stuck Value is only possible if specified in the test's process settings.

Test Outcomes

A number of outcomes are possible when the Stuck Value process is executed:

Default State

Data has changed at least once over the preceding defined duration period.

Stuck Value State

Data has not changed at all over the preceding defined duration period.

SUPPRESSED STATE

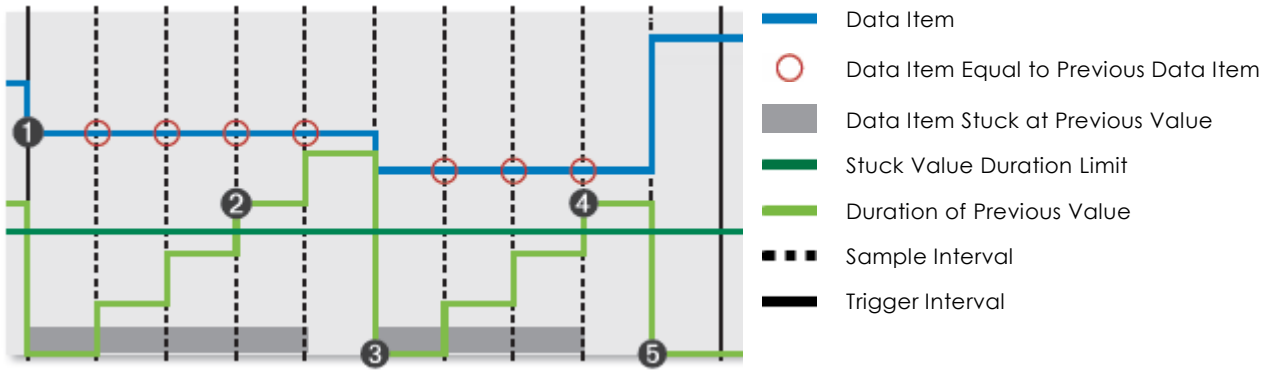
The monitor has been suppressed. For example, if the precondition has not been met.

Conditional Logic

The Stuck Value process provides the following conditional logic.

Stuck Value Monitoring

Stuck Value process uses Stuck Value Monitoring to detect whether data has remained unchanged for a specified duration, to cause a Stuck Value state. The process returns to the default state when the value changes again.



The following events are depicted in the graph:

1. The process goes into the default state (the value has changed), and a **default** event is raised.
2. The data point has not changed within the specified duration (the stuck value duration limit has been exceeded). A stuck value state is triggered and a **stuck value** event is raised.
3. The data point has changed since the previous data point. Duration of unchanged data is back to zero. A default state is reached, and a **default** event is raised.
4. The data point has not changed within the specified duration (the stuck value duration limit has been exceeded). A stuck value state is triggered and a **stuck value** event is raised.
5. The data point has changed since the previous data point. Duration of unchanged data is back to zero. A default state is reached, and a **default** event is raised.

Adding a Stuck Value Process

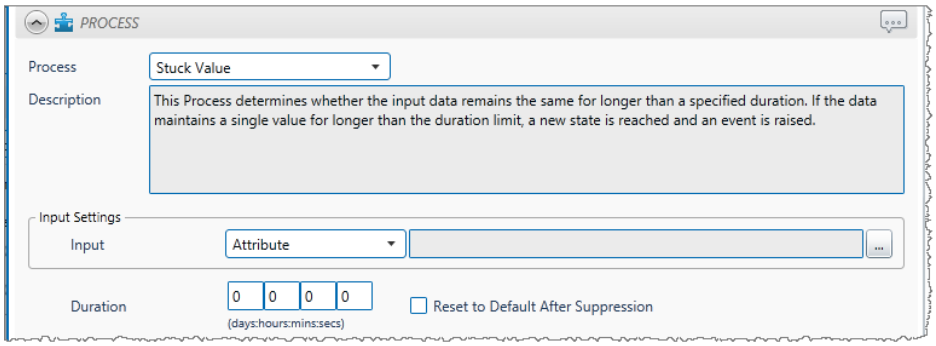
To define the Stuck Value for a test, you need to specify the input data and a duration limit.

Adding the Process

In the Sentinel **Test** page:

1. Expand the **Process** panel.
2. Select **Stuck Value** from the drop-down list.

   The Process panel shows the Stuck Value process components.



3. From the **Input** drop-down list, select an input from the following:

   Attribute
   This option is only available if the **Source Type** is **Entity** or **Hierarchy**.

   Click the ellipsis button to select an attribute by using the P2 Server Attribute Picker. You are limited to selecting an attribute of the test source monitor items. This attribute of each of the monitor items is a separate process input.

   Source Tag
   This option is only available if the **Source Type** is **Tag**.

   Calculation
   Click the ellipsis button to open the *Edit Calculation* window. The expression is resolved in the P2 Server calculation engine.

   If the Source Type is Entity or Hierarchy:
   Type a calculation, prefixed by 'this' as the **Source Entity** token, for example: **{this:THP} + 34**.

   If the Source Type is Tag:
   Type a calculation, prefixed by 'this' as the **Source Tag** token, for example: **{this} * 2**.

   Entity Attribute
   Click the ellipsis button to open the *P2 Server Browser* to select an entity. From here, select a P2 Server attribute, or attribute value, by using *the* P2 Server Attribute Picker for the selected entity.

4. Define the **Duration**.

a. Type integer values in the **days**, **hours**, **mins** (minutes), and **secs** (seconds) in the **Duration** boxes to define a duration period. The default value is zero.

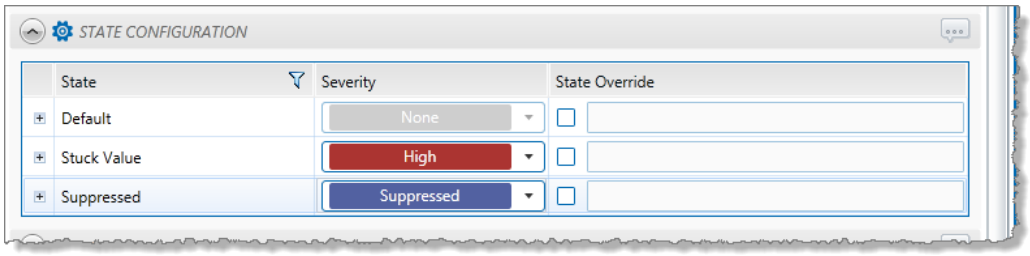
b. To reset the state to default after a suppressed state, select the **Reset to Default After Suppression** check box. If the **Reset to Default After Suppression** check box is not selected, the process will take into consideration the values before and after the suppression period when calculating the duration.

Configuring States

For the Stuck Value process, you can configure the following states, each with an optional state override and comments:

- Stuck Value
- Suppressed

You cannot change the severity of the Default state; however, you can add a state override and comments.



Note: Only configure states where you have set a limit.

Appendix H. Steady State Detection Process

The Steady State Detection evaluates up to four separate data inputs to determine whether the asset under surveillance has reached a steady state. This process can also evaluate whether data is continuously transient, that is: if it does not reach the steady state for longer a specified duration.

The standard deviation of each input is evaluated at every sample interval. Each input's standard deviation is calculated over the duration specified for that input, and measured against the deviation threshold specified for that input.

For example: for Input 1, the process is configured to calculate the standard deviation for all samples collected within the last two hours; it then determines whether this figure exceeds the current deviation threshold value. Simultaneously, the standard deviation for Input 2 for all samples collected over the last hour (Input 2's configured deviation duration) is evaluated to determine whether it has exceeded the current deviation threshold for Input 2. The combined outcome for all configured inputs is used to determine the test outcome for that sample interval.

Steady State Detection is used for scenarios where fluctuations of values are expected initially (***transient state***), but where these variations should subside over time, leading to a ***steady state***.

If the data continues to fluctuate for one of more of the inputs (that is, if it continues to be in the transient state) for longer than a specified duration, this triggers a ***continuous transient state***.

State Transition Rules

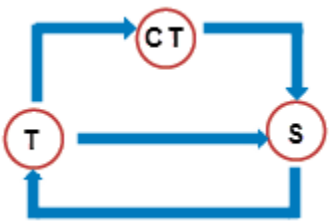
The Steady State Detection process has clearly defined state transition logic paths. Transition from one state to another is dependent on the current evaluation of data, and on the current state.

State transitions cause events to be raised, allowing for the escalation of actions via the P2 Sentinel framework. Different actions can be assigned to different state outcomes.

The following table outlines the allowable state transitions of the Steady State Detection process.

This state can transition to		This state
Transient	→	Steady
	→	Continuous Transient
Continuous Transient	→	Steady
Steady	→	Transient

The following diagram outlines the state transition logic of the Steady State Detection process.



T Transient State

CT Continuous Transient State

S Steady State

Test Outcomes

A number of outcomes are possible when the Steady State Detection process is executed:

STEADY STATE

For all inputs, the standard deviation for that input is at or below the input's deviation threshold.

TRANSIENT STATE

For one or more inputs, the standard deviation for that input is above the input's deviation threshold.

CONTINUOUS TRANSIENT STATE

The transient state persists for up to or longer than the defined continuous transient duration.

SUPPRESSED STATE

The monitor has been suppressed. For example, if the precondition has not been met.

Using Standard Deviation

The P2 Sentinel uses the statistical standard deviation method to calculate dispersion of the different input values over a given duration.

Conditional Logic

The Steady State Detection process provides the following conditional logic.

Note: All of the example graphs in the following sections show tests that have used the *Last Known Value* sample method.

Output Status Tag

An ***Output Status Tag*** can be set for both the ***Continuous Transient State*** and the ***Steady State***. In each case, this tag can be an entity attribute, either as it is, or as part of a calculation.

If an output status tag is set for the continuous transient state, the tag will show a status of one within P2 Explorer when a continuous transient event is raised, and zero for any other state.

Similar behaviour applies to the output status tag for steady state (showing a status of one for steady state, and zero for any other state). Within P2 Server Browser, the status tag can be observed, for example altering a shape's appearance to indicate whether the monitor's data item is in a particular state or not.

Transient State

The Transient State can be considered the default state of the Steady State Detection Process.

Every input is evaluated. If any one of the inputs' standard deviation is above that input's deviation threshold, a transient event is raised and the process goes into a transient state.

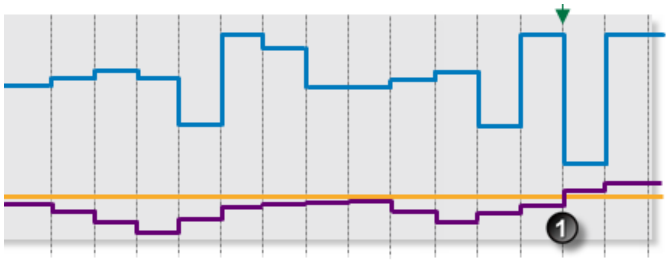
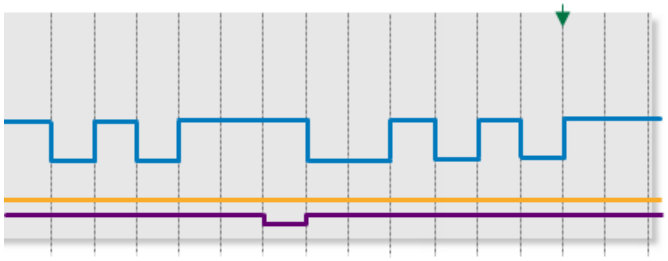
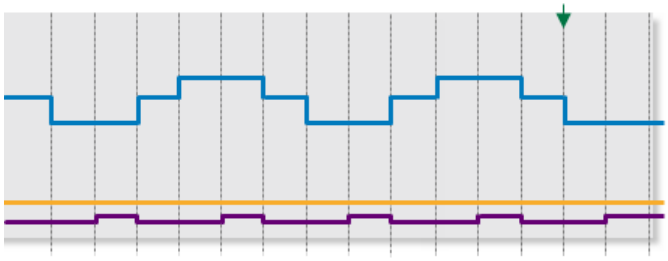
The following example demonstrates how a steady state moves to a transient state. Three inputs are used. In this example, the following settings are used:

- All three inputs have fixed deviation thresholds.
- All three inputs have a deviation duration of five hours.
- The sample interval is 1 hour.

Data item — Deviation threshold — Sample interval

Standard deviation (calculated for the 5 hours preceding the sample interval)

The sample interval being reported on.

			Collective Evaluation of Inputs
Input 2	**11:00am**		
		At **11:00am** the standard deviation for Input 2 goes above the deviation threshold for Input 2.	At **11:00am** one of the three inputs has breached the primary deviation limit. 1 A transient event is raised, and a transient state is reached.
Input 1	**11:00am**		
		At **11:00am** the standard deviation for Input 1 is still below the deviation threshold for Input 1. (This input has not caused the transient event.)	At **11:00am** one of the three inputs (Input 2) is above the primary deviation limit.
Input 3	**11:00am**		
		At **11:00am** the standard deviation for Input 3 is still below the deviation threshold for Input 3. (This input has not caused the transient event.)	At **11:00am** one of the three inputs (Input 2) is above the primary deviation limit.

Continuous Transient State

A continuous transient event occurs when the transient state persists for up to or longer than the defined continuous transient duration.

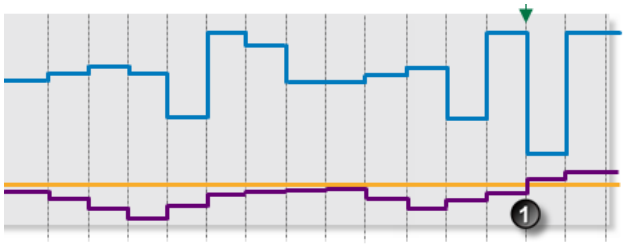
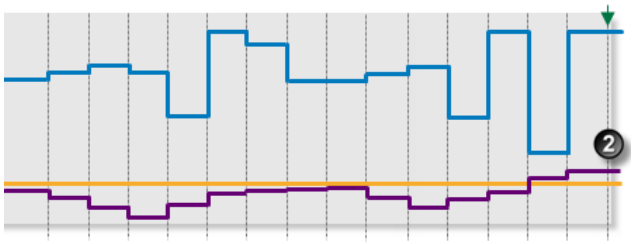
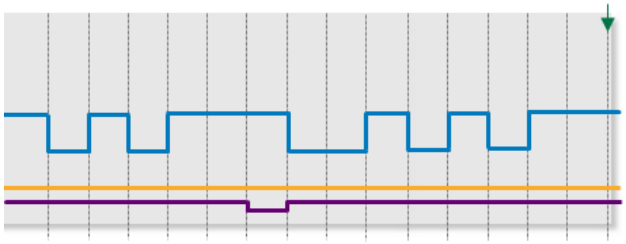
The following example demonstrates the continued duration of the transient state, which causes a continuous transient event to occur. In this example, the following settings are used:

- Both inputs have a deviation duration of five hours.
- The continuous transient state duration is 2 hours.
- The sample interval is 1 hour.
- Both inputs use a fixed deviation threshold.

Data item — Deviation threshold — Sample interval

Standard deviation (calculated for the 5 hours preceding the sample interval)

The sample interval being reported on.

		Collective Evaluation of Inputs
Input 2 **11:00am** 	At **11:00am** the standard deviation for Input 2 goes above the deviation threshold for Input 2.	At **11:00am** one of the three inputs has breached the primary deviation limit. 1 A transient event is raised, and a transient state is reached.
Input 2 **1:00pm** 	At **1:00pm** the standard deviation for Input 2 is still above the standard deviation threshold for Input 2.	At **1:00pm** the transient state has a duration of 2 hours. 2 A continuous transient state is reached, and a continuous transient event is raised.
Input 1 **1:00pm** 	At **1:00pm** the standard deviation for Input 1 is still below the standard deviation threshold for Input 1. *Therefore, Input 1 has not caused or affected either the transient event or the continuous transient event.*	At **1:00pm** the transient state has a duration of 2 hours, due to the continued high standard deviation for Input 2.

Steady State

For all inputs, the standard deviation is at or below that input's deviation threshold.

The following example demonstrates how a transient state changes to a steady state. Three inputs are used. In this example, the following settings are used:

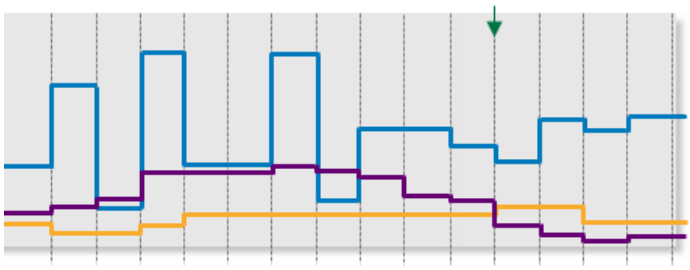
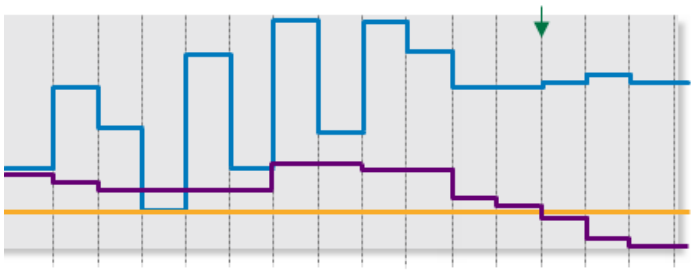
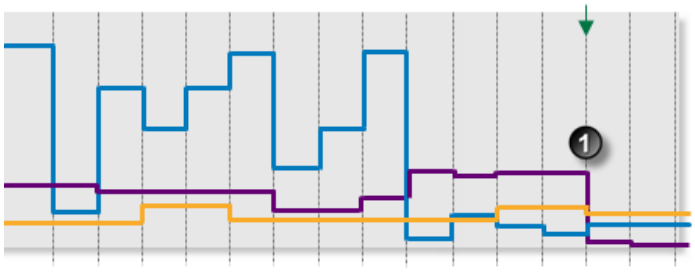
- The sample interval is 1 hour.
- Input 2 uses a fixed deviation threshold.
- Input 1 and input 3 use variable deviation thresholds.
- All three inputs have a deviation duration of five hours.

In the example, all three inputs have a deviation duration of five hours. For each input, at each sample interval: all samples collected over the previous five hours are used to calculate the standard deviation for that input.

Data item | Deviation threshold | Sample interval

Standard deviation (calculated for the 5 hours preceding the sample interval)

The sample interval being reported on.

		Collective Evaluation of Inputs
Input 1 **9:00am** 	At **9:00am** the standard deviation for Input 1 goes below the deviation threshold for Input 1.	At **9:00am** one out of three inputs has its standard deviation below its deviation threshold.
Input 2 **10:00am** 	At **10:00am**, the standard deviation for Input 2 goes below the deviation threshold for Input 2.	At **10:00am** two out of three inputs have their standard deviation below their respective deviation thresholds.
Input 3 **11:00am** 	At **11:00am** the standard deviation for Input 3 goes below the deviation threshold for Input 3.	At **11:00am** *all three inputs* have their standard deviation below their respective deviation thresholds. 1 A steady state is reached, and a steady state event is raised.

Adding a Steady State Detection Process

The Steady State Detection Process evaluates the standard deviation of one or more defined inputs. Based on the combined outcome of these evaluations, a state persists or a new state is raised.

Setting Process Values and Limits

Setting up the Steady State Detection process involves selecting inputs and deviation thresholds. Deviation thresholds can either be fixed values, or they can be variable data taken from P2 Server entities. Inputs can only be defined as variable data taken from P2 Server entities.

The following deviation thresholds are available. Select a deviation threshold type from the drop-down list, then type in or select a limit.

Fixed Value
Type in a numerical value.

Source Tag
This option is only available if the **Source Type** is **Tag**.

Attribute
This option is only available if the test's **Source Type** is **Entity** or **Hierarchy**.

Click the ellipsis  button to open the P2 Server Attribute Picker, to select an attribute of the source entities.

Calculation
Click the ellipsis  button to open the *Edit Calculation* window. The expression is resolved in the P2 Server calculation engine.

If the Source Type is Entity or Hierarchy:
Type a calculation, prefixed by 'this' as the **Source Entity** token, for example: **{this:THP} + 34**.

If the Source Type is Tag:
Type a calculation, prefixed by 'this' as the **Source Tag** token, for example: **{this} * 2**.

Tag
Click the ellipsis  button to open the *P2 Server Browser* to select a tag.

Entity Attribute
Click the ellipsis  button to open the *P2 Server Browser* to select an entity. From here, select a P2 Server attribute, or attribute value, by using the P2 Server Attribute Picker for the selected entity.

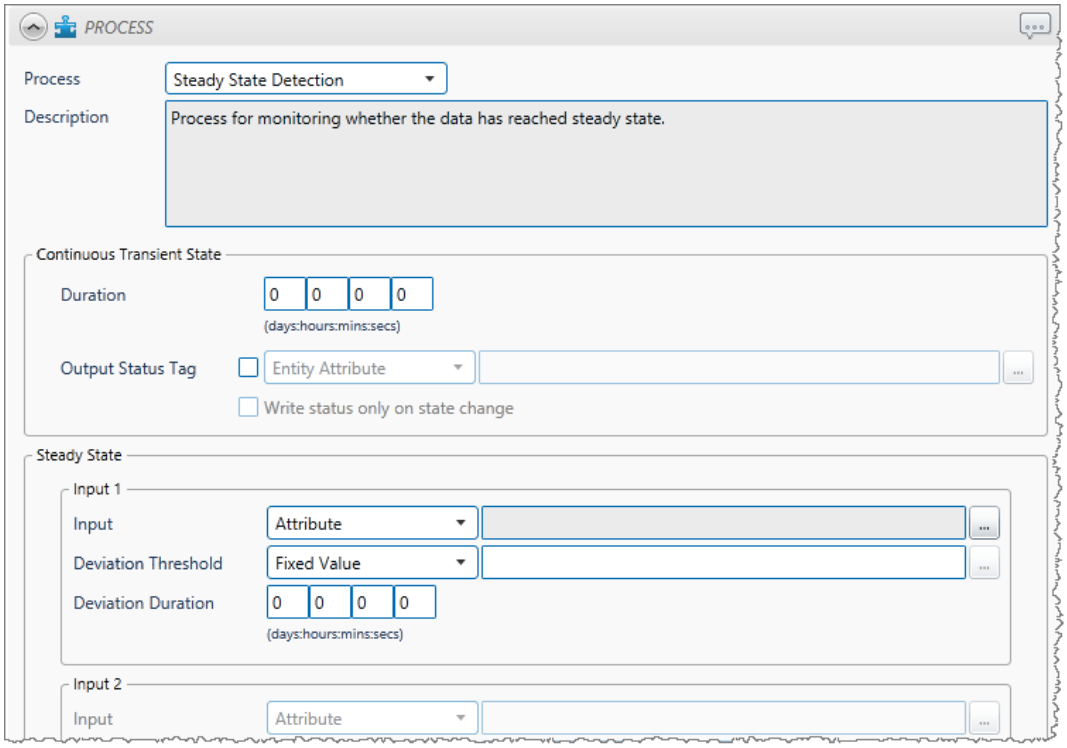
Adding the Process

As with all P2 Sentinel processes, the Steady State Detection Process is defined within a Sentinel **Test** page.

Steady State Detection Process

In the Sentinel **Test** page:

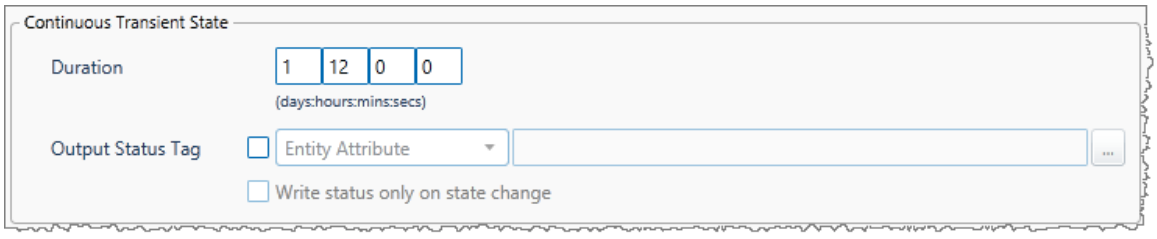
1. Expand the **Process** panel.
2. Select **Steady State Detection** from the **Process** drop-down list.



Define Continuous Transient State Settings

The duration specified here is used to determine the transition from transient state to continuous transient state. An output status tag can reflect this state transition on a P2 Server Browser page.

1. Type integer values in the **days**, **hours**, **mins** (minutes), and **secs** (seconds) **Duration** boxes to define a duration period. The default value is zero.



A Continuous Transient State Duration of 1 Day, 12 Hours, 0 Minutes and 0 Seconds

2. Optionally set the Output State Tag.
   a. Select the **Output Status Tag** check box.
   b. Select one of the options from the drop-down list, then click the ellipsis button to select.

      Attribute (only available of the source type is entity or hierarchy)
      This option is only available if the test's Source Type is Entity or Hierarchy.

Click the ellipsis [...] button to open the P2 Server Attribute Picker, to select an attribute of the source entities.

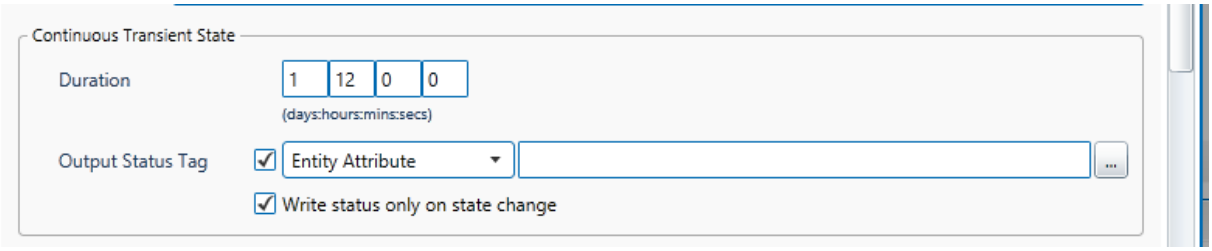
Tag

Click the ellipsis [...] button to open the P2 Server Browser to select a tag.

Entity Attribute

Click the ellipsis [...] button to open the P2 Server Browser to select an entity. From here, select a P2 Server attribute, or attribute value, by using the P2 Server Attribute Picker for the selected entity.

c. To ensure that the status is set only on a state change, select the **Write status only on state change** check box.



Continuous Transient State with an Output Status Tag Selected

Defining the Steady State Settings

At least one input will be evaluated to determine whether the process has reached a steady state.

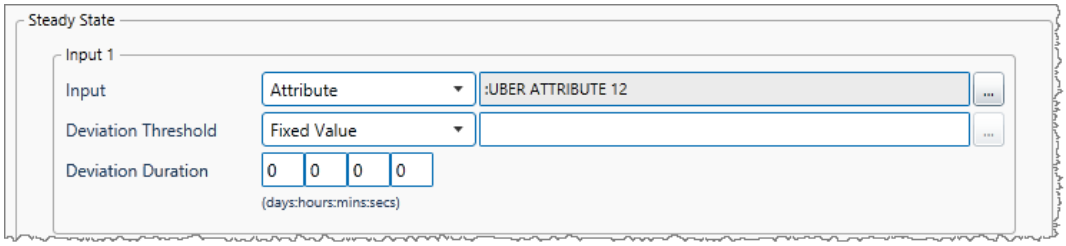
If every enabled input's standard deviation is at or below that input's deviation threshold, a steady state is reached.

The various different inputs are:

- Input 1
- Input 2 (optional)
- Input 3 (optional)
- Input 4 (optional)

Define the Settings for Input 1

At every sample interval, all values for Input 1's preceding duration period are used to calculate a standard deviation for Input 1. If the standard deviation exceeds the deviation threshold for Input 1, a transient event is raised, and a transient state is reached.



1. From the **Input** drop-down list, select one of the following and then type in or select a corresponding value:

Attribute

This is available where the **Source Type** is either **Entity** or **Hierarchy**.

Click the ellipsis button to open the **P2 Server Attribute Picker**. This shows templates of the source entities. To view primary templates of the source entities, select the **Primary Template** check box. Select an attribute.

Source Tag
This is available where the **Source Type** is a **Tag**.

Calculation
Click the ellipsis button to open the *Edit Calculation* window.

- Where the source type is **Entity** or **Hierarchy**, enter '*this*' for the source entity token, followed by an attribute or attribute value definition. For example: **{this:THP} + 34**. Another example: **{this:Choke!Current Position}*1.2** The expression is resolved in the P2 Server calculation engine.
- Where the source type is **Tag**, enter '*this*' for the tag token. For example: **{this} * 1.2**. The expression is resolved in the P2 Server calculation engine.

Entity Attribute
Click the ellipsis button to open the *P2 Server Browser* to select an entity. From here, select a P2 Server attribute, or attribute value, by using the P2 Server Attribute Picker for the selected entity.

2. From the **Deviation Threshold** drop-down list, select one of the following and then type in or select a corresponding value:

Fixed Value
Type in a numerical value.

Attribute
This option is only available if the test's **Source Type** is **Entity** or **Hierarchy**.
Click the ellipsis button to open the P2 Server Attribute Picker, to select an attribute of the source entities.

Source Tag
This is available where the **Source Type** is a **Tag**.

Calculation
Click the ellipsis button to open the *Edit Calculation* window. The expression is resolved in the P2 Server calculation engine.

- If the **Source Type is Entity or Hierarchy**:
  Type a calculation, prefixed by 'this' as the **Source Entity** token, for example: **{this:THP} + 34**.
- If the **Source Type is Tag**:
  Type a calculation, prefixed by 'this' as the **Source Tag** token, for example: **{this} * 2**.

Tag
Click the ellipsis button to open the *P2 Server Browser* to select a tag.

Entity Attribute
Click the ellipsis button to open the *P2 Server Browser* to select an entity. From here, select a P2 Server attribute, or attribute value, by using the P2 Server Attribute Picker for the selected entity.

3. Type integer values in the **days**, **hours**, **mins** (minutes), and **secs** (seconds) **Deviation Duration** boxes to define a deviation duration period for the steady state for Input 1. The default value is zero.

The various options for the **Input** drop-down list and the **Deviation Threshold** drop-down list are outlined above, in the section: "**Setting Process Values and Limits**", above.

Optionally Define the Settings for the Remaining Inputs

If you are using other inputs, define these in the same way as you for Input 1.

Input options for Inputs 2, 3 and 4 are:

Fixed Value
Type in a numerical value.

Attribute
This option is only available if the test's **Source Type** is **Entity** or **Hierarchy**.
Click the ellipsis button to open the P2 Server Attribute Picker, to select an attribute of the source entities.

Source Tag
This is available where the **Source Type** is a **Tag**.

Calculation
Click the ellipsis button to open the *Edit Calculation* window. The expression is resolved in the P2 Server calculation engine.

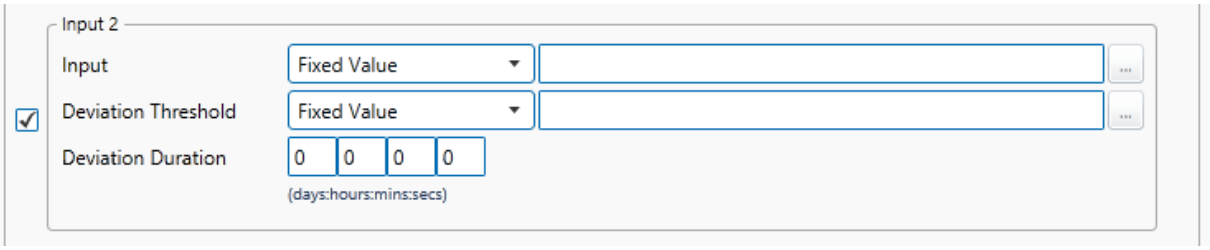
– If the **Source Type is Entity or Hierarchy**:
Type a calculation, prefixed by 'this' as the **Source Entity** token, for example: **{this:THP} + 34**.

– If the **Source Type is Tag**:
Type a calculation, prefixed by 'this' as the **Source Tag** token, for example: **{this} * 2**.

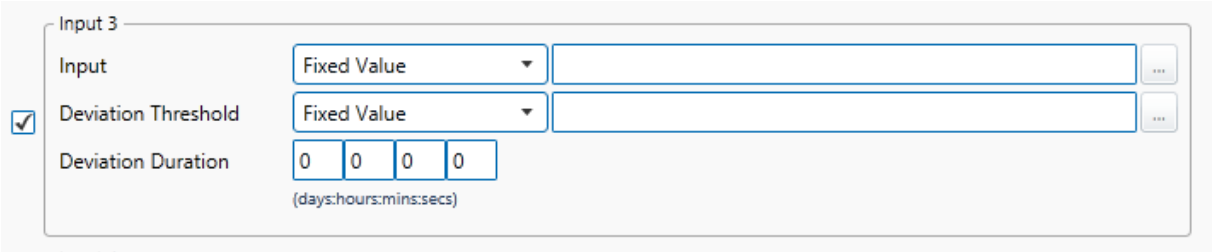
Tag
Click the ellipsis button to open the *P2 Server Browser* to select a tag.

Entity Attribute
Click the ellipsis button to open the *P2 Server Browser* to select an entity. From here, select a P2 Server attribute, or attribute value, by using the P2 Server Attribute Picker for the selected entity.

1. To define Input 2, select the check box to the left of the **Input 2** section, then define the **Input**, **Deviation Threshold** and **Deviation Duration** for Input 2.



2. To define Input 3, select the check box to the left of the **Input 3** section, then define the **Input**, **Deviation Threshold** and **Deviation Duration** for Input 3.



3. To define Input 4, select the check box to the left of the **Input 4** section, then define the **Input**, **Deviation Threshold** and **Deviation Duration** for Input 4.

Optionally Define the Output Status Tag

To set the Output Status Tag for the steady state:

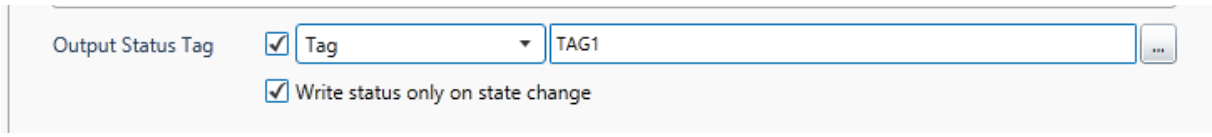
1. Select the **Output Status Tag** check box.
2. Select one of the following types and values:

   Attribute
   This option is only available if the test's **Source Type** is **Entity** or **Hierarchy**.
   Click the ellipsis button to open the P2 Server Attribute Picker, to select an attribute of the source entities.

   Tag
   Click the ellipsis button to open the *P2 Server Browser* to select a tag.

   Entity Attribute
   Click the ellipsis button to open the *P2 Server Browser* to select an entity. From here, select a P2 Server attribute, or attribute value, by using the P2 Server Attribute Picker for the selected entity.

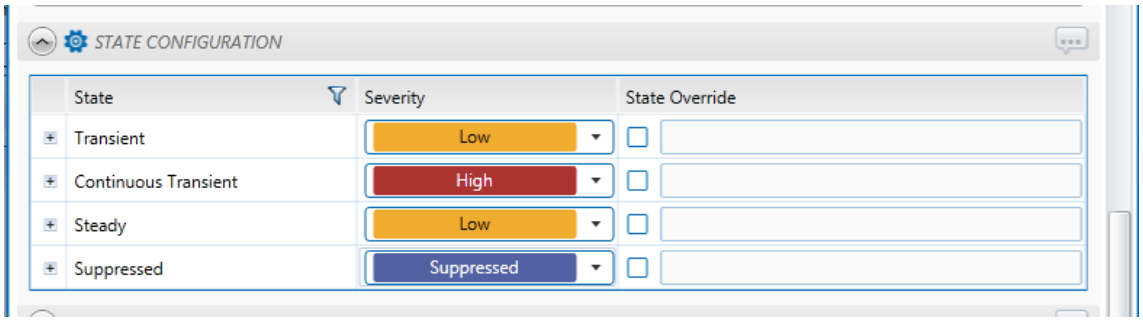
3. To ensure that the status is set only on a state change, select the **Write status only on state change** check box.



Configuring States

For the Steady State Detection process, you can configure the following states, each with an optional state override and comments:

- Transient
- Continuous Transient
- Steady
- Suppressed



To configure the state outcomes for a test in the **State Configuration** panel of the test, see 3.6 Configure States. If Case Management is enabled in Sentinel, this is also where you manage cases.

Appendix I. Logic Process

The Logic process independently evaluates up to four different inputs, each with its own limits and offsets. The different states (state 1 up to state 8), are determined based on the application of various logic rules that use one or more of the input evaluation outcomes as their operands. For example, a State 1 event is raised if the State 1 logic state was defined as:

Input 1 data is below the Input 1 minimum offset
AND Input 2 data is above the Input 2 maximum offset
and if both of these conditions occur simultaneously (at the same sample interval)

Also, when used as part of a Logic state expression, the inputs for the Logic process can each have a ***duration*** specified, whereby an outcome has to be above the maximum offset for the full specified duration to be considered "above the maximum offset", or, likewise, it should be below the minimum offset for the full specified duration to be considered "below the minimum offset".

Logic Process allows multiple logical combinations and inputs to be used, to determine the different states. This process is particularly useful when you need to measure several inputs simultaneously, and when combinations of conditions should raise various states.

State Transition Rules

Unlike many of the other Sentinel processes, the Logic process does not have a state transition logic path. Transition from one state to another depends entirely on the current evaluation of data, and is unaffected by the current state.

However, the different states follow a rule of precedence, thus allowing for the escalation of actions based on severity, via the P2 Sentinel framework. Different actions can be assigned to different state outcomes.

Logic states are given priority in the order they are defined. So, State 1 is evaluated first. If the logic fails, then State 2 is evaluated, and so on. Thus it makes sense to put the highest severity items in the highest positions (State 1 and State 2), and reserve the lower severities for the lowest positions.

The following table lists the order of precedence for the Logic process logic states.

Logic State	Under these conditions
State 1	This has the highest priority.
State 2	This has the second highest priority.
State 3	This has the third highest priority.
…	…
State N -1	This has the second lowest priority.
State N	This has the lowest priority.

Test Outcomes

A number of outcomes are possible when the Logic process is executed:

Outcome	Description
Default State	The default state is reached when none of the logic states evaluate to True, and when the monitor is not in a suppressed state.
State 1	Boolean logic is applied to the operators and operands defined for State 1. If the logic evaluates to True, and if the monitor is not already in State 1, State 1 is reached and a State 1 event is raised.
State 2	Boolean logic is applied to the operators and operands defined for State 2. If the logic evaluates to True, and if the monitor is not already in State 2, State 2 is reached and a State 2 event is raised.
State 3	Boolean logic is applied to the operators and operands defined for State 3. If the logic evaluates to True, and if the monitor is not already in State 3, State 3 is reached and a State 3 event is raised.
State 4	Boolean logic is applied to the operators and operands defined for State 4. If the logic evaluates to True, and if the monitor is not already in State 4, State 4 is reached and a State 4 event is raised.
State 5	Boolean logic is applied to the operators and operands defined for State 5. If the logic evaluates to True, and if the monitor is not already in State 5, State 5 is reached and a State 5 event is raised.
State 6	Boolean logic is applied to the operators and operands defined for State 6. If the logic evaluates to True, and if the monitor is not already in State 6, State 6 is reached and a State 6 event is raised.
State 7	Boolean logic is applied to the operators and operands defined for State 7. If the logic evaluates to True, and if the monitor is not already in State 7, State 7 is reached and a State 7 event is raised.
State 8	Boolean logic is applied to the operators and operands defined for State 8. If the logic evaluates to True, and if the monitor is not already in State 8, State 8 is reached and a State 8 event is raised.
Suppressed State	The monitor has been suppressed. For example, if the precondition has not been met.

Conditional Logic

The Logic process provides the following conditional logic.

Note: All of the example graphs in the following sections show tests that have used the Last Known Value sample method.

Evaluating the Different States

Up to eight different states (State 1 through to State 8) can be set up for evaluation. Any state can only be raised if evaluations for preceding states have evaluated to False. For example, State 6 can only be raised if it evaluates to True *and* State 1, State 2, State 3, State 4 and State 5 all evaluate to False. Likewise, State 3 can only be raised if it evaluates to True ***and*** State 1 and State 2 both evaluate to False.

Mode Settings

The mode settings apply to all of the defined Inputs.

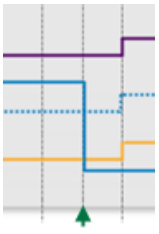
Offset Mode

The offset mode is set to be fixed or percentage, and applies to all of the defined limits. When offset mode is fixed value, it is added to (or subtracted from, in the case of a negative offset) the limit value. If an offset is a percentage, then it is multiplied against the limit value and the resulting product is added or subtracted to the limit value.

Suppress Minimums

If the **Suppress all minimums if any input is within limits of offsets** check box is selected, all inputs are evaluated as a group, in the following way.

If any of the inputs is within its limits, then none of the other inputs can be evaluated as "below minimums", even if they have had a minimum offset defined. For example, if Input 2 data is within its offset limits, then Input 1, Input 3 and Input 4 cannot be evaluated as "below minimum".

Data item Limit Min Offset Max Offset Sample Interval	
Input 1	
 11:00am	**At 11:00am, data for Input 1 is below the minimum offset.** **However, because Input 2 is within the offset limits at this time, and the Suppress all minimums if any input is within limits of offsets** check box is selected, Input 1 is not "below minimum", but "within limits".
Input 2	
 11:00am	**At 11:00am, data for Input 2 is within the offset limits.** **Because of this, there can be no "below minimum" evaluations for any of the other limits at 11:00am.**

Input 3

11:00am

At 11:00am, data for Input 3 is below the minimum offset.

However, because Input 2 is within the offset limits at this time, and the Suppress all minimums if any input is within limits of offsets check box is selected, Input 3 is not "below minimum", but "within limits".

Input 4

11:00am

At 11:00am, data for Input 4 is above the maximum offset.

Input 4 evaluates as "above maximum" at 11:00am.

Defining Inputs

At least one, and up to four different inputs can be set up in the Logic process. Of those inputs that are set up, various evaluation outcomes can be used as operands in the logic applied to the different states. Each input (Input 1, Input 2, Input 3 and Input 4) has its own settings:

Input

The data that is evaluated.

Limit

The base value from which the offsets are calculated.

Max Offset

If this is selected, then it is the value by which the maximum offset is calculated; this value is applied to the limit, either as a percentage or as an absolute value (depending on the selected offset mode).

Min Offset

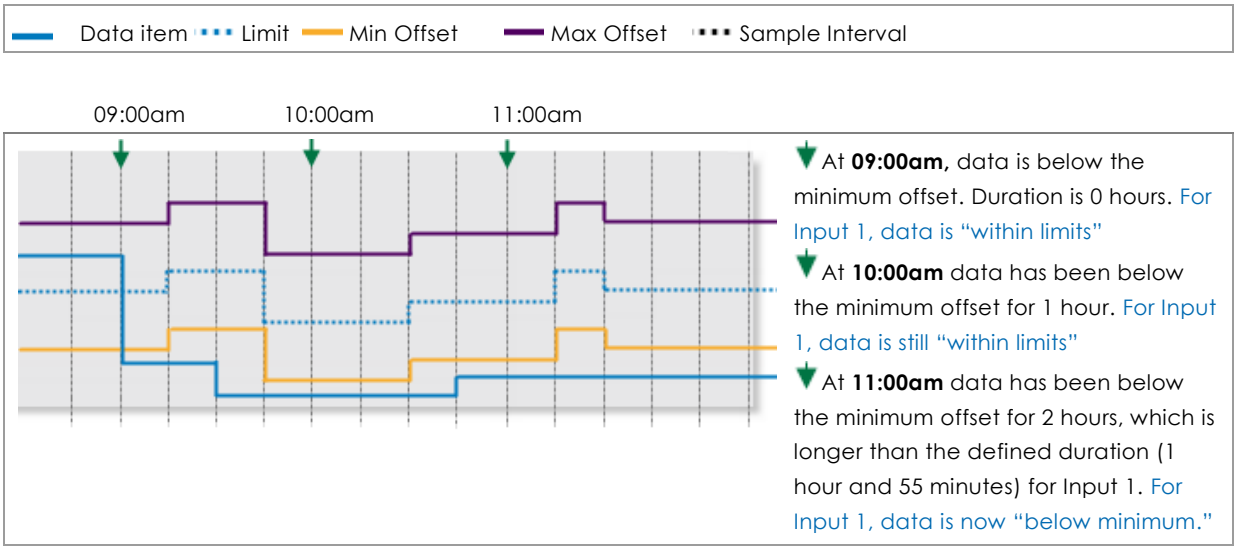
If this is selected, then it is the value by which the minimum offset is calculated; this value is applied to the limit, either as a percentage or as an absolute value (depending on the selected offset mode).

Duration

If a duration is defined, this affects the evaluation of an input. An input will only be evaluated as "below minimum" when it remains below the minimum offset for longer than that input's defined duration. Likewise, an input will only be evaluated as "above maximum" when it remains above the maximum offset for longer than that input's defined duration.

Example: Evaluating an Input with Min Offset Duration

The following example demonstrates how an input is only evaluated as "below minimum" after a certain duration. In this example, duration is defined as 1 hour and 55 minutes.



Determining States

The Logic process requires that at least one state (State 1) is defined. Up to eight different states can be defined. Each state is made up of a combination of outcomes of the various inputs.

For example, State 1 can be defined as: `1 Max AND 3 Min OR 2 Max AND 4 Min`

In order for State 1 to be raised, the following evaluations must occur simultaneously: Input 1 evaluates to "above maximum" AND Input 3 evaluates to "below minimum" OR Input 2 evaluates to "above maximum" AND Input 4 evaluates to "below minimum".

How the Logic Process Evaluates Conditions

Each state has up to four operands, with up to three logical operators. The Logic process uses Boolean logic to evaluate conditions.

In Boolean Logic, the rules to be aware of are:

- "And" takes precedence over "or"
- "True and True" evaluates to True
- "True and False" evaluates to False
- "False and False" evaluates to False
- "True or False" evaluates to True
- "False or False" evaluates to False
- "True or True" evaluates to True

For P2 Sentinel, group pairs according to the precedence rules, and then from left to right, to better understand how the logical evaluation is performed:

`1 Min and 2 Max or 3 Min and 4 Min` groups to:
`(1 Min and 2 Max) or (3 Min and 4 Min)`, and is evaluated as:
`(True) or (False)`, which is further evaluated to the final outcome:
`True`

The following table demonstrates how various states have been set up, and are then evaluated. The highest state (closest to State 1) takes precedence over other states.

Evaluate:	Expression evaluates to:							Evaluates to	Raises a State
Operand & (operator)	1	(1)	2	(2)	3	(3)	4		
State 1	True	AND	True	AND	False	OR	False	False	No state raised (False outcome)
State 2	True	AND	False	OR	True	AND	True	True	State 2 is raised
State 3	True	AND	True	AND	True	AND	True	True	State 2 takes precedence
State 4	True	OR	False	AND	True	-	-	-	State 2 takes precedence
State 5	-	-	-	-	-	-	-	-	No State Defined
State 6	-	-	-	-	-	-	-	-	No State Defined
State 7	-	-	-	-	-	-	-	-	No State Defined
State 8	-	-	-	-	-	-	-	-	No State Defined

In the example, **State 1** is evaluated as follows:

Operand 1	Operator 1	Operand 2	Operator 2	Operand 3	Operator 3	Operand 4	Final Outcome
1 Max	AND	3 Min	AND	2 Max	OR	4 Min	
True	AND	True	AND	False	OR	False	
		True	AND	False	OR	False	
				False	OR	False	
							False

State 2 is evaluated as follows:

Operand 1	Operator 1	Operand 2	Operator 2	Operand 3	Operator 3	Operand 4	Final Outcome
1 Max	AND	4 Min	OR	2 Min	AND	3 Min	
True	AND	False	OR	True	AND	True	
		False	OR			True	
							True

State 3 is evaluated as follows:

Operand 1	Operator 1	Operand 2	Operator 2	Operand 3	Operator 3	Operand 4	Final Outcome
1 Max	AND	3 Min	AND	2 Min	AND	4 Max	
True	AND	True	AND	True	AND	True	
		True	AND			True	
							True

and so on.

Definition of Operands in the Logic Process

The following operands are available to the Logic Process. Note that for any of the limits, "within limits" means that a limit has not been exceeded. In these definitions, *N* could be 1, 2, 3 or 4 and is referring to the different inputs: Input 1, Input 2, Input 3, Input 4.

N Min

If the input value for *N* is currently lower than the minimum offset for *N*, and has been, continuously, for longer than the defined duration (if any duration has been defined for Limit *N*) , or if it is currently lower than the minimum offset for *N* (if no duration has been defined) then *N Min* evaluates to True. Otherwise, it evaluates to False.
Example: *1 Min*, refers to the Minimum Offset for Input 1.

N Max

If the input value for *N* is currently higher than the maximum offset for *N,* and has been, continuously, for longer than the defined duration (if any duration has been defined for Limit *N*) , or if it is currently higher than the maximum offset for *N* (if no duration has been defined) then *N Max* evaluates to True. Otherwise, it evaluates to False.
Example: *2 Max*, refers to the Maximum Offset for Input 2.

N Out

If the input value for *N* is currently lower than the minimum offset for *N,* and has been, continuously for longer than the defined duration (if any duration has been defined for Limit *N*) , or if it is currently lower than the minimum offset for *N* (if no duration has been defined) then *N Min* evaluates to True. Otherwise, it evaluates to False.
Example: 1 Min, refers to the Minimum Offset for Input 1.

Or, if the input value for *N* is currently higher than the maximum offset for *N*, and has been, continuously, for longer than the defined duration (if any duration has been defined for Limit *N*) , or if it is currently higher than the maximum offset for *N* (if no duration has been defined) then *N Max* evaluates to True. Otherwise, it evaluates to False.
Example: *2 Out*, refers to the Maximum Offset and the Minimum Offset for Input 2.

N In

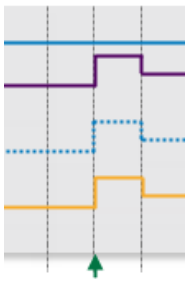
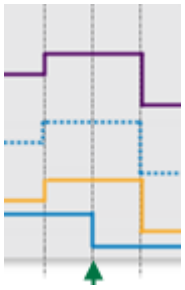
If the input value for *N* is less than or equal to the maximum offset value, and also greater than or equal to the minimum offset value (regardless of duration), then *N In* evaluates to True. Otherwise, it evaluates to False.
Example: *2 In*, refers to the Maximum Offset and the Minimum Offset for Input 2.

N In, with Suppress all minimums…

If the **Suppress all minimums if any input is within limits of offsets** check box is selected, and if any of the other inputs is within limits then the minimum offset is ignored. In these circumstances, if the input value is less than or equal to the Maximum Offset, then *N In* evaluates to True. Otherwise it evaluates to False.

Example: Determining States

The following illustration demonstrates how at 11:00am State 1 is raised when Input 1 evaluates to "above maximum" while Input 3 evaluates to "below minimum".

Input evaluation				Logical evaluation
Input 1 at 11:00am  11:00am **At 11:00am, data for Input 1 is above the maximum offset.** For Input 1, data is "above maximum".		**Input 3 at 11:00am**  11:00am **At 11:00am, data for Input 3 is below the minimum offset.** For Input 3, data is "below minimum".		**1 Max and 3 Min**
1 Max **true**	**and** **and**	**3 Min** **true**		**true**
Input 2 at 11:00am  11:00am **At 11:00am, data for Input 2 is within the offset limits.** For Input 2, data is "within limits", that is it's not "above maximum".		**Input 4 at 11:00am**  11:00am **At 11:00am, data for Input 4 is below the minimum offset.** For Input 4, data is "below minimum".		**2 Max and 4 Min**
2 Max **false**	**and** **and**	**4 Min** **true**		**false**

1 Max AND 3 Min OR 2 Max AND 4 Min evaluates to `TRUE OR FALSE`.

`TRUE OR FALSE` evaluates to `TRUE`. Thus a State 1 event is raised, and State 1 is reached.

Adding a P2 Sentinel Logic Process

The P2 Sentinel Logic Process uses Boolean logic to use the outcome of up to four different inputs to establish various states.

Setting Process Values and Limits

Part of setting up the Logic process involves selecting values, such as the different inputs, the different limits, and the minimum and maximum offsets. Values can either be fixed, or they can be variable data taken from P2 Server tags.

The following values are available. Select a value type from the drop-down list, then type in or select a value.

Fixed Value

If you choose this, type in a fixed numerical value.

Note: This is not an option for *Input 1*.

Attribute

This option is only available if the test's **Source Type** is **Entity** or **Hierarchy**.

Click the ellipsis button to open the P2 Server Attribute Picker, to select an attribute of the source entities.

Source Tag

This option is only available if the **Source Type** is **Tag**.

Calculation

Click the ellipsis button to open the *Edit Calculation* window. The expression is resolved in the P2 Server calculation engine.

If the Source Type is Entity or Hierarchy:
Type a calculation, prefixed by 'this' as the **Source Entity** token, for example: **{this:THP} + 34**.

If the Source Type is Tag:
Type a calculation, prefixed by 'this' as the **Source Tag** token, for example: **{this} * 2**.

Tag

Click the ellipsis button to open the *P2 Server Browser* to select a tag.

Entity Attribute

Click the ellipsis button to open the *P2 Server Browser* to select an entity. From here, select a P2 Server attribute, or attribute value, by using the P2 Server Attribute Picker for the selected entity.

Adding the Process

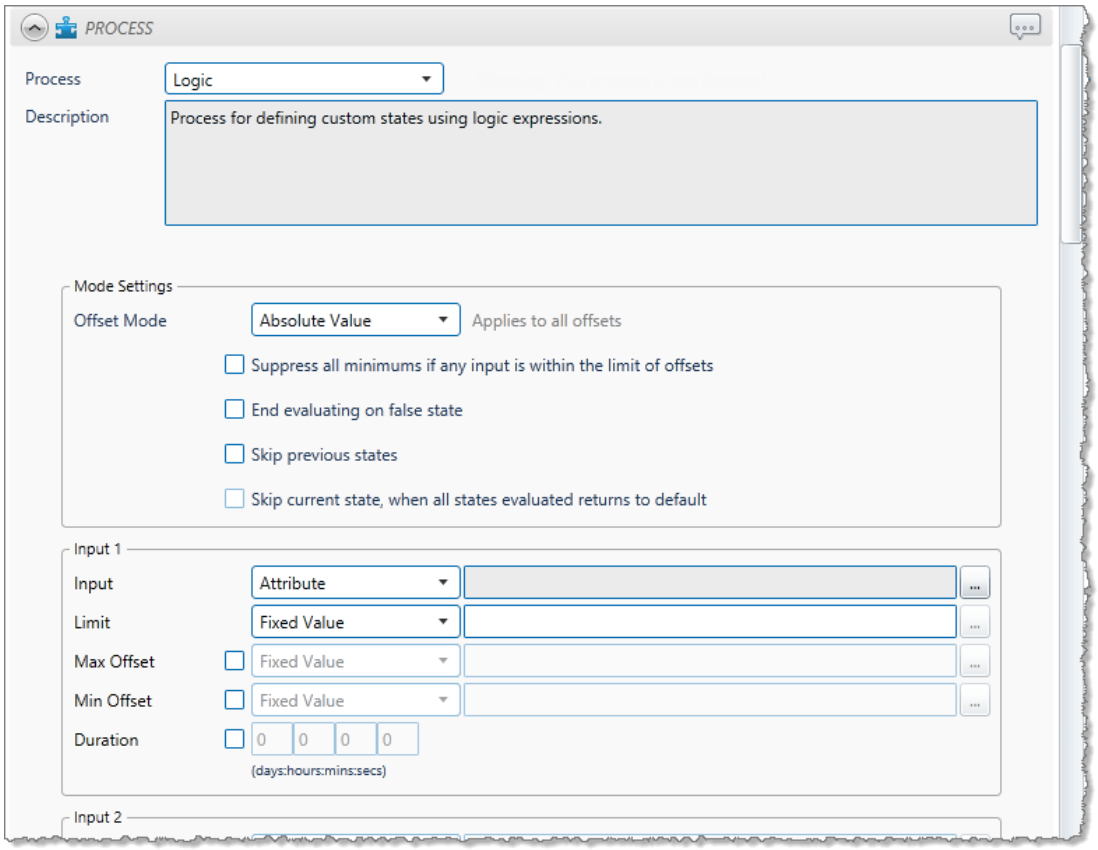
As with all P2 Sentinel processes, the Logic Process is defined within a Sentinel Test page.

Logic Process

In the Sentinel **Test** page:

1. Expand the **Process** panel.
2. Select ***Logic*** from the **Process** drop-down list.

The screen now shows the details for the Logic process.



Define the Mode Settings

The mode settings apply to all of the offsets defined in the process. The following options are available:

Offset Mode

Percentage or ***Absolute Value***. The offset mode determines how the max and min offsets for the various inputs are calculated from their defined limits.

Suppress all minimums if any input is within the limit of offsets

Select the check box if you want to suppress all minimums, when any input is within the offset limits.

End evaluating on false state

Select this check box to stop the process from continuing, after evaluating a state as *false*.

Skip previous states

Select this check box to prevent the process from evaluating previous states and start from the current active state. If at State N, the process will skip evaluation of States 1 to N-1 on next run.

Skip current state, when all states evaluated returns to default

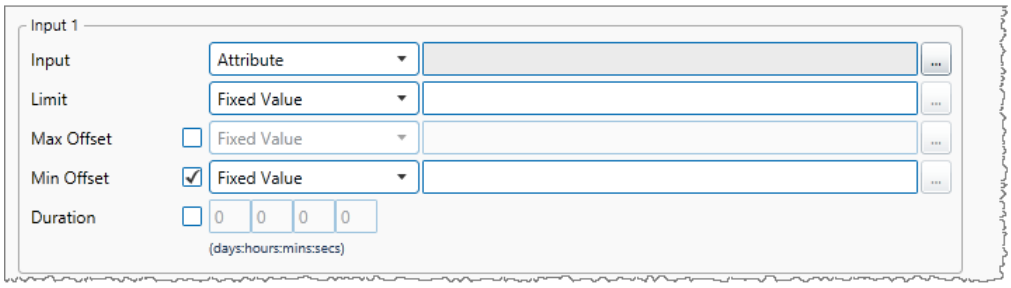
This check box is only available if ***Skip previous states*** has been selected. Select this check box to stop the process from evaluating the current state and previous states. If at State N, the process skips evaluation of State 1 to N and starts at State N+1. Upon reaching the last State, the process will return to a default state.

Select the Inputs

At least one and up to four different Inputs need to be specified for the Logic process.

Define Input 1

Input 1 is required in the Logic process.



1. From the **Input** drop-down list, select one of the following and then select a corresponding value:
   - Attribute (only available if the **Source Type** is *Entity* or *Hierarchy*)
   - Source Tag (only available if the **Source Type** is *Tag*)
   - Calculation
   - Tag
   - Entity Attribute
2. From the **Limit** drop-down list, select one of the following and then type in or select a corresponding value:
   - Fixed Value
   - Attribute (only available if the **Source Type** is *Entity* or *Hierarchy*)
   - Source Tag (only available if the **Source Type** is *Tag*)
   - Calculation
   - Tag
   - Entity Attribute
3. Optionally define a **Max Offset**.

   Note: You must select either a ***Max Offset*** or a ***Min Offset***, or both.

   a. Select the **Max Offset** check box.

   b. From the **Max Offset** drop-down list, select one of the following and then type in or select a corresponding value:
      - Fixed Value
      - Attribute (only available if the **Source** Type is *Entity* or *Hierarchy*)
      - Source Tag (only available if the **Source Type** is *Tag*)
      - Calculation
      - Tag
      - Entity Attribute
4. Optionally define a Min Offset.

   a. Select the **Min Offset** check box.

   b. From the **Min Offset** drop-down list, select one of the following and then type in or select a corresponding value:
      - Fixed Value

- Attribute (only available if the **Source** Type is *Entity* or *Hierarchy*)
- Source Tag (only available if the **Source Type** is *Tag*)
- Calculation
- Tag
- Entity Attribute

5. Optionally define a duration:

   a. Select the **Duration** check box.

   b. Type integer values in the **days**, **hours**, **mins** (minutes), and **secs** (seconds) **Duration Limit** boxes to define a duration period. The default value is zero.

The different value type options are outlined above, in the section: "**Setting Process Values and Limits**", above.

Define Inputs 2, 3 and 4 (Optional)

Input 2, Input 3 and Input 4 are captured in the same way as Input 1. It is important to remember that during processing, the inputs are evaluated in order of precedence (Input 1 having the highest precedent).

6. Select the check box to the left of the relevant *Input* panel (for example *Input 2*).

.

7. From the **Input** drop-down list, select one of the following and then select a corresponding value:

   – Fixed Value
   – Attribute (only available if the **Source** Type is *Entity* or *Hierarchy*)
   – Source Tag (only available if the **Source Type** is *Tag*)
   – Calculation
   – Tag
   – Entity Attribute

8. Capture the Limit, Max Offset, Min Offset and optional Duration for Input 2 (Input 3, Input4), following the instructions for defining Input 1.

Select the Logic State Settings

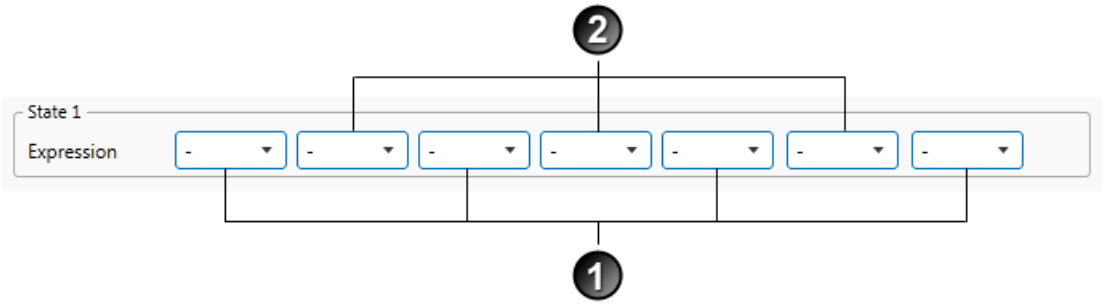
At least one logic state (State 1) and up to eight logic states must be selected for the Logic Process.

For each logic state that you want to set up for the process, do the following:

9. Select the check box to the right of the logic state name.

Note: The **State 1** check box is already selected, as this is a required state for this process.

10. Select the operands and operators to build up a logical expression for the state.



1	Operands 1, 2, 3 and 4
2	Operators 1, 2 and 3

a. Select the first operand from the first drop-down list for State 1.

The operands all relate to the Min Offsets and Max Offsets of the various *Inputs*. All possibilities are listed in the drop-down; however, you may only select valid options (that is, options that are defined in the *Inputs* section). So, for example, you should not select Min 4 if you have not defined *Input 4* as one of your inputs, or if you have not defined a Min Offset for Input 4.

The operand drop-down list comprises of the following:

-
This equates to no selection, and is the default.

1 Min
If the data for Input 1 is lower than the Min Offset for Input 1, for the defined duration (if applicable), *1 Min* evaluates to *True*, otherwise *False*.

1 Max
If the data for Input 1 is higher than the Max Offset for Input 1, for the defined duration (if applicable), *1 Max* evaluates to *True*, otherwise *False*.

1 Out
If the data for Input 1 is either higher than the Max Offset for Input 1, or lower than the Min Offset for Input 1, for the defined duration (if applicable), *1 Out* evaluates to *True*, otherwise *False*.

1 In ("Within Limits")
If the data for Input 1 is between the Max Offset for Input 1, and the Min Offset for Input 1, for the defined duration (if applicable), *1 In* evaluates to *True*, otherwise *False*. If the **Suppress all minimums if any input is within limits of offsets** check box is selected, and any of the other inputs is "within limits", then if data for Input 1 is below the Max Offset for Input 1, *1 In* evaluates to *True*, otherwise *False*.

2 Min
If the data for Input 2 is lower than the Min Offset for Input 2,for the defined duration (if applicable), *2 Min* evaluates to *True*, otherwise *False*.

2 Max
If the data for Input 2 is higher than the Max Offset for Input 2, for the defined duration (if applicable), *2 Max* evaluates to *True*, otherwise *False*.

2 Out
If the data for Input 2 is either higher than the Max Offset for Input 2, or lower than the Min Offset for Input 2, for the defined duration (if applicable), *2 Out* evaluates to *True,* otherwise *False*.

2 In ("Within Limits")
If the data for Input 2 is between the Max Offset for Input 2, and the Min Offset for Input 2, for the defined duration (if applicable), *2 In* evaluates to *True,* otherwise *False*. If the **Suppress all minimums if any input is within limits of offsets** check box is selected, and any of the other inputs is "within limits", then if data for Input 2 is below the Max Offset for Input 2, *2 In* evaluates to *True,* otherwise *False*.

3 Min
If the data for Input 3 is lower than the Min Offset for Input 3, for the defined duration (if applicable), *3 Min* evaluates to *True,* otherwise *False*.

3 Max
If the data for Input 3 is higher than the Max Offset for Input 3, for the defined duration (if applicable), *3 Max* evaluates to *True,* otherwise *False*.

3 Out
If the data for Input 3 is either higher than the Max Offset for Input 3, or lower than the Min Offset for Input 3, for the defined duration (if applicable), *3 Out* evaluates to *True,* otherwise *False*.

3 In ("Within Limits")
If the data for Input 3 is between the Max Offset for Input 3, and the Min Offset for Input 3, for the defined duration (if applicable), *3 In* evaluates to *True,* otherwise *False*. If the **Suppress all minimums if any input is within limits of offsets** check box is selected, and any of the other inputs is "within limits", then if data for Input 3 is below the Max Offset for Input 3, *3 In* evaluates to *True,* otherwise *False*

4 Min
If the data for Input 4 is lower than the Min Offset for Input 4 , for the defined duration (if applicable), *4 Min* evaluates to *True,* otherwise *False*.

4 Max
If the data for Input 4 is higher than the Max Offset for Input 4, for the defined duration (if applicable), *4 Max* evaluates to *True,* otherwise *False*.

4 Out
If the data for Input 4 is either higher than the Max Offset for Input 4, or lower than the Min Offset for Input 4, for the defined duration (if applicable), *4 Out* evaluates to *True,* otherwise *False*.

4 In ("Within Limits")
If the data for Input 4 is between the Max Offset for Input 4, and the Min Offset for Input 4, for the defined duration (if applicable), *4 In* evaluates to *True,* otherwise *False*. If the **Suppress all minimums if any input is within limits of offsets** check box is selected, and any of the other inputs is "within limits", then if data for Input 4 is below the Max Offset for Input 4, *4 In* evaluates to *True,* otherwise *False*

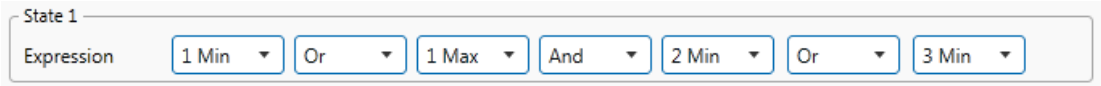
b. Select the first operator from the next drop-down list for State 1.

This is used for the logical evaluation, and can be any of the following:

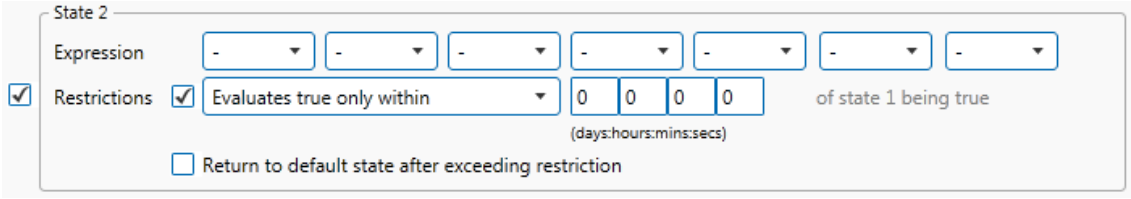
-, And, Or.

c. Select the remaining operands and operators that you want to use for the expression.

The final expression will look similar to this:



11. Continue adding logical expressions for up to 7 additional states, until you have all the states that you want for this process. For each additional state:



a. Select the check box next to the state.

b. Specify the **Expression** to evaluate, as per step 2.

c. If required, apply a **Restriction** by selecting the check box below the expression.

Enabling a restriction allows you to restrict the time that the state can be evaluated as true. The options in the drop-down list are:

Evaluates true only within
This option evaluates the state as true only within the specified time period (DD:HH:MM:SS) of the previous state. This requires the process to only evaluate the state as true within the time restriction. If at State N with time restriction X, then any time after X of State N-1 being evaluated as true will indefinitely return false until the next time State N-1 is raised after departing State N-1.

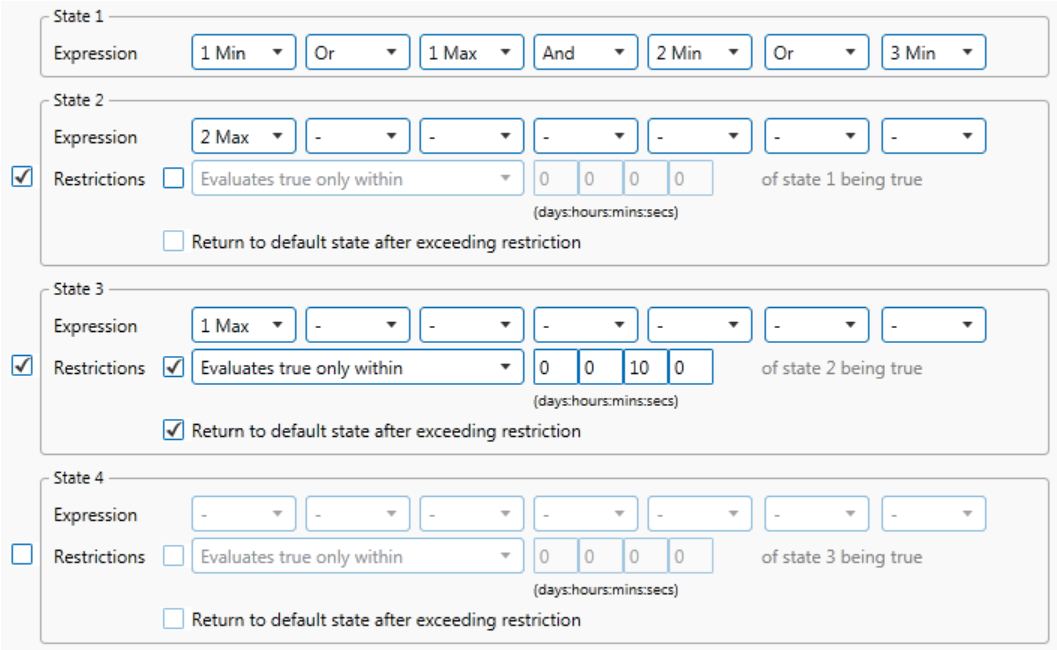
Evaluates true after
This option evaluates the state as true only after the specified time period (DD:HH:MM:SS) of the previous states. This requires the process to only evaluate the state as true after the time restriction. If at State N with time restriction X, then any time before X of State N-1 being evaluating true will return false until the time restriction has been met.

d. If you have applied the above restriction, you also have the option of selecting **Return to default state after exceeding restriction**.

When selected, the process returns to the default state when restrictions have been exceeded, as follows:

- When **Evaluates true only within** is being used, and any time after the time restriction where the state has yet to evaluate to true.
- When **Evaluates true only after** is being used, and if the state evaluates true prior to the time restriction.

The logic states may now look something like this:



Add Comments to the Process Panel

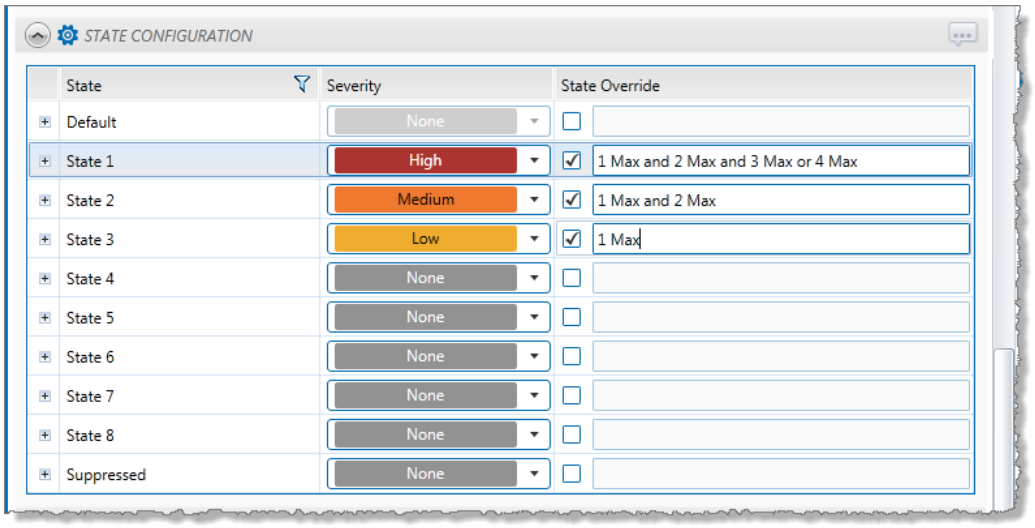
- Click the comment button at the top right of the panel.

Configuring States

For the Logic process, you can configure the following states, each with an optional state override and comments:

- Default
- State 1
- State 2
- State 3
- State 4
- State 5
- State 6
- State 7
- State 8
- Suppressed

You cannot change the severity of the Default state; however, you can add a state override and comments.



Note: Only configure states where you have set a limit.

To configure the state outcomes for a test in the **State Configuration** panel of the test, see 3.6 Configure States. If Case Management is enabled in Sentinel, this is also where you manage cases.

Appendix J. Performance Curve Process

The Performance Curve process compares process variable data against limits and conditions that are defined by a performance curve. The performance curve uses a polynomial equation with coefficient and constant values from either fixed values or P2 Server entities, or a combination of both.

Performance Curve is a complex process capable of concurrently monitoring multiple conditions such as transgression of limits, state duration, and movement between states.

State Transition Rules

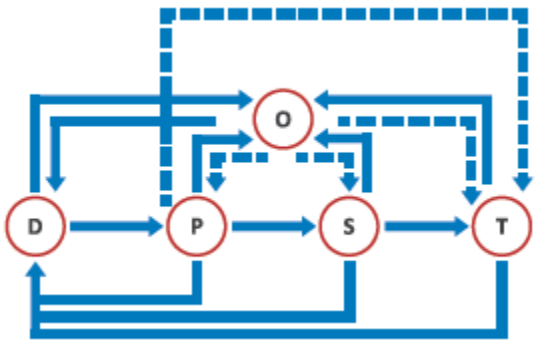
The Performance Curve process has clearly defined state transition logic paths. Transition from one state to another is equally dependant on the current evaluation of data, and on the current state.

State transitions cause events to be raised, allowing for the escalation of actions via the P2 Sentinel framework. Different actions can be assigned to different state outcomes.

The following table outlines the allowable state transitions of the Performance Curve process.

This state can transition	To this state	Under these conditions
Default	Primary	Data has transgressed the primary state upper or lower deviation limits.
	Out of Range	The x value of the data is not within the range defined by Min X and Max X.
Primary	Secondary	Any of the secondary state conditions have been met.
	Tertiary	Only if the tertiary deviation limit is breached.
	Default	Data is not erroneous, and is within the deviation limits of the curve.
Secondary	Tertiary	Any of the tertiary state conditions has been met.
	Default	Data is not erroneous, and is within the deviation limits of the curve.
	Out of Range	The x value of the data is not within the range defined by Min X and Max X.
Tertiary	Default	Data is not erroneous, and is within the deviation limits of the curve.
	Out of Range	The x value of the data is not within the range defined by Min X and Max X.
Out of Range	Default	When data comes out of an Out of Range state, the state transition logic is applied to whatever the previous state was. So if, for example, the previous state was the primary state, a secondary state can be reached if any of the secondary state conditions have been met.
	Primary	
	Secondary	
	Tertiary	

The following diagram outlines the state transition logic of the Performance Curve process.



D Default

P Primary

S Secondary

T Tertiary

O Out of Range

Test Outcomes

A number of outcomes are possible when the Performance Curve process is executed:

Default State

Data is not in an erroneous state and is within the operating envelope.

Primary State

Data is measured against the defined fixed or variable primary deviation limit (upper and/or lower). If it breaches a primary deviation limit, a primary state is reached, and a primary event is raised.

Secondary State

A number of possible conditions can cause a secondary state. These are explained in more detail in the Secondary State section, further on in the document.

Tertiary State

As with the secondary state, a number of conditions can cause a tertiary state. These are explained in more detail in the Tertiary State section, further on in the document.

Out of Range State

When the X coordinate of the data falls outside the range defined by Min X and Max X, and Out of Range State is reached. This is explained in more detail in the Out of Range State section, further on in the document.

Suppressed State

The monitor has been suppressed. For example, if the precondition has not been met.

Conditional Logic

The Performance Curve process provides the following conditional logic.

Note: All of the example graphs in the following sections show tests that have used the Last Known Value sample method.

Input Settings

Depending on which ***Input Mode*** is selected, you will need to define various other input settings.

Choose between the ***Values*** input mode (where both the x and the y parameters can be fixed values or variable P2 server entities), and the ***Liquid Control Valve*** input mode.

Liquid Control Valve

The specialised Liquid Control Valve input mode uses the Flow Coefficient Equation (see diagram below) to calculate the Y value, based on specified (fixed or variable) values for: Flow Rate (F), Specific Gravity (SG) and Pressure Drop (P).

$$C_v = F\sqrt{\frac{SG}{\Delta P}}$$

Values

The Values input mode is used when you are not specifically measuring a Liquid Control Valve.

Curve Settings

Choose between the X-Y Values *curve type*, where a fixed, limited list of x and y values are manually captured, and the Polynomial curve type.

The Polynomial curve uses coordinates that are calculated at every sample interval, based on the x and y (fixed or variable) input values, creating a potentially varying range of deviation limits, whereas the X-Y Values creates a static set of limits that is the same at every sample interval. Polynomials can be set from zero (straight line), to nine degrees (more complex curve). Coordinates to the polynomial equation can also be fixed or variable.

Min X and Max X

Define out of range limits for the x value of the data.

Chart Preview

The Performance Curve uses a graph to map out values based on the selected formula with the specified deviations. Use the **Convert to XY Values** functionality to help with adjusting the polynomial curves.

For a polynomial curve type, if the process uses a hierarchy as the process source and a P2 Server entity in the curve settings, you can select which entity to preview in the chart.

Mode Settings

Define whether the deviation mode is a percentage or an absolute value, to establish how primary, secondary and tertiary deviation limits are calculated. Also select whether to set upper or lower deviation limits, or both.

The Rolling Sum Period

A secondary state rolling sum period can be defined for evaluating some of the secondary state conditions; likewise, a tertiary state rolling sum period can be defined for evaluating some of the tertiary state conditions.

The rolling sum period is a defined period (specified in days and hours). At every sample interval, the rolling sum period is that period preceding the sample interval. So, for example, if the secondary state rolling sum period is set at 1 day 2 hours then at 3pm on Tuesday 15 January 2013, the secondary state rolling sum period is from 1pm on Monday 14 January (covering the last 1 day and 2 hours). Any evaluations relating to that sample interval's secondary state rolling sum period conditions must fall within that time.

Primary State Deviation Limit

The primary state deviation limit must be set for the process to work.

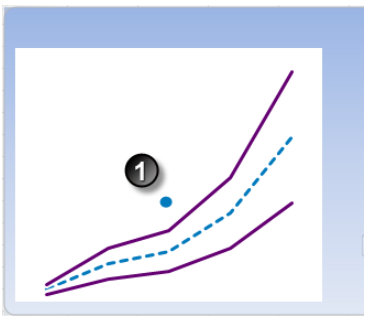
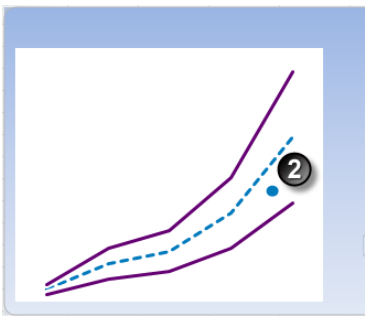
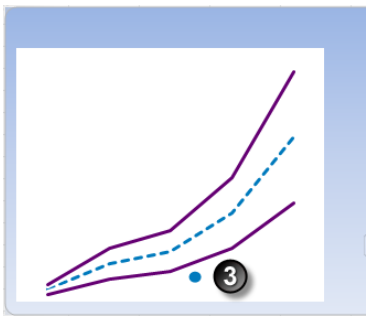
If the configured primary state deviation limit is breached, a primary event occurs, and a primary state is reached.

Example of a Primary State Deviation Limit

The following chart demonstrates a breach of the primary deviation limit, causing a primary event to occur.

- Input mode is values.
- Deviation mode is percentage.
- Limits are set for upper deviation and lower deviation.
- Curve settings are X-Y values; that is, they are static.
- The sample interval is every two hours.

Data item | Expected curve | Primary deviation limit

5:00am	7:00am	9:00am
		
1 At **5:00am**, the **X** and **Y** coordinates of the data place it beyond the primary deviation limit. A primary state is reached, and a primary event is raised.	2 At **7:00am**, the **X** and **Y** co-ordinates of the data place it within an acceptable range. A default state is reached, and a default event is raised.	3 At **9:00am**, the **X** and **Y** coordinates of the data place it beyond the primary deviation limit again. A primary state is reached, and a primary event is raised.

Secondary State

There are several possible ways to reach the secondary state outcome in the Performance Curve process:

- Secondary State Deviation Limit
- Secondary State Duration Limit
- Secondary State Sustained Value Limit
- Secondary State Rolling Sum Total Duration Limit
- Secondary State Rolling Sum Breach Occurrences Limit

You can choose to set one or more conditions to trigger the secondary state. For example, a test may have a secondary deviation limit defined, as well as configured variables for determining secondary state rolling sum breach occurrences.

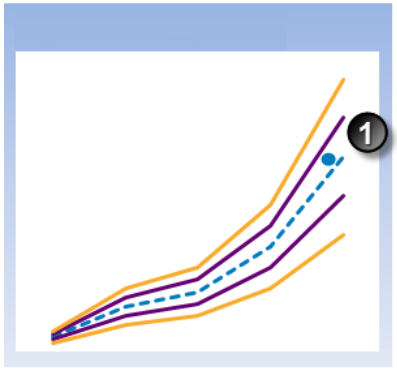
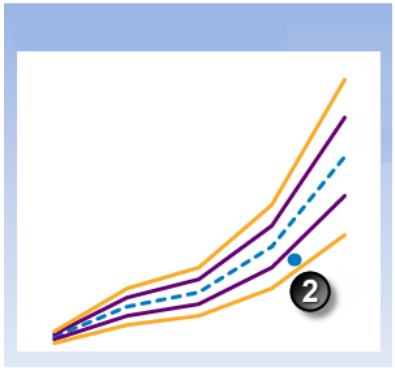
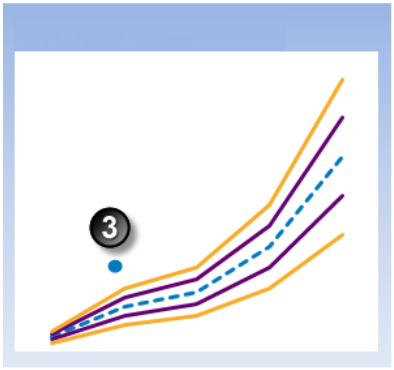
Secondary State Deviation Limit

If the configured secondary deviation limit is breached, a secondary event occurs, and a secondary state is reached.

Example of Secondary State Deviation Limit

The example depicted below demonstrates a breach of the secondary deviation limit, causing a secondary event to occur.

• Input mode is values. • *Deviation mode* is a percentage value.	• *Curve settings* are X-Y values; that is, they are static. • The sample interval is every two hours.
Data item Primary deviation limit	Expected curve Secondary deviation limit

5:00am	7:00am	9:00am
		
1 At **5:00am**, the **X** and **Y** coordinates of the data place it below the *upper primary deviation limit*. A default state is reached, and a **default** event is raised.	2 At **7:00am**, the **X** and **Y** coordinates of the data place it below the *lower primary deviation limit*. A primary state is reached, and a **primary** event is raised.	3 At **9:00am**, the **X** and **Y** coordinates of the data place it above the *upper secondary deviation limit*. A secondary state is reached, and a **secondary** event is raised.

Secondary State Duration Limit

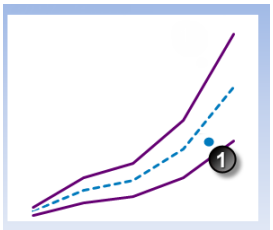
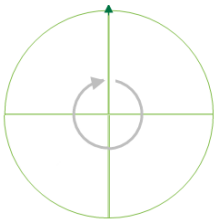
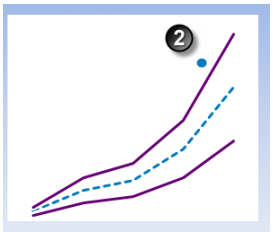
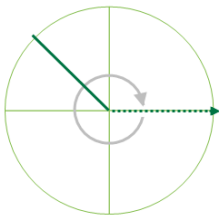
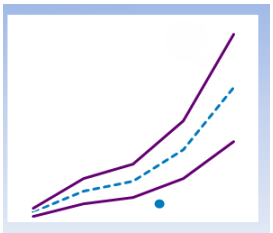
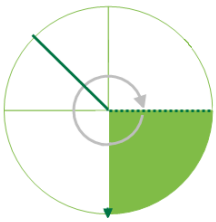
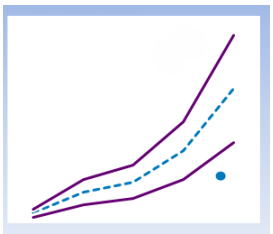
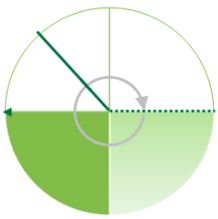
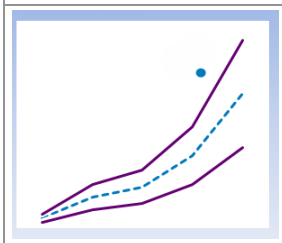
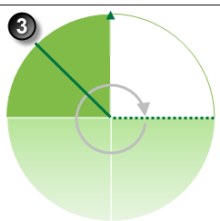
Monitor for data that continuously exceeds the primary deviation limit, for longer than the secondary state duration limit.

If data that continuously exceeds the primary deviation limit for longer than specified in the secondary state duration limit, a secondary event occurs, and a secondary state is reached.

Example of Secondary State Duration Limit

- Input mode is values.
- Deviation mode is a percentage value.
- Secondary state duration is set to 5 hours.
- Curve settings are X-Y values; that is, they are static.
- The sample interval is every two hours.

Data item | Primary state duration | Expected curve
Start of primary state | Primary deviation limit | Current time

Duration and Limits		Duration of data continuously exceeding the primary deviation limit	
	1 At **1:00am**, the **X** and **Y** coordinates of the data place it above the *lower primary deviation limit*. A default state is reached, and a **default** event is raised.		At **1:00am**, *primary state duration is at zero*.
	2 At **3:00am**, the **X** and **Y** coordinates of the data place it above the *upper primary deviation limit*. A primary state is reached, and a **primary** event is raised.		At **3:00am**, *primary state duration is at zero*. The *primary limit has been exceeded*, so timing of primary duration starts now.
	At **5:00am**, the **X** and **Y** coordinates of the data place it below the *lower primary deviation limit*. The primary state endures.		At **5:00am**, *primary state duration is now at 2 hours* (a full sample interval).
	At **7:00am**, the **X** and **Y** coordinates of the data place it below the *lower primary deviation limit*. The primary state endures.		At **7:00am**, *primary state duration is now at 4 hours* (two full sample intervals).
	At **9:00am**, the **X** and **Y** coordinates of the data place it above the *upper primary deviation limit*. The primary state endures.		3 At **9:00am**, *primary state duration is now at 6 hours*, exceeding the secondary state duration limit of 5 hours. A secondary state is reached, and a **secondary** event is raised.

Secondary State Sustained Value Limit

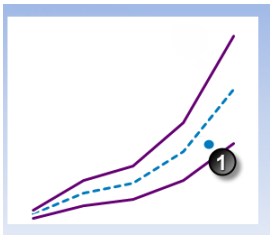
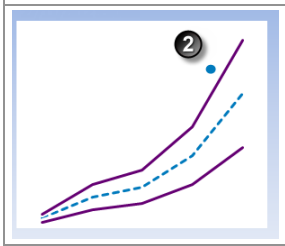
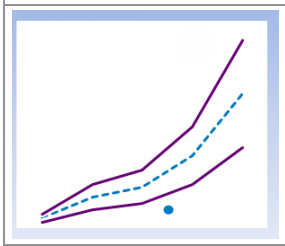
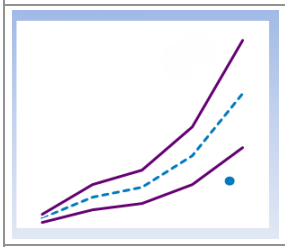
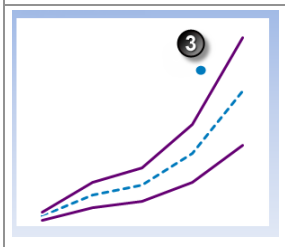
Monitor for when data exceeds the primary deviation limit for more than a specified number of times (secondary state, sustained value limit), consecutively. If this is the case, a secondary event occurs and a secondary state is reached.

Example of Secondary State Sustained Value Limit

- Input mode is values.
- *Curve Settings* are X-Y values; that is, they are static.
- Secondary state sustained value limit is set to 3.
- *Deviation mode* is a percentage value.
- The sample interval is every two hours.

Data item	Primary state duration	Expected curve
Start of primary state	Primary deviation limit	Occurrence counter

Duration and Limits

	1 At **1:00am**, the **X** and **Y** coordinates of the data place it above the *lower primary deviation limit*. A default state is reached, and a **default** event is raised.	0 At **1:00am**, the *primary deviation limit has been exceeded zero times*.
	2 At **3:00am**, the **X** and **Y** coordinates of the data place it above the *upper primary deviation limit*. A primary state is reached, and a **primary** event is raised.	1 At **3:00am**, the *primary deviation limit has been exceeded once*.
	At **5:00am**, the **X** and **Y** coordinates of the data place it below the *lower primary deviation limit*. The primary state endures.	2 At **5:00am**, the *primary deviation limit has been exceeded twice (consecutively)*.
	At **7:00am**, the **X** and **Y** coordinates of the data place it below the *lower primary deviation limit*. The primary state endures.	3 At **7:00am**, *the primary deviation limit has been exceeded three times (consecutively)*.
	At **9:00am**, the **X** and **Y** coordinates of the data place it above the *upper primary deviation limit*. The primary state endures.	4 3 At **9:00am**, the primary deviation limit *has been exceeded four times (consecutively)*, surpassing the secondary state sustained value limit of 3. A secondary state is reached, and a **secondary** event is raised.

Secondary State Rolling Sum Total Duration Limit

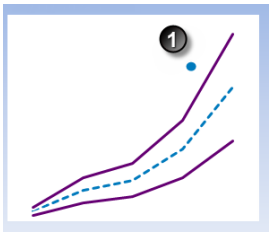
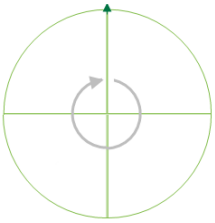
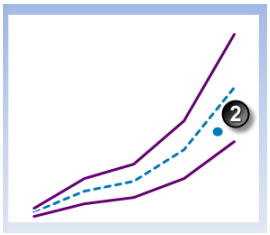
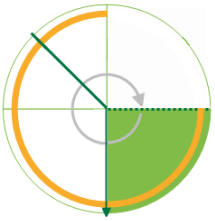
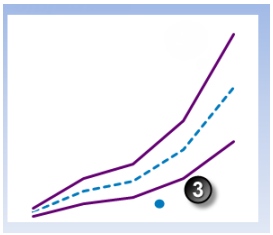
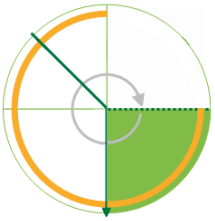
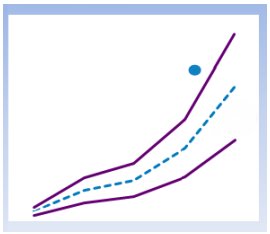
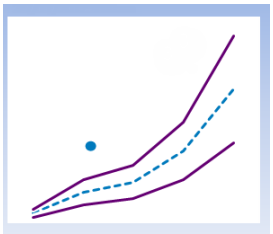
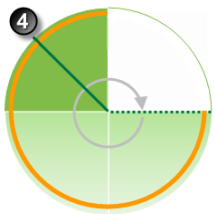
Monitor for a specified accumulated duration of all periods where data is in breach of the primary deviation limit, within the preceding specified secondary state rolling sum period.

If the total combined primary state duration is longer than the specified secondary state rolling sum duration limit, a secondary event occurs, and a secondary state is reached.

Example of Secondary State Rolling Sum Total Duration Limit

- Input mode is values.
- Curve settings are X-Y values; that is, they are static.
- Secondary state duration is set at 5 hours.
- Deviation mode is a percentage value.
- The sample interval is every two hours.

Data item | Primary state duration | Expected curve | Current rolling sum period
Start of primary state | Primary deviation limit | Current time

Duration and Limits		Accumulated duration of data exceeding the primary deviation limit	
	1 At **1:00am**, the **X** and **Y** coordinates of the data place it above the *upper primary deviation limit*. A primary state is reached, and a **primary** event is raised.		At **1:00am**, duration is at zero. *Primary limit has been exceeded*, so timing starts now.
	2 At **3:00am**, the **X** and **Y** coordinates of the data place it *between the upper and lower primary deviation limits*. A default state is reached, and a **default** event is raised.		At **3:00am**, *the accumulated duration is now at 2 hours* (a full sample interval). The process is no longer in the primary state, so timing stops.
	3 At **5:00am**, the **X** and **Y** coordinates of the data place it below the *lower primary deviation limit*. A primary state is reached, and a **primary** event is raised.		At **5:00am**, *the accumulated duration remains at 2 hours* (a single sample interval). The *primary limit has been exceeded, so timing starts again.*
	At **7:00am**, the **X** and **Y** coordinates of the data place it above the *upper primary deviation limit*.		At **7:00am**, *the accumulated duration is now at 4 hours* (two full sample intervals). The process is still in the primary state, so timing continues.
	At **9:00am**, the **X** and **Y** coordinates of the data place it above the *upper primary deviation limit*.		4 At **9:00am**, *the accumulated duration is now at 6 hours*, exceeding the secondary state duration limit of 5 hours. A secondary state is reached, and a **secondary** event is raised.

Secondary State Rolling Sum Breach Occurrences Limit

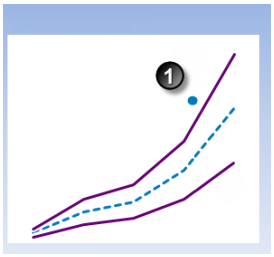
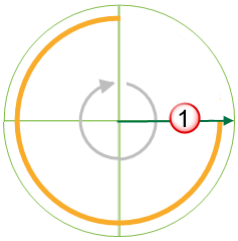
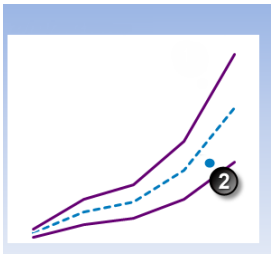
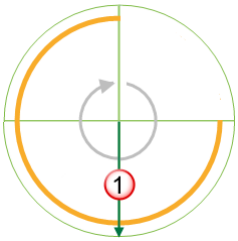
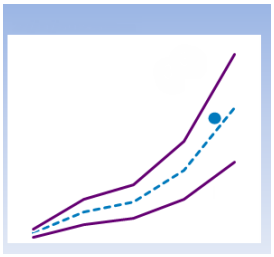
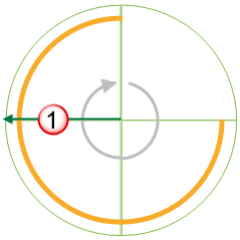
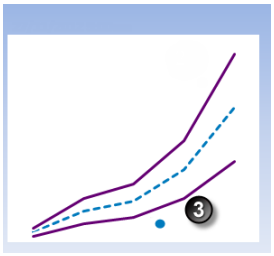
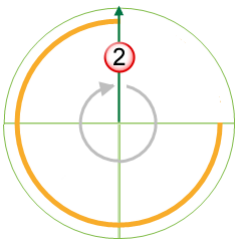
Monitor for when a set number of values (secondary state breach occurrences limit) has breached the primary deviation limit, during the preceding specified secondary rolling sum period.

Example of Secondary State Rolling Sum Breach Occurrences Limit

In the following example, the secondary state breach occurrences limit is set to 2.

- Input mode is values.
- Curve settings are X-Y values; that is, they are static.
- Secondary state rolling sum breach occurrences limit is set at 2.
- Deviation mode is a percentage value.
- The sample interval is every two hours.

Data item
Primary state duration
Expected curve
Start of primary state
Primary deviation limit
Occurrence counter
Current rolling sum period

Duration and Limits		Accumulated Breach Occurrences	
	1 At **1:00am**, the **X** and **Y** coordinates of the data place it above the *upper primary deviation limit*. A primary state is reached, and a **primary** event is raised.		At **1:00am**, breach occurrences counter is one.
	2 At **3:00am**, the **X** and **Y** coordinates of the data place it between the *upper and lower primary deviation limits*. A default state is reached and a **default** event is raised.		At **3:00am**, breach occurrences counter remains at one.
	At **5:00am**, the **X** and **Y** coordinates of the data place it between the *upper and lower primary deviation limits*. The default state endures.		At **5:00am**, breach occurrences counter remains at one.
	3 At **7:00am**, the **X** and **Y** coordinates of the data place it below the *lower primary deviation limit*. A primary state is reached and a **primary** event is raised.		4 At **7:00am**, breach occurrences counter reaches two. A secondary state is reached and a **secondary** event is raised.

Tertiary State

There are several ways to reach the tertiary state outcome in the Performance Curve process:

- Tertiary State Deviation Limit
- Tertiary State Duration Limit
- Tertiary State Sustained Value Limit
- Tertiary State Rolling Sum Total Duration Limit
- Tertiary State Rolling Sum Breach Occurrences Limit

You can choose to set one or more conditions to trigger the tertiary state. For example, a test may have a tertiary deviation limit defined, as well as configured variables for determining tertiary state rolling sum breach occurrences.

Tertiary State Deviation Limit

If the configured tertiary deviation limit is breached, a tertiary event occurs, and a tertiary state is reached.

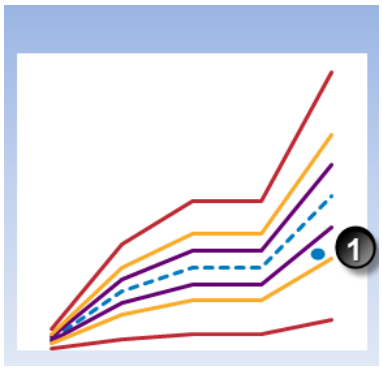
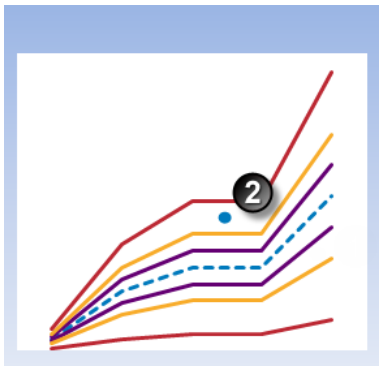
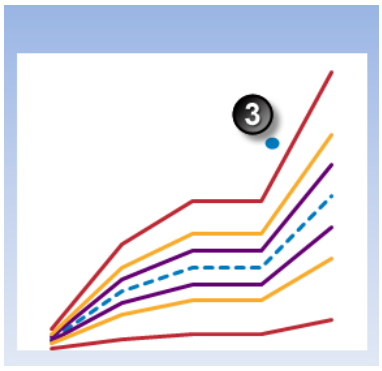
The graph demonstrates a breach of the tertiary deviation limit, causing a tertiary event to occur.

Example of Breach of Tertiary State Deviation Limit

The example depicted below demonstrates a breach of the tertiary deviation limit, causing a tertiary event to occur.

- Input mode is values.
- Curve settings are X-Y values; that is, they are static.
- Deviation mode is a percentage value.
- The sample interval is every two hours.

Data item | Expected curve | Primary deviation limit
Secondary deviation limit | Tertiary deviation limit

5:00am	7:00am	9:00am
		
1 At **5:00am**, the **X** and **Y** coordinates of the data place it below the *lower primary deviation limit*. A primary state is reached, and a **primary** event is raised.	2 At **7:00am**, the data **X** and **Y** coordinates of the data place it above the *upper secondary deviation limit*. A secondary state is reached, and a **secondary** event is raised.	3 At **9:00am**, the **X** and **Y** coordinates of the data place it above the *upper tertiary deviation limit*. A tertiary state is reached, and a **tertiary** event is raised.

Tertiary State Duration Limit

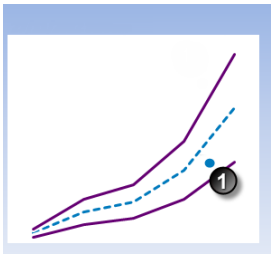
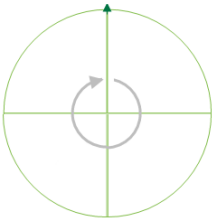
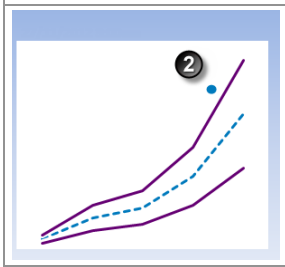
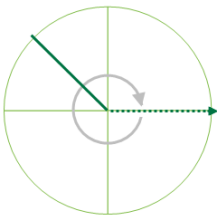
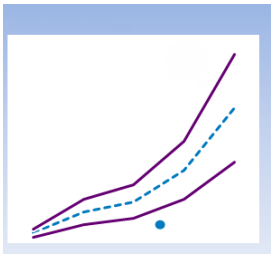
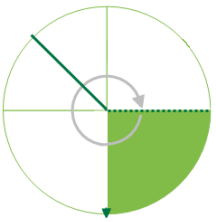
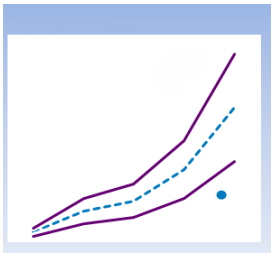
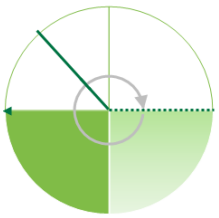
Monitor for data that continuously exceeds the primary deviation limit, for longer than the tertiary state duration limit.

If data that continuously exceeds the primary deviation limit for longer than specified in the tertiary state duration limit, a tertiary event occurs, and a tertiary state is reached.

Example of Tertiary State Duration Limit

- Input mode is values.
- Curve settings are X-Y values; that is, they are static.
- Secondary state duration is set at 1.5 hours.
- Deviation mode is a percentage value.
- The sample interval is every two hours.
- Tertiary state duration is set at 3.5 hours.

Data item | Primary state duration | Expected curve
Start of primary state | Primary deviation limit | Current time

Duration and Limits		Duration of data continuously exceeding the primary deviation limit
	1 At **1:00am**, the **X** and **Y** coordinates of the data place it between the *upper and lower primary deviation limits*. A default state is reached, and a **default** event is raised.	 At **1:00am**, *duration is at zero.*
	2 At **3:00am**, the **X** and **Y** coordinates of the data place it above the *upper primary deviation limit*. A primary state is reached, and a **primary** event is raised.	 At **3:00am**, *duration is at zero.* Primary limit has been exceeded, so timing starts now.
	At **5:00am**, the **X** and **Y** coordinates of the data place it below the *lower primary deviation limit*. The primary state endures.	 At **5:00am**, *duration is now at 2 hours* (a full sample interval), exceeding the secondary state duration limit of 1.5 hours. A secondary state is reached, and a **secondary** event is raised.
	At **7:00am**, the **X** and **Y** coordinates of the data place it below the *lower primary deviation limit*. The secondary state endures.	 3 At **7:00am**, *data has exceeded the primary deviation for 4 consecutive hours* (two full sample intervals), exceeding the secondary state duration limit of 3.5 hours. A tertiary state is reached, and a **tertiary** event is raised.

Tertiary State Sustained Value Limit

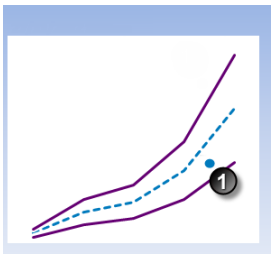
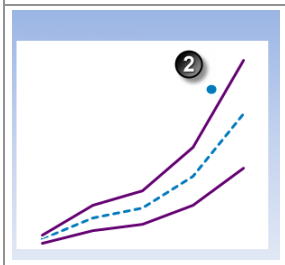
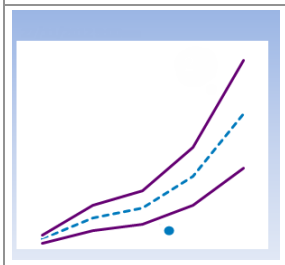
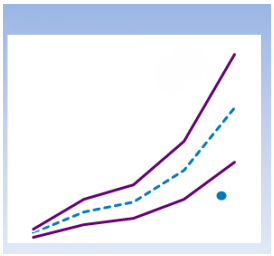
Monitor for when data exceeds the primary deviation limit for more than a specified number of times (tertiary state sustained value limit), consecutively. If this is the case, a tertiary event occurs, and a tertiary state is reached.

Example of Tertiary State Sustained Value Limit

- Input mode is values.
- Curve settings are X-Y values; that is, they are static.
- Secondary state sustained value limit is set at 2.
- Deviation mode is a percentage value.
- The sample interval is every two hours.
- Tertiary state sustained value limit is set at 3.

Data item	Primary state duration	Expected curve
Start of primary state	Primary deviation limit	Occurrence counter

Duration and Limits

	1 At **1:00am**, the **X** and **Y** coordinates of the data place it between the *upper and lower primary deviation limits*. A default state is reached, and a **default** event is raised.	0 At **1:00am**, the *primary deviation limit has been exceeded zero times*.
	2 At **3:00am**, the **X** and **Y** coordinates of the data place it above the *upper primary deviation limit*. A primary state is reached, and a **primary** event is raised.	1 At **3:00am**, the *primary deviation limit has been exceeded once*.
	At **5:00am**, the **X** and **Y** coordinates of the data place it below *the lower primary deviation limit.*	2 3 At **5:00am**, the *primary deviation limit has been exceeded twice (consecutively)*. In this example, this is the secondary sustained value limit, so a secondary state is reached, and a **secondary** event is raised.
	At **7:00am**, the **X** and **Y** coordinates of the data place it beyond the primary deviation limit.	3 4 At **7:00am**, the *primary deviation limit has been exceeded three times (consecutively)*. In this example, this is the tertiary sustained value limit, so a tertiary state is reached, and a **tertiary** event is raised.

Tertiary State Rolling Sum Total Duration Limit

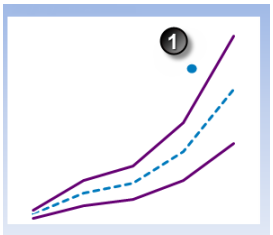
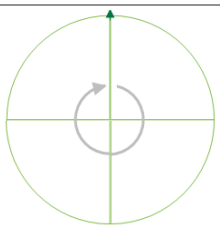
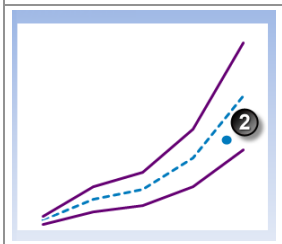
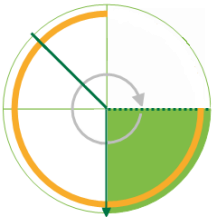
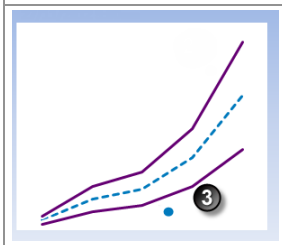
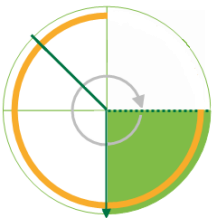
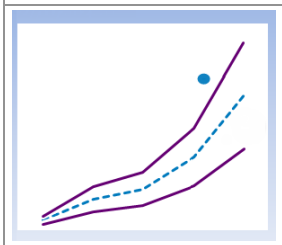
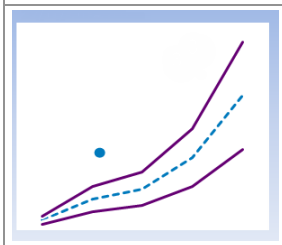
Monitor for a specified accumulated duration of all periods where data is in breach of the primary deviation limit, within the preceding specified tertiary state rolling sum period.

If the total combined primary state duration is longer than the specified tertiary state rolling sum duration limit, a tertiary event occurs, and a tertiary state is reached.

Example of Tertiary State Rolling Sum Total Duration Limit

- Input mode is values.
- Curve settings are X-Y values; that is, they are static.
- Secondary state duration is set at 3.5 hours.
- Deviation mode is a percentage value.
- The sample interval is every two hours.
- Tertiary state duration is set at 5 hours.

Data item | Exceeding primary limits | Expected curve | Current rolling sum period
Start of primary state | Primary deviation limit | Current time

Duration and Limits		Accumulated duration of data exceeding the primary deviation limit	
	1 At **1:00am**, the **X** and **Y** coordinates of the data place it above the *upper primary deviation limit*. A primary state is reached, and a **primary** event is raised.		At **1:00am**, *duration is at zero*. Primary limit has been exceeded, so timing starts now.
	2 At **3:00am**, the **X** and **Y** coordinates of the data place it between the *upper and lower primary deviation limits*. A Default State is reached, and a **default** event is raised.		At **3:00am**, *the accumulated duration is now at 2 hours* (a full sample interval). Input data is no longer exceeding the primary limits, so timing stops.
	3 At **5:00am**, the **X** and **Y** coordinates of the data place it below the *lower primary deviation limit*. A primary state is reached, and a **primary** event is raised.		At **5:00am**, *the accumulated duration remains at 2 hours* (a single sample interval). Input data is beyond primary limits, so timing resumes.
	At **7:00am**, the **X** and **Y** coordinates of the data place it of the data place it above the *upper primary deviation limit*.		4 At **7:00am**, *the accumulated duration is now at 4 hours* (two full sample intervals), exceeding the secondary state duration limit. A secondary state is reached, and a **secondary** event is raised.
	At **9:00am**, the **X** and **Y** coordinates of the data place it above the *upper primary deviation limit*.		5 At **9:00am**, the *accumulated duration is now at 6 hours*, exceeding the tertiary state duration limit. A tertiary state is reached, and a **tertiary** event is raised.

Tertiary State Rolling Sum Breach Occurrences Limit

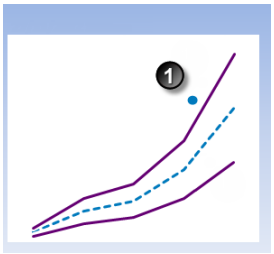
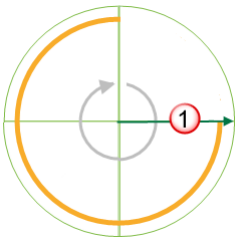
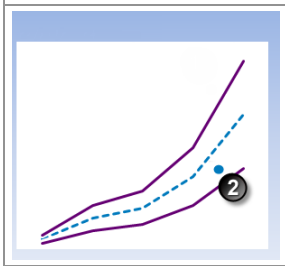
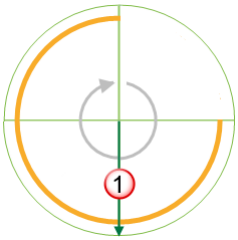
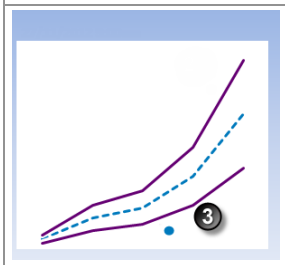
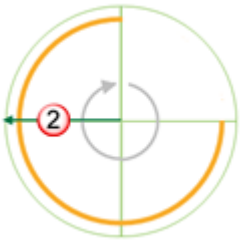
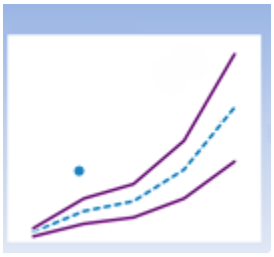
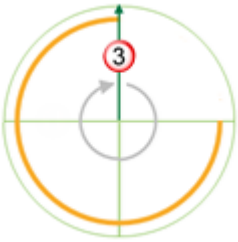
Monitor whether a set number of values (tertiary state breach occurrences limit) has breached the primary deviation limit, during the preceding specified tertiary rolling sum period. If this occurs, a tertiary event is raised, and a tertiary state is reached.

Example of Tertiary State Rolling Sum Breach Occurrences Limit

In the following example, the tertiary state rolling sum breach occurrences limit is set to **3**.

- Input mode is values.
- Curve settings are X-Y values; that is, they are static.
- Secondary state rolling sum breach occurrences limit is set to 2.
- Deviation mode is a percentage value.
- The sample interval is every two hours.
- Tertiary state rolling sum breach occurrences limit is set to 3.

Data item
Primary state duration
Expected curve
Start of primary state
Primary deviation limit
Occurrence counter
Current rolling sum period

Duration and Limits		Accumulated Breach Occurrences	
	1 At **1:00am**, the **X** and **Y** coordinates of the data place it above the *upper primary deviation limit*. A primary state is reached, and a **primary** event is raised.		At **1:00am**, *breach occurrences counter is one*.
	2 At **3:00am**, the **X** and **Y** coordinates of the data place it between the *upper and lower primary deviation limits*. A default state is reached and a **default** event is raised.		At **3:00am**, *breach occurrences counter remains at one*.
	3 At **5:00am**, the **X** and **Y** coordinates of the data place it below the *lower primary deviation limit*. A primary state is reached and a **primary** event is raised.		4 At **5:00am**, *breach occurrences counter reaches two*. A secondary state is reached and a **secondary** event is raised.
	At **7:00am**, the **X** and **Y** coordinates of the data the **X** and **Y** coordinates of the data place it above the upper primary deviation limit.		5 At **7:00am**, *breach occurrences counter reaches three*. A tertiary state is reached and a **tertiary** event is raised.

Out of Range State

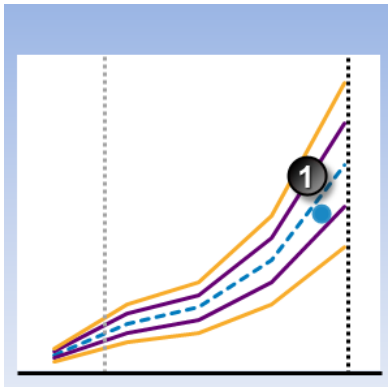
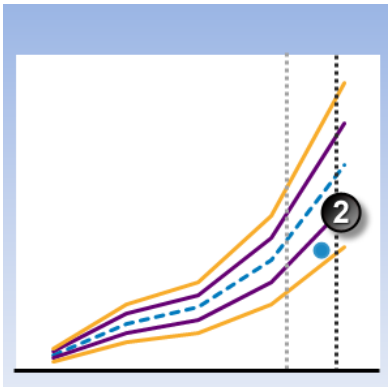
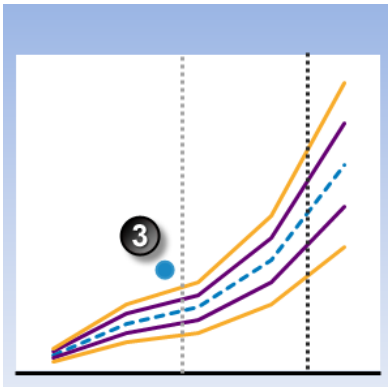
If the X coordinate of the data is outside the range defined by ***Min X*** and ***Max X***, an ***out of range*** event occurs, and an ***out of range*** state is reached.

Example of an Out of Range State

In the following example, Min X and Max X are both fixed values.

- Input mode is values.
- Curve settings are X-Y values; that is, they are static.
- Secondary state rolling sum breach occurrences limit is set at 2.
- Deviation mode is a percentage value.
- The sample interval is every two hours.
- Min X and Max X are both fixed values.

Data item | Expected curve
Primary deviation limit | Secondary deviation limit
Min X | Max X | X Axis

5:00am	7:00am	9:00am
		
1 At **5:00am**, the **X** and **Y** coordinates of the data place it between the *upper and lower deviation limits.* A default state is reached, and a **default** event is raised.	2 At **7:00am**, the data **X** and **Y** coordinates of the data place it below the *lower primary deviation limit*. A primary state is reached, and a **primary** event is raised.	At **9:00am**, the **X** and **Y** coordinates of the data place it above the *upper secondary deviation limit*. This would normally cause a secondary event.
Evaluate whether the X coordinate is within the range.		
In addition, *the X coordinate is within the range defined by Min X and Max X.*	In addition, *the X coordinate is within the range defined by Min X and Max X.*	3 However, because *the X coordinate of the data is not between the range defined by Min X and Max X*, an **out of range** state is reached and an **out of range** event is raised.

Adding a Performance Curve Process

The Performance Curve Process compares process variable data against defined limits and conditions. If a limit or condition is breached when the process is executed, a new state is reached and an event is raised.

Setting Process Values and Limits

Part of setting up the Performance Curve process involves selecting limits, such as the primary state deviation limit, secondary state deviation limit, tertiary state deviation limit, breach occurrences limits and so on. Limits can either be fixed values, or they can be variable data taken from P2 Server entities.

The following limits are available. Select a limit type from the drop-down list, then type in or select a limit.

Fixed Value

Type in a numerical value.

Attribute

This option is only available if the test's **Source Type** is **Entity** or **Hierarchy**.

Click the ellipsis  button to open the P2 Server Attribute Picker, to select an attribute of the source entities.

Source Tag

This option is only available if the **Source Type** is **Tag**.

Calculation

Click the ellipsis  button to open the *Edit Calculation* window. The expression is resolved in the P2 Server calculation engine.

If the Source Type is Entity or Hierarchy:
Type a calculation, prefixed by 'this' as the **Source Entity** token, for example: **{this:THP} + 34**.

If the Source Type is Tag:
Type a calculation, prefixed by 'this' as the **Source Tag** token, for example: **{this} * 2**.

Tag

Click the ellipsis  button to open the *P2 Server Browser* to select a tag.

Entity Attribute

Click the ellipsis  button to open the *P2 Server Browser* to select an entity. From here, select a P2 Server attribute, or attribute value, by using the P2 Server Attribute Picker for the selected entity

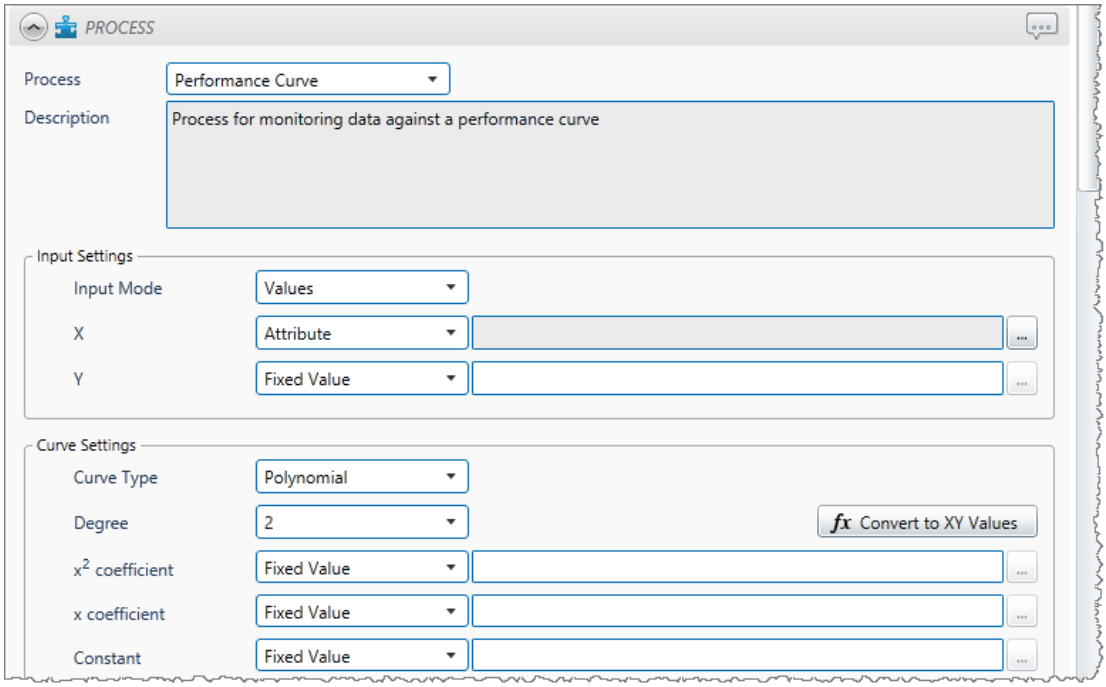
Adding the Process

As with all P2 Sentinel processes, the Performance Curve Process is defined within a Sentinel Test page.

Performance Curve Process

In the Sentinel **Test** page:

1. Expand the **Process** panel.
2. Select **Performance Curve** from the **Process** drop-down list.



Select Input Settings

There are two input modes available to the Performance Curve process, as described in the "**Input Settings**" section, above:

- Values
- Liquid Control Valve

USING THE VALUES MODE

In the **Input Settings section:**

1. Select *Values* from the drop-down list.
2. Select X and Y coordinates, which are used for creating the curves. For each coordinate, select one of the following from the drop-down list; then type in or select a corresponding value:
   - Fixed Value
   - Attribute (only available if the **Source Type** is *Entity* or *Hierarchy*)
   - Source Tag (only available if the **Source Type** is *Tag*)
   - Calculation
   - Tag
   - Entity Attribute

These different options are outlined above, in the section "**Setting Process Values and Limits**", above.

USING THE LIQUID CONTROL VALVE MODE

In the **Input Settings section:**

1. Select *Liquid Control Valve* from the drop-down list.
2. Select X and Y coordinates, which are used for creating the curves.
   a. For the X coordinate, select one of the following from the drop-down list; then type in or select a corresponding value:
      - Fixed Value
      - Attribute (only available if the **Source Type** is *Entity* or *Hierarchy*)
      - Source Tag (only available if the **Source Type** is *Tag*)
      - Calculation
      - Tag
      - Entity Attribute

   b. For the Y coordinate, there are three factors:
      - Flow Rate (US gallons per minute)
      - Specific Gravity
      - Pressure Drop

      For each of these, select one of the following from the drop-down list; then type in or select a corresponding value:
      - Fixed Value
      - Attribute (only available if the **Source Type** is *Entity* or *Hierarchy*)
      - Source Tag (only available if the **Source Type** is *Tag*)
      - Calculation
      - Tag
      - Entity Attribute

   These different options are outlined above, in the section: "**Setting Process Values and Limits**", above.

Define the Curve Settings

After you have selected the input settings, you need to define the curve settings. This will determine how the curve is created, using the input settings as a base factor.

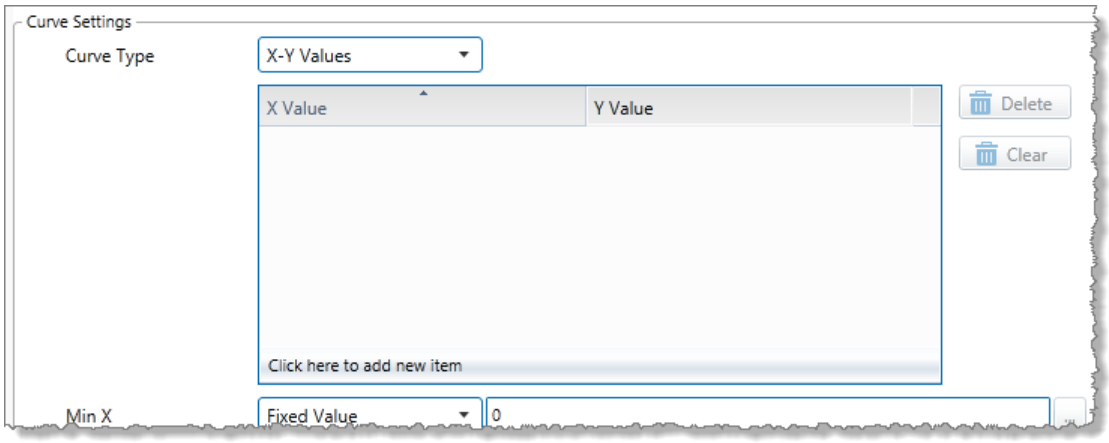
There are two types of curve to choose from:

- Polynomial
- X-Y Values

Defining X-Y Values

Points are plotted directly from the X and Y coordinates as they are captured into the table. The resulting graph forms the basis of the Performance Curve limits. The recommended maximum number of X-Y pairs is ten.

1. From the **Curve Type** drop-down list, select *X-Y Values*.

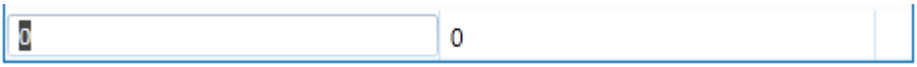


2. Add the X and Y values.

   a. Click **Click here to add new item**, located at the end of the table.

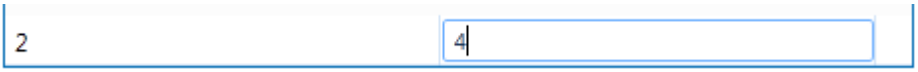
   Click here to add new item is replaced with two text boxes: one each for the X and Y values, with the cursor positioned in the first box.

   b. Capture the X value in the left text box (the X Value box), then press the *tab* key to move the cursor to the second text box (the Y Value box).

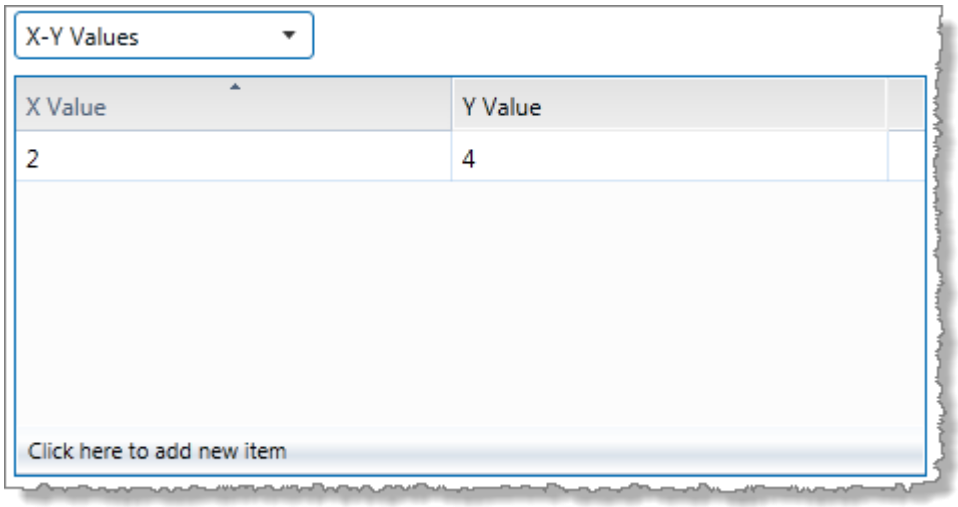
   

   c. Capture the Y value.

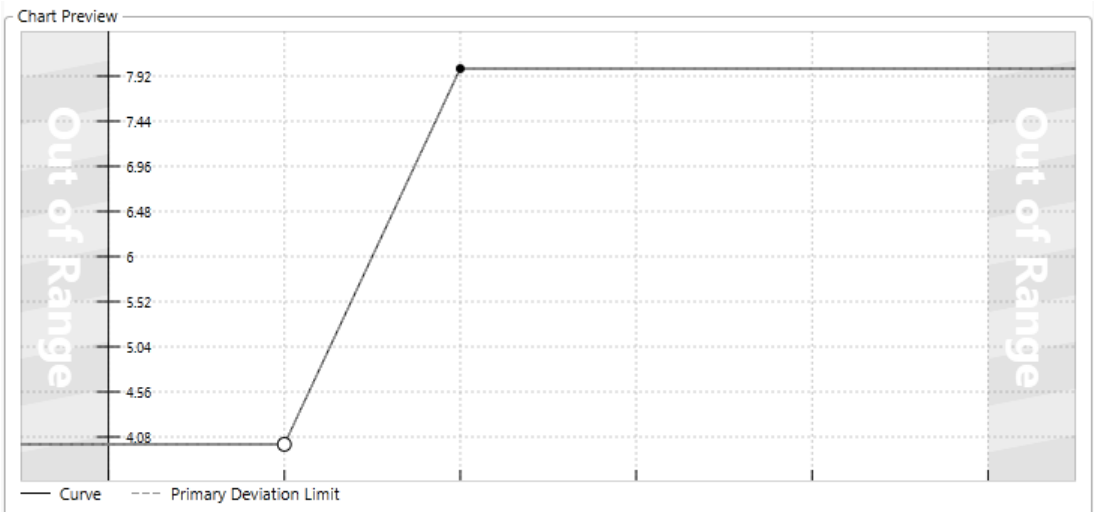
   d. Press the **Tab** key.

   The X and Y values are added to the table, and **Click here to add new item** replaces the two text boxes.

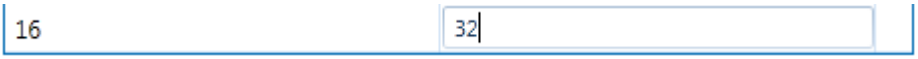
   

e. Add the second pair of X and Y values.

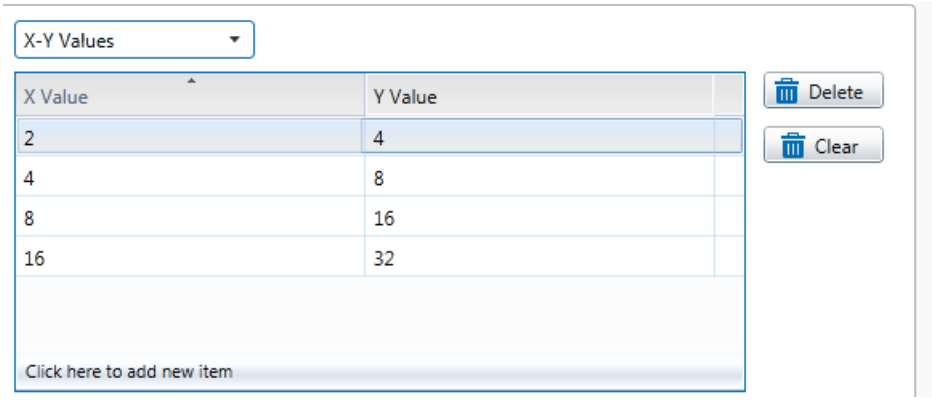
The **Chart Preview** (located below the **Curve Settings** section) now has a line drawn between the first two pairs of coordinates:



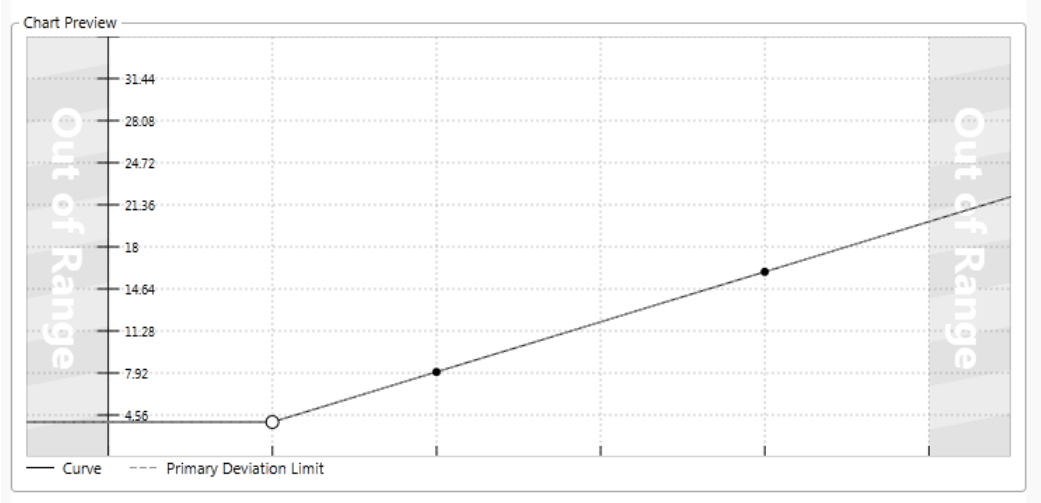
f. Continue to add X and Y values in this way, until your table of X-Y values is captured.



Each pair of values is added to the table in numerical order of the X value.



The Chart Preview now displays the line connecting all of the coordinate pairs:



UPDATING A PAIR OF X-Y VALUES

1. Select the pair that you want to update by clicking the mouse on the row (or select the row by selecting the corresponding point on the chart).
2. To update the X value, click in the X Value table item; then overtype with a new value.
3. To update the Y value, click in the Y Value table item; then overtype with a new value.

TO DELETE AN X-Y PAIR FROM THE TABLE

1. Select the pair that you want to delete by clicking the mouse on the row (or select the row by selecting the corresponding point on the chart).
2. Click the **Delete** button to the right of the table.

   The row is removed from the table, and the Chart Preview adjusts to reflect this.

TO CLEAR ALL X-Y VALUES IN THE TABLE

- Click the **Clear** button to the right of the table.

  All rows are removed from the table, and the Chart Preview is cleared.

USING THE CHART TO SELECT A ROW ON THE TABLE

1. If you want to change the values for a particular point on the chart, click that point.

   The solid point on the chart changes to a circle, and the cursor highlights the corresponding row on the table of X-Y values.
2. You can then update these values in the row.

Defining a Polynomial curve

Points are plotted using values derived from the polynomial equation. The resulting graph forms the basis of the Performance Curve limits. There are up to 9 degrees of polynomial.

1. From the **Curve Type** drop-down list, select *Polynomial* (the default).
2. Select the number of degrees for the polynomial equation, from the **Degrees** drop-down list. The default is 2.
3. Select the different factors for the equation.

   Each of these values may be any of the following:

   - Fixed Value
   - Attribute (only available if the **Source Type** is *Entity* or *Hierarchy*)
   - Source Tag (only available if the **Source Type** is *Tag*)
   - Calculation
   - Tag
   - Entity Attribute

   These different options are outlined above, in the section "**Setting Process Values and Limits**", above.

   The number of coefficients to capture depends on the polynomial *degree* selected.

Note: When capturing fixed values, you may use negatives. Decimal values are rounded up to the second place.

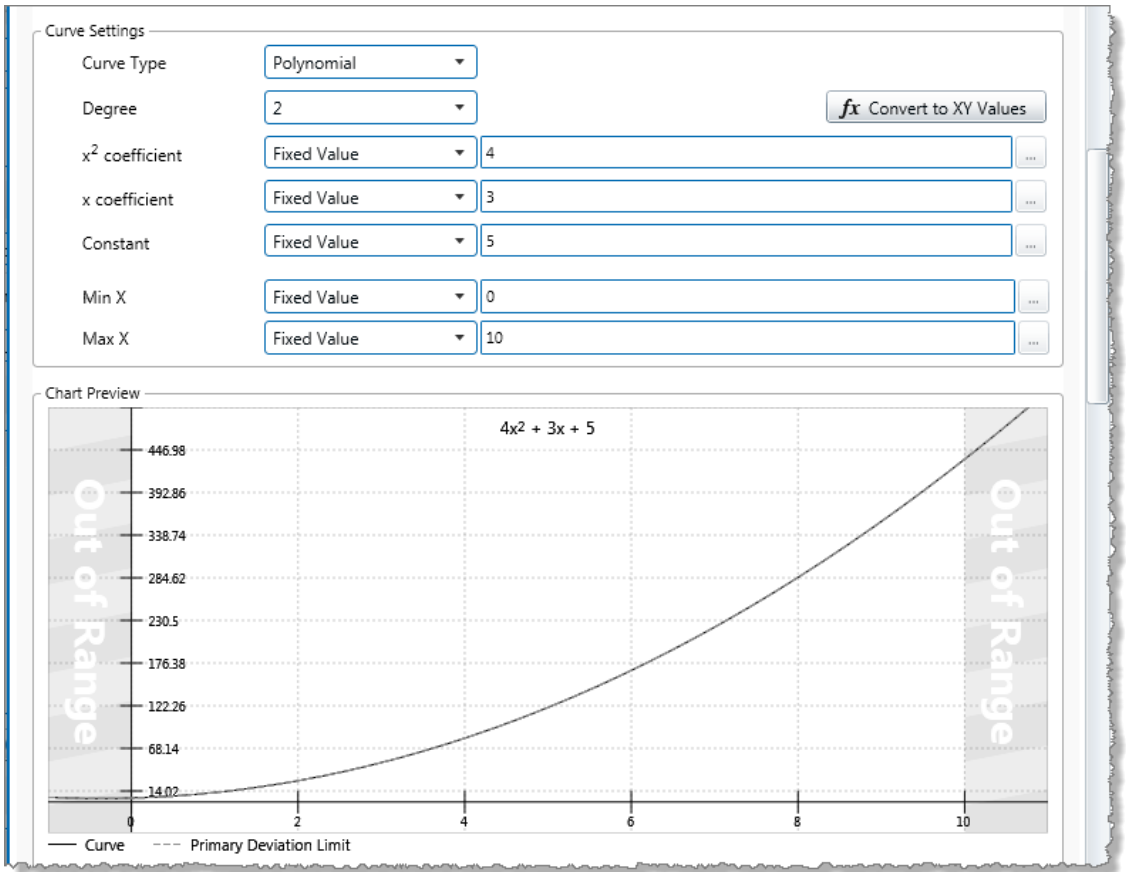
a. Capture the highest coefficient. For a 5th degree polynomial, this is the x^5 coefficient. For a 3rd degree polynomial, this is the x^3 coefficient, and so on.

b. Capture the next highest coefficient (for a 5th degree polynomial, this is the x^4 coefficient).

c. Continue until all coefficients have been captured, including the **x coefficient**.

d. Capture the constant value in the **Constant** text box.

The chart resulting from these factors is displayed in the Chart Preview below:



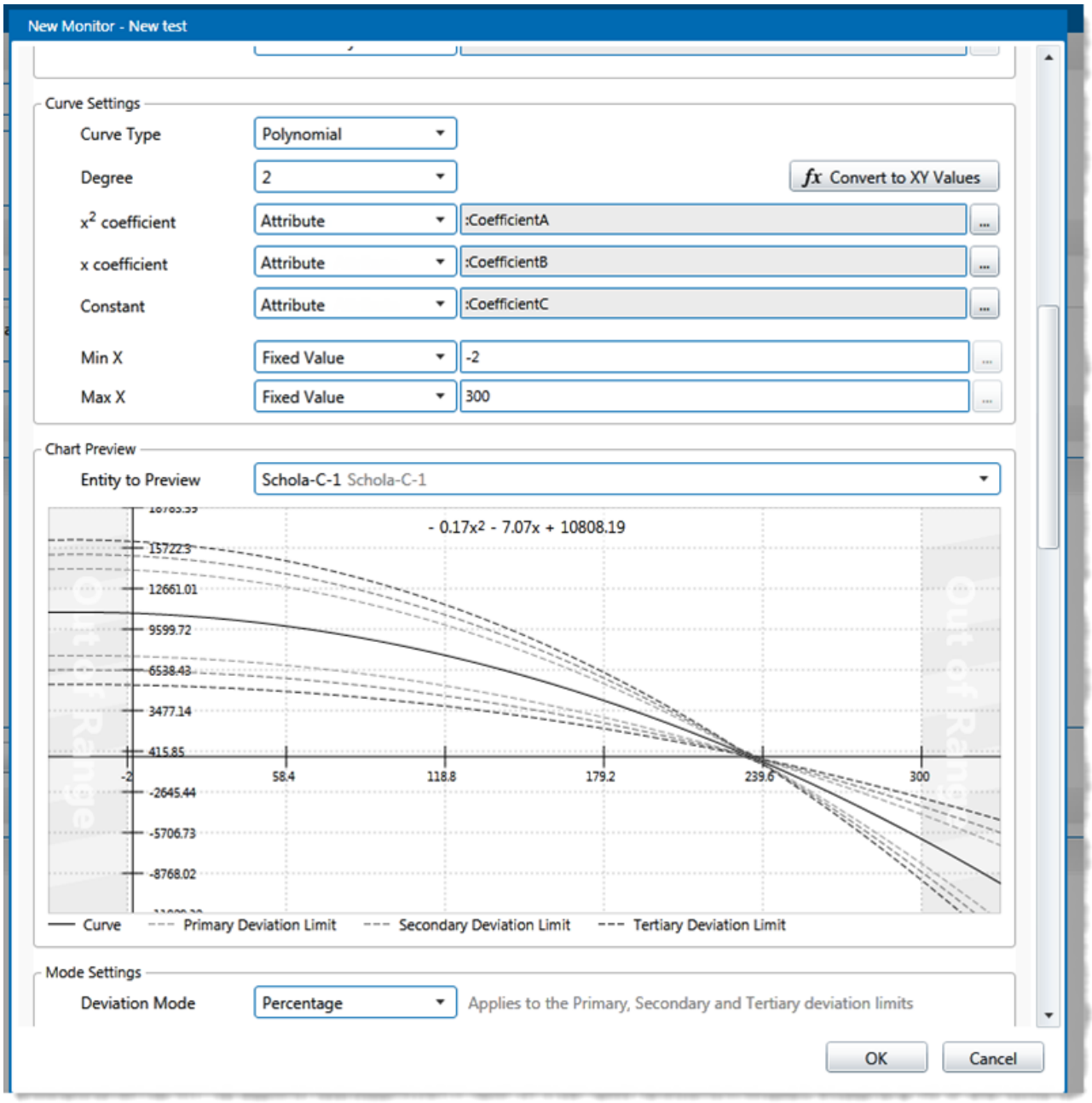
Curve settings rendered in a chart preview

Selecting the Entity to Preview

If the process is using a hierarchy as the source and a P2 Server entity (attribute or entity) in the curve settings, you can select which entity to preview in the chart. The entities listed are those that belong to the selected hierarchy.

- Select an entity from the **Entity to Preview** drop-down list.

The current values of the P2 Server entities of the selected coefficients are applied to the equation. This is reflected in the chart preview.

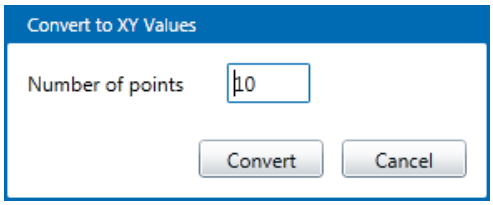


Converting to X-Y Values

If you want to adjust the polynomial curve, you can use the **Convert to XY Values** function.

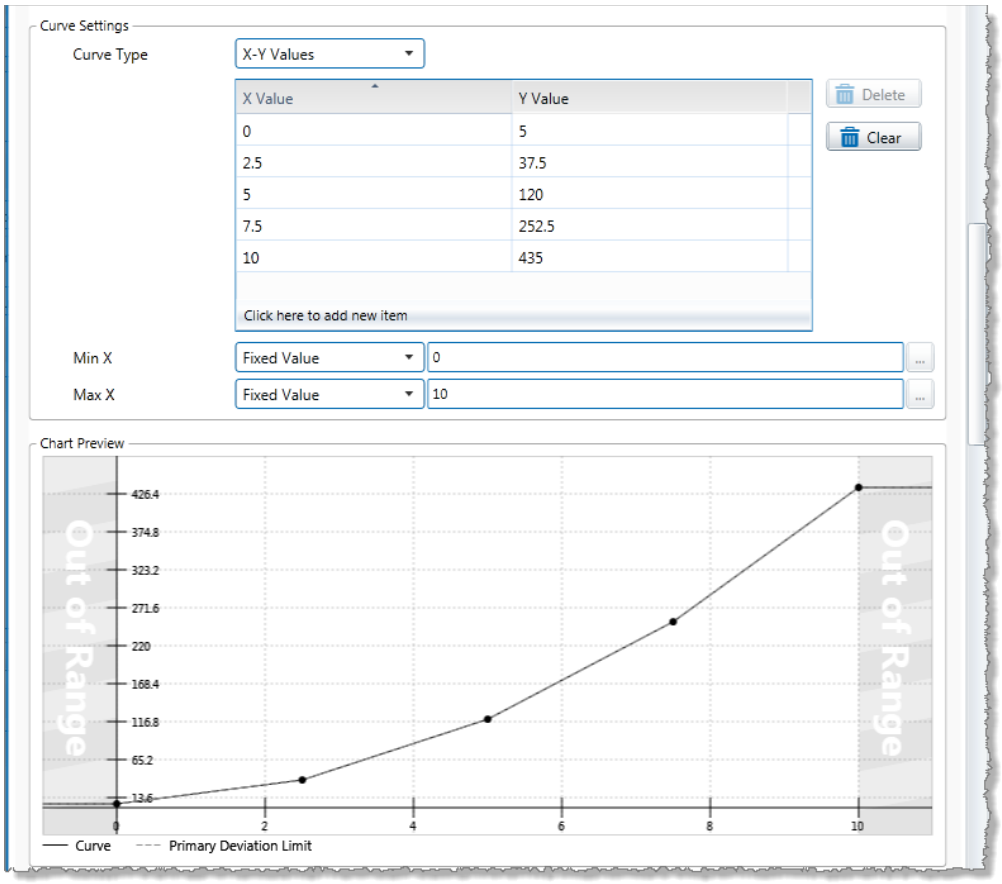
1. Click the **fx Convert to XY Values** button.

A **Convert to XY Values** window appears.



2. Select the number of points, by typing a positive integer in the **Number of points box**, then click **Convert**.

   The Curve Settings are converted to XY Values, and the resulting chart is now made up of lines connecting the coordinate pairs.



In this example 5 points were selected.

3. Adjust any of these points to refine the chart, if necessary, by following the instructions in the section "**Defining X-Y Values**" (**Updating a Pair of X-Y Values)**.

Define the Out of Range Values

A range of acceptable values is defined by a Min X and a Max X value. The default range is 0: 10 (defined by Min X : Max X).

To change the range:

1. For Min X: Select one of the following from the drop-down list; then type in or select a corresponding value.

   - Fixed Value
   - Attribute (only available if the **Source Type** is *Entity* or *Hierarchy*)
   - Source Tag (only available if the **Source Type** is *Tag*)
   - Calculation
   - Tag
   - Entity Attribute

   These different options are outlined above, in the section: "**Setting Process Values and Limits**", above.

2. For Max X, do the same.

   If fixed values are used, the ***Out of Range*** values cause an adjustment to the Chart Preview.

Define the Mode Settings

Define whether the deviation mode is a percentage or an absolute value, to establish how primary, secondary and tertiary deviation limits are calculated. Also select whether to set upper or lower deviation limits, or both.

Note: The mode settings apply to primary, secondary and tertiary deviation limits.

1. From the **Deviation Mode** drop-down list, select ***Percentage*** or ***Absolute Value***. The deviation mode determines how the deviation limits will be calculated.
2. Select the **Upper Deviation** check box to set an upper deviation limit.
3. Select the **Lower Deviation** check box to set a lower deviation limit.

Select Deviation Limit Settings

Note: The Primary Deviation Limit is mandatory for the Performance Curve Process.

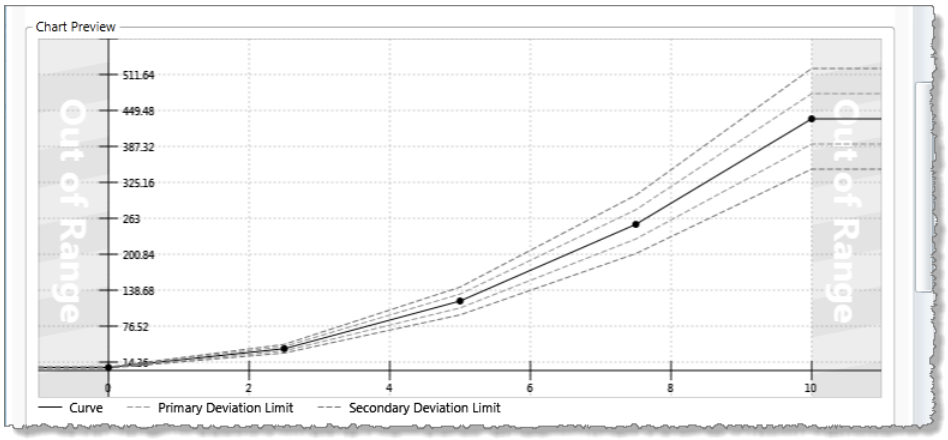
1. From the **Primary Limit** drop-down list, select one of the following and then type in or select a corresponding value:

   - Fixed Value
   - Attribute (only available if the **Source Type** is *Entity* or *Hierarchy*)
   - Source Tag (only available if the **Source Type** is *Tag*)
   - Calculation
   - Tag
   - Entity Attribute

   These different options are outlined above, in the section: "**Setting Process Values and Limits**", above.

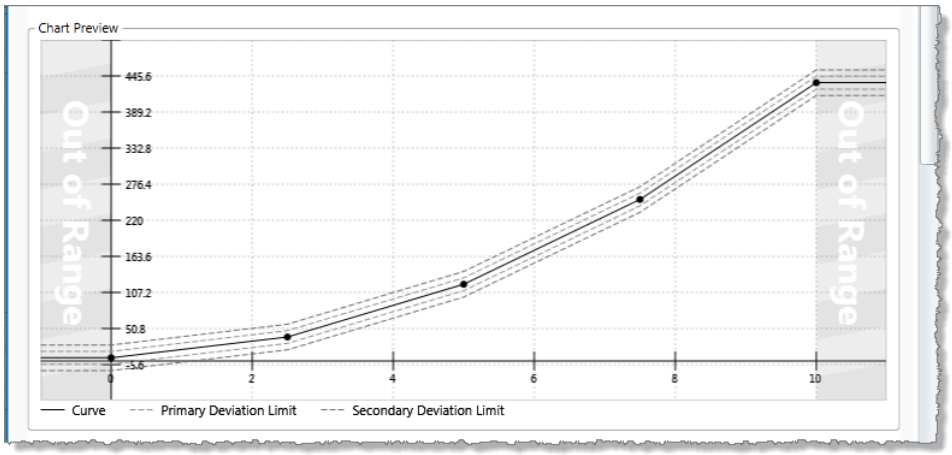
2. Optionally define secondary limits in the same way (first select the **Secondary Limit** check box).
3. Optionally define tertiary limits in the same way (first select the **Tertiary Limit** check box).

   The Chart Preview changes to show how the limits are applied.



The chart above shows primary and secondary upper and lower deviation limits of fixed values 10 and 20 respectively. Here, limits are calculated using the percentage deviation mode.

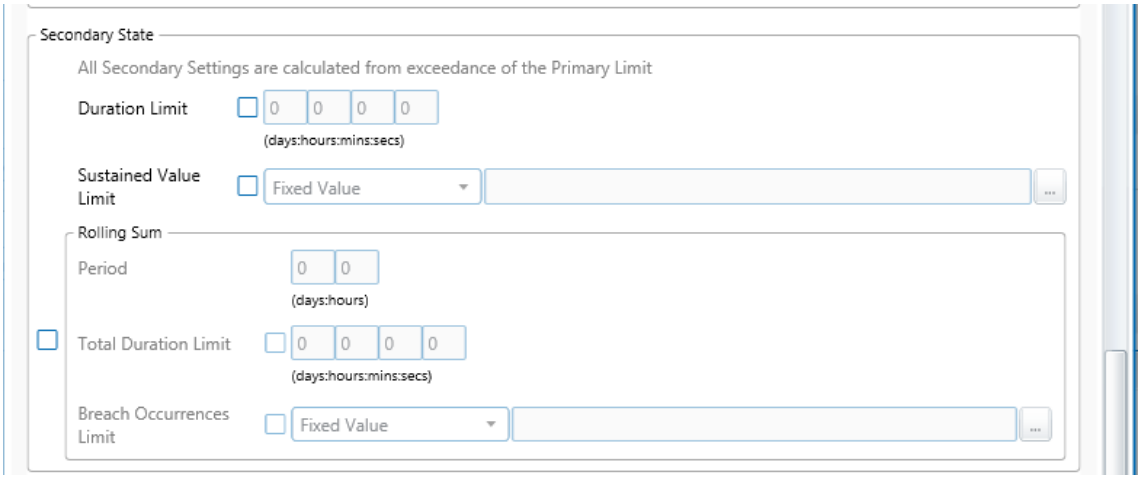
Using the same settings but applying the absolute value mode, deviation limits are calculated differently, as shown in the following chart preview:



Select Secondary State Settings

Note: All Secondary State settings are calculated from the primary deviation limit.

All secondary state settings are captured or selected in the **Secondary State** section of the process, with the exception of the Secondary Deviation Limit, which is set in the **Deviation Limit Settings** section of the process.

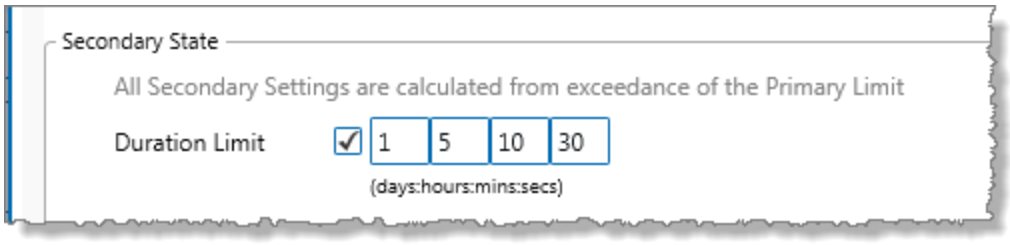


To Set a Secondary State Duration Limit

The Secondary State Duration Limit is used for monitoring where data is continuously beyond the primary deviation limit, for longer than the specified secondary duration limit.

In the **Secondary State** section:

1. Select the **Duration Limit** check box.
2. Type integer values in the **days**, **hours**, **mins** (minutes), and **secs** (seconds) **Duration Limit** boxes to define a duration period. The default value is zero.



A Secondary State Duration Limit of 1 Day, 5 Hours, 10 Minutes and 30 Seconds

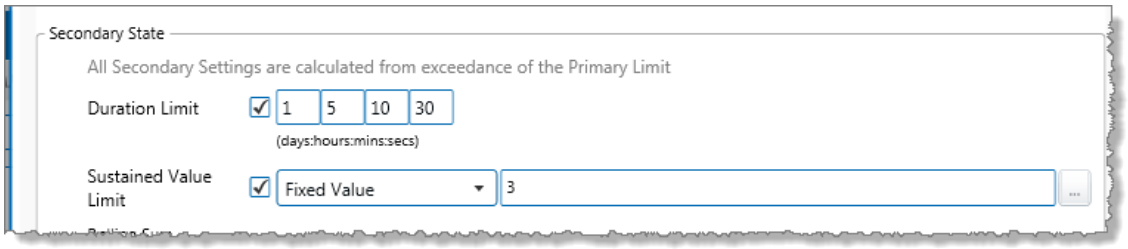
To Set a Secondary State Sustained Value Limit

The Secondary State Sustained Value Limit is used for monitoring where data is beyond the primary deviation limit for more than a specified number of times (secondary state sustained value limit), consecutively.

In the **Secondary State** section:

1. Select the **Sustained Value Limit** check box.
2. From the **Sustained Value Limit** drop-down list, select one of the following and then type in or select a corresponding value:
   - Fixed Value
   - Attribute (only available if the **Source Type** is *Entity* or *Hierarchy*)
   - Source Tag (only available if the **Source Type** is *Tag*)
   - Calculation
   - Tag
   - Entity Attribute

   These different options are outlined above, in the section "**Setting Process Values and Limits**", above.



A Sustained Value Limit of 3 (Fixed Value)

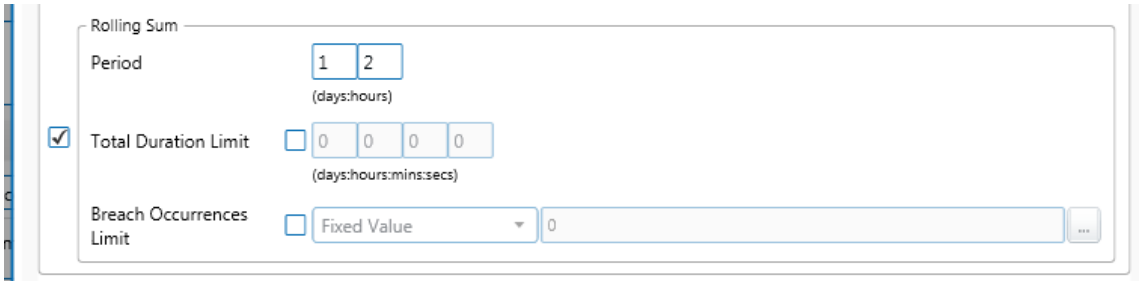
To Set a Secondary State Rolling Sum Period

The rolling sum period is a defined period (specified in days and hours). At every sample interval, the rolling sum period applies to that period preceding the sample interval.

Set a secondary state rolling sum period if you are going to define a secondary state total duration limit or a secondary state breach occurrences limit.

In the **Secondary State** section:

1. Select the check box to the left of the **Rolling Sum** section.
2. Type integer values in the **days** and **hours** *Period* boxes to define the rolling sum period. The default value is zero.

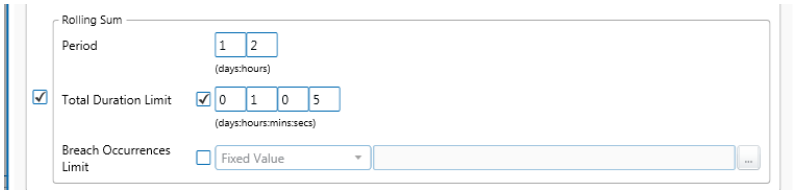


A Secondary State Rolling Sum Period of 1 Day and 2 Hours

To Set a Secondary State Rolling Sum Total Duration Limit

The Secondary State Rolling Sum Total Duration Limit is used to monitor for a specified accumulated duration of all periods where data is in breach of the primary deviation limit, within the preceding specified secondary state rolling sum period.

1. In the **Rolling Sum** section, within the **Secondary State** section:
2. Select the **Total Duration Limit** check box.
3. Type integer values in the **days**, **hours**, **mins** (minutes), and **secs** (seconds) **Total Duration Limit** boxes to define a total duration limit period. The default value is zero.



A Total Duration Limit of 1 Hour and 5 Seconds

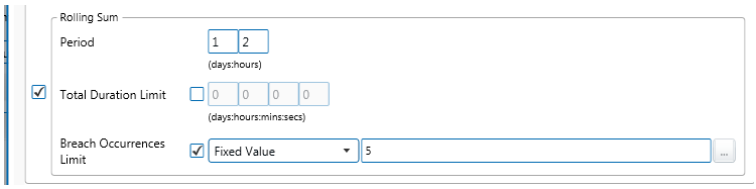
To Set a Secondary State Rolling Sum Breach Occurrences Limit

The Secondary State Rolling Sum Breach Occurrences Limit is used to monitor for when a set number of values (secondary state breach occurrences limit) has breached the primary deviation limit, during the preceding specified secondary state rolling sum period.

In the **Rolling Sum** section, within the **Secondary State** section:

1. Select the Breach Occurrences Limit check box.
2. From the **Breach Occurrences Limit** drop-down list, select one of the following and then type in or select a corresponding value:
   - Fixed Value
   - Attribute (only available if the **Source Type** is *Entity* or *Hierarchy*)
   - Source Tag (only available if the **Source Type** is *Tag*)
   - Calculation
   - Tag
   - Entity Attribute

   These different options are outlined above, in the section: "**Setting Process Values and Limits**", above.

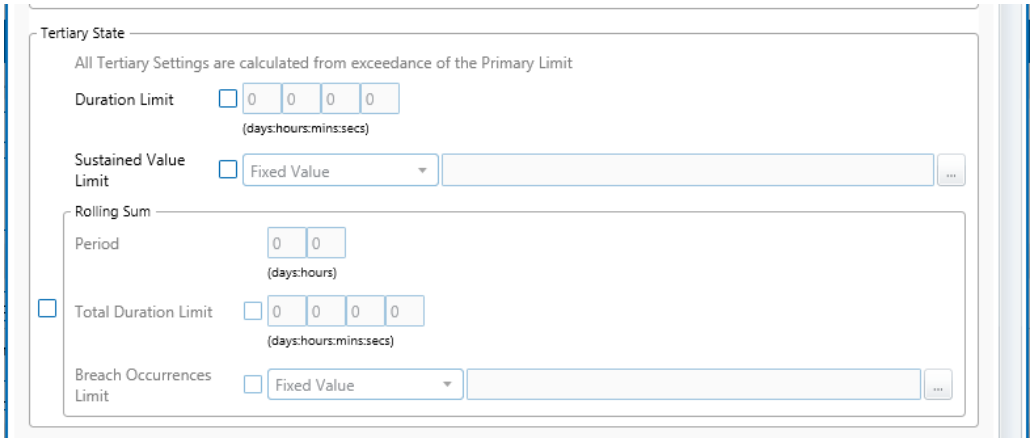


A Breach Occurrences Limit of 5 (Fixed Value)

Select Tertiary State Settings

Note: All Tertiary State settings are calculated from the primary deviation limit.

All tertiary state settings are captured or selected in the **Tertiary State** section of the process, with the exception of the Tertiary Deviation Limit, which is set in the **Deviation Limit Settings** section of the process.

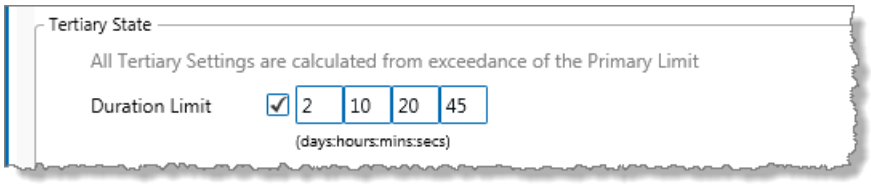


To Set a Tertiary State Duration Limit

The Tertiary State Duration Limit is used for monitoring where data is continuously beyond the primary deviation limit, for longer than the specified tertiary state duration limit.

In the **Tertiary State** section:

1. Select the **Duration Limit** check box.
2. Type integer values in the **days**, **hours**, **mins** (minutes), and **secs** (seconds) **Duration Limit** boxes to define a duration period. The default value is zero.



A Tertiary State Duration Limit of 2 Days, 10 Hours, 20 Minutes and 45 Seconds

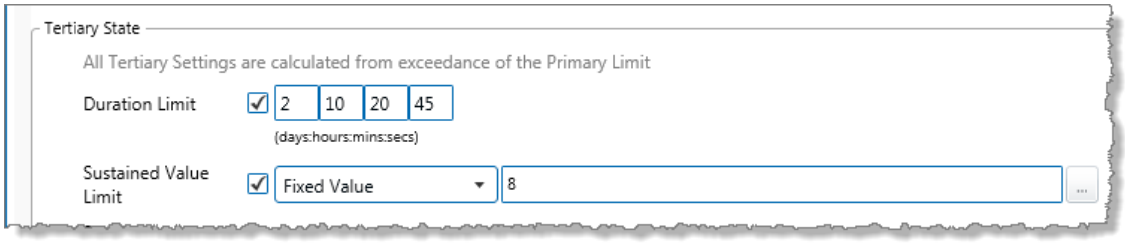
To Set a Tertiary State Sustained Value Limit

The Tertiary State Sustained Value Limit is used for monitoring where data is beyond the primary deviation limit for more than a specified number of times (tertiary state sustained value limit), consecutively.

In the **Tertiary State** section:

1. Select the **Sustained Value Limit** check box.
2. From the **Sustained Value Limit** drop-down list, select one of the following and then type in or select a corresponding value:
   - Fixed Value
   - Attribute (only available if the **Source Type** is *Entity* or *Hierarchy*)
   - Source Tag (only available if the **Source Type** is *Tag*)
   - Calculation
   - Tag
   - Entity Attribute

   These different options are outlined above, in the section: "**Setting Process Values and Limits**", above.



A Sustained Value Limit of 8 (Fixed Value)

To Set a Tertiary State Rolling Sum Period

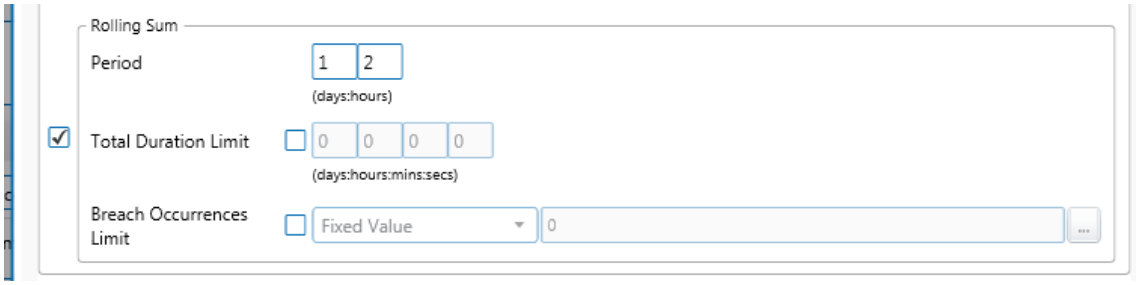
The rolling sum period is a defined period (specified in days and hours). At every sample interval, the rolling sum period applies to that period preceding the sample interval.

Set a tertiary state rolling sum period if you are going to define a Tertiary State Total Duration Limit or a Tertiary State Breach Occurrences Limit.

In the **Tertiary State** section:

1. Select the check box to the left of the Rolling Sum section.

2. Type integer values in the **days** and **hours** *Period* boxes to define the rolling sum period. The default value is zero.



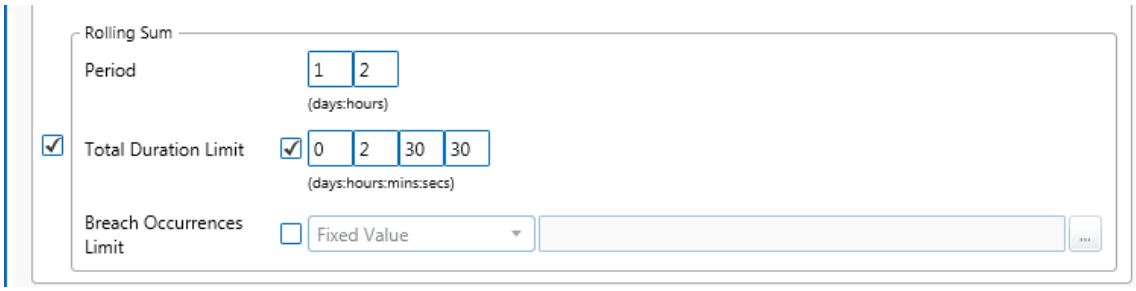
A Tertiary State Rolling Sum Period of 1 Day and 2 Hours

To Set a Tertiary State Rolling Sum Total Duration Limit

The Tertiary State Rolling Sum Total Duration Limit is used to monitor for a specified accumulated duration of all periods where data is in breach of the primary deviation limit, within the preceding specified tertiary state rolling sum period.

In the **Rolling Sum** section, within the **Tertiary State** section:

1. Select the **Total Duration Limit** check box.
2. Type integer values in the **days**, **hours**, **mins** (minutes), and **secs** (seconds) **Total Duration Limit** boxes to define a total duration limit period. The default value is zero.



A Total Duration Limit of 2 Hours, 30 Minutes and 30 Seconds

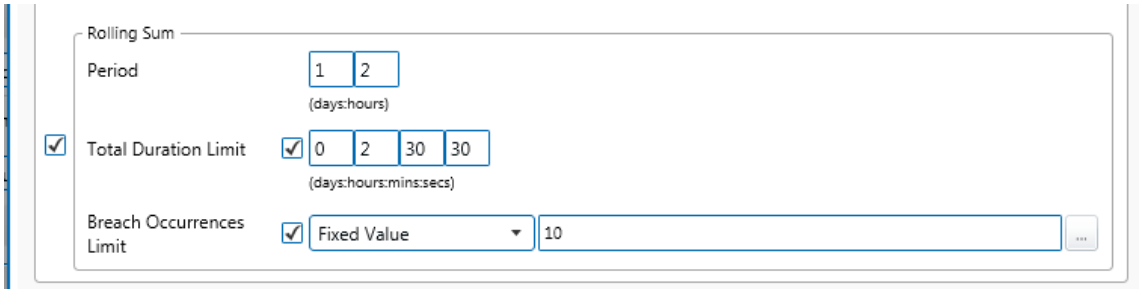
To Set a Tertiary State Rolling Sum Breach Occurrences Limit

The Tertiary State Rolling Sum Breach Occurrences Limit is used to monitor for when a set number of values (tertiary state breach occurrences limit) has breached the primary deviation limit, during the preceding specified tertiary rolling sum period.

In the **Rolling Sum** section, within the **Tertiary State** section:

1. Select the Breach Occurrences Limit check box.
2. From the **Breach Occurrences Limit** drop-down list, select one of the following and then type in or select a corresponding value:
   - Fixed Value
   - Attribute (only available if the **Source Type** is *Entity* or *Hierarchy*)
   - Source Tag (only available if the **Source Type** is *Tag*)
   - Calculation
   - Tag
   - Entity Attribute

These different options are outlined above, in the section: "**Setting Process Values and Limits**", above.



A Breach Occurrences Limit of 10 (Fixed Value)

Adding Comments to the Process Panel

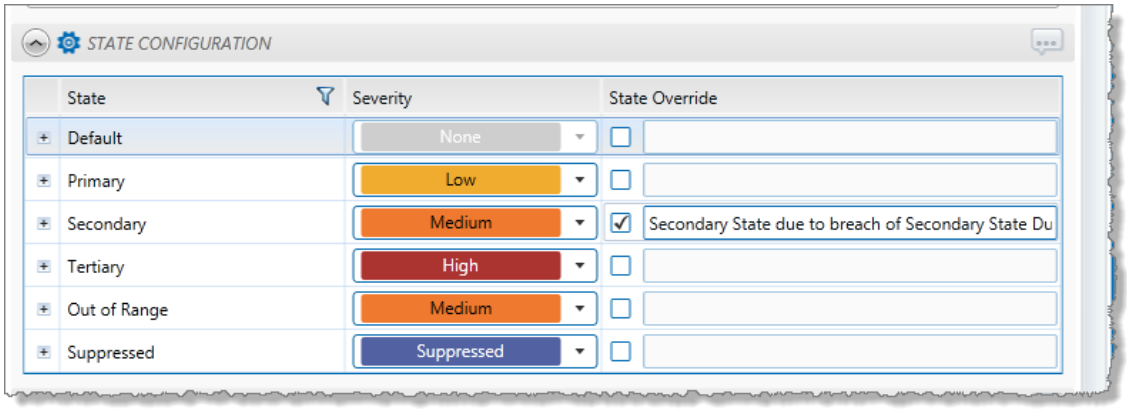
- To add comments to the process panel click the comment button, at the top right of the panel.

Configuring States

For the Performance Curve process, you can configure the following states, each with an optional state override and comments:

- Primary
- Secondary
- Tertiary
- Out of Range
- Suppressed

You cannot change the severity of the Default state; however, you can add a state override and comments.



Note: Only configure states where you have set a limit.

To configure the state outcomes for a test in the **State Configuration** panel of the test, see 3.6 Configure States. If Case Management is enabled in Sentinel, this is also where you manage cases.

Appendix K. The Sentinel Engine

This section describes how the Sentinel Engine reads and processes data. The information here is supplementary to what is provided in this User's Guide, to give you an insight into how and when the different parts are processed.

The Sentinel Engine is responsible for:

- Scheduling and running monitors
- Processing tests and process logic
- Storing/retrieving time series data in the Sentinel data cache
- Running debug user processes from Sentinel Studio

How a Monitor is Processed

Sentinel schedules each active monitor to run at a particular point in time. When this time is reached, the monitor processes the data from the 'Last Run Time' to 'Now'. This time period is then divided into sections; the section period depends on the configuration settings 'MinCatchupMonitorRunPeriodMinutes' and 'MaxCatchupMonitorRunPeriodMinutes'.

For each section of the processing time period, the monitor is processed in the following stages (in this order):

1. Each test in the monitor is assigned a processing thread (each **test** will get processed independently and in parallel to all other tests; this may mean individual tests run across different CPUs).
2. For each **test**, the following steps are taken:

   Note: If an error occurs during any of these steps, the test stops executing, which in turn stops the Monitor from processing the current time period.

   a. The list of entities which are to be processed is resolved. For hierarchy mode, this involves querying the Data Dictionary for entities from a point in the hierarchy, possibly with a particular template.

   b. Test suppression is checked.

   c. Data for each Primary Input is fetched from the Data Broker. If no data is returned for an Entity, the behaviour specified by the 'NoDataBehavior' configuration setting is performed (Error, Suppress, or Ignore).

   d. Data for the precondition is fetched from the Data Broker. If no data is returned for an Entity, the behaviour specified by the 'NoDataBehavior' configuration setting is performed (Error, Suppress, or Ignore).

   e. The precondition is processed and the period which is being processed is further sliced into periods of 'Process', 'Suppressed' or 'Do not process'. (See the Suppressions section below).

   f. All other input data is fetched from the Data Broker for entities which will be processed. If no data is returned for an input, the behaviour specified by the 'NoDataBehavior' configuration setting is performed (Error, Suppress, or Ignore).

g. The Process for this Test is used to process all of the data for all periods where the Precondition raised a 'Process' time slice. Events which are raised by the Process are held in memory for later processing.

3. The Monitor will wait until all tests 'threads' have successfully finished processing. The following steps occur in sequence:

Note: if an error occurs at any stage, the monitor will stop processing and wait until it is re-scheduled. Each step is a 'transaction' so the steps may partially commit changes to the database.

a. Each test is checked to see if any errors occurred during processing. If errors did occur, processing for this monitor is ended at this step. The monitor will then schedule again and 'retry' to process the same processing period.

b. Any events which were raised by the process are written to the database.

c. Any data which is to be written back to data sources is sent to the data broker.

d. Actions are run for each event.

e. If 'Case Management' is enabled, cases are raised by Sentinel.

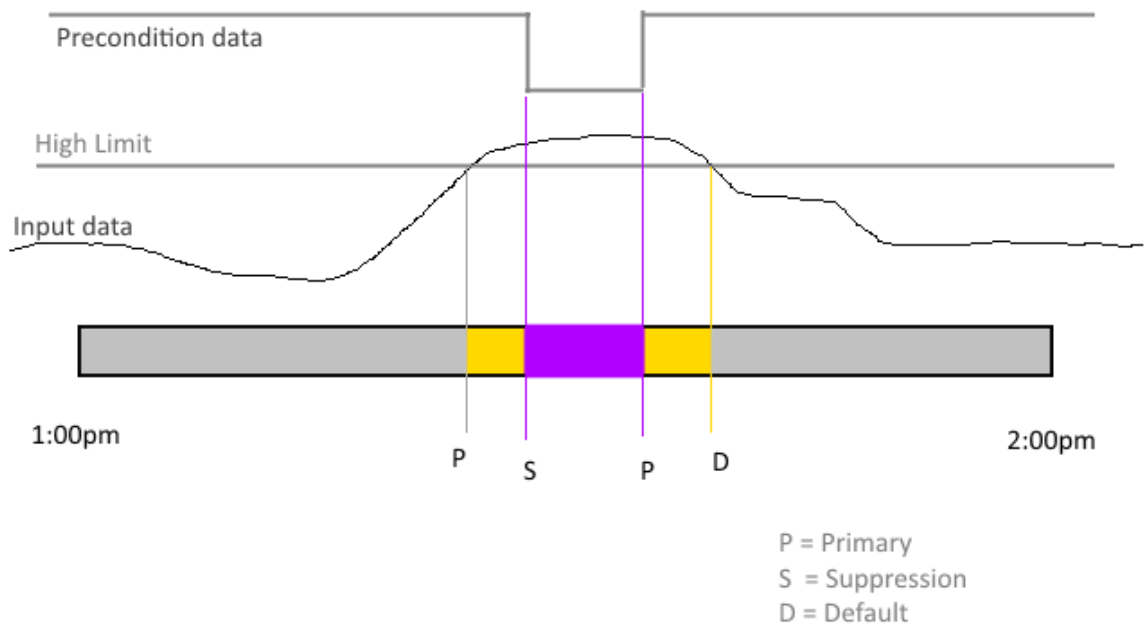
f. The monitor's 'Last Run Time' is updated ready for the next run.

Note: If the Sentinel Engine Service is stopped, it has to signal to any running monitors to stop processing and then wait for them to successfully stop. This also means that any data cache data which is in memory needs to be flushed back to the files in the data cache (see the Data Cache section below). The service will not stop until all these steps have been performed. **It is possible to 'kill' the Engine process using task manager but there is a risk that upon restart, the data cache will not contain the latest data.**

Suppressions

Test Suppression or Preconditions are calculated for the time period which is being processed.

In the example below, the test is monitoring input data to see if it has exceeded a high limit. There is also precondition data which is high or low. The precondition is configured to process when the value is high and suppress when low.



After a suppression is ended, the engine automatically raises an event with the same state as was raised prior to the suppression event. When this occurs, there will not be any event metadata on the 'out-of-suppression' event. In some circumstances, after the engine has raised the 'out-of-suppression' event, a point of data will get processed at the time the suppression ends, which may override the automatic state and in this case, event metadata will get added to the event.

Data Cache

When a process is using time windowing (performing some calculation/operation over a historical period), then Sentinel uses a local cache of the time-series data which has previously been processed. This cache allows rapid access of the data and stops the need for fetching the same data over and over from a data source.

This data is stored as individual streams in the 'Cache' folder in the main installation directory.

Because the data cache uses the local hard drive to persist the time-series streams of data, the processing speed of these streams (and of the Sentinel Monitor) can be impacted if some other process is using the hard drive frequently. For example, P2 Logger, any local database which is installed on the same drive, or multiple VMs sharing a physical drive.

If contention is an issue, the data cache can be moved to another drive by adding a Registry key:

HKEY_LOCAL_MACHINE/SOFTWARE/ISS/BabelFish Sentinel/CachePath

Set the key to REG_SZ and set the value to the path to the cache folder on the other drive.

After adding the key, remember to restart the Sentinel Engine Service.

Sentinel Studio Debugger

When User Processes are run in the Studio Debugger, the logic is run by the Sentinel Engine so the Engine Service must be running.

Glossary

Action
The automatic step taken when a state is reached in a test. Typical actions include sending an email or SMS to a selection of personnel. Another action is a call made to a designated web service. A monitor may have several actions, and these can be assigned to various state outcomes, of various tests belonging to the monitor.

Asset
In P2 Sentinel, attributes or attribute values that are the subject of monitoring are all linked to an *asset,* which is then used in reporting. The asset refers to the equipment or location that is being monitored, and is linked to the attribute or attribute value, using the relationship defined within P2 Server.

P2 Server Browser
A tool that enables the P2 Server Data Dictionary to be traversed.

Case Management
Case Management is all about actions and workflows surrounding events raised in source applications such as P2 Sentinel. Sentinel has configuration options for raising cases for certain events, under specific conditions. These cases can be automatically prioritised according to a set of configurable rules.

Category
The category is used to filter the monitors displayed in report filtering and does not affect the functionality of the monitor. Examples are: financial, operational, environmental, occupational health and safety, and maintenance. A monitor's category is saved to any cases raised in Sentinel.

Continuous Data
Data is continuous if there is no clear distinction between possible values. With continuous data, all values within a range have meaning. Sets of data involving measurements that can have fractions or decimals are generally continuous. An example of continuous data is the temperature of a motor. It sometimes makes sense to treat continuous data as being discrete data. For example, something like volume is continuous, but if small differences are irrelevant we can group volumes into a number of discrete bins.

Discrete Data
Data is discrete if there is clear distinction between the possible values. Data can be known and counted exactly. With discrete data, only certain values within a range have meaning. An example of discrete data is a count of the number of objects, such as pumps in a facility. There can be 1, 2, 3 etc. pumps. You cannot have half a pump. With discrete data, the units of measurement cannot be split up. It sometimes makes sense to treat discrete data as being continuous. For example, if we're counting large amounts of some discrete entity, we may choose to think of 1,235,816 and 1,235,818 as nearby points on an approximate continuum.

Entity Volume
The entity volume is the maximum number of entities, collectively, that processes belonging to a licence group may use, for all tests, and across all monitors within the P2 Sentinel installation. The entity volume for each licence group, and the allocation of the various processes to the different licence groups, depends on the licence agreement for the installation.

Event
An event occurs when a test item causes a state change by transgressing the conditions specified in a test, or by reaching a state specified in a test.

Folder
A container for logical grouping of monitors.

Monitor
A monitor contains one or more tests that share a trigger and a set of available actions.

Monitor Item
The primary measurement or value being monitored within a test. The measurement may be an entity, an attribute, or an attribute value.

Process
A set of logical functions and calculations used to determine the state, and the subsequent event of every monitor item in a test.

Process Limit
Every continuous data process has its own set of process limits. The process limit is the value (fixed or variable), that the test item is compared to during a test run. A fixed value process limit is defined when the test is configured; a variable process limit holds the value of the variable (for example, the value of an attribute) at the time of the test.

State
The state of a test item, after it has gone through the test. There are a number of possible states, including (but not limited to) Default, High High Exceeded, High Exceeded, No Data, Digital, and Suppressed. The possible states depend on the process that is used for a test. All tests using the standard processes include the Default state and the Suppressed state as possible outcomes, regardless of which process is used.

Test
Each monitor has at least one test. A test evaluates source data using a defined process, and raises events when the state changes. The resulting state can trigger specified actions.

Trigger
A trigger defines when the initial and subsequent monitor tests are processed. All tests within a monitor share a single trigger. When a trigger initiates testing, the whole period since the last trigger time is processed.

Workspace
A container for the logical grouping of folders, monitors and event views.