# Admin Console

## User Documentation

8.0

ca technologies

# Copyright Notice

# Contact CA

**Contact CA Support**

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

**Providing Feedback About Product Documentation**

Send comments or questions about CA Technologies product documentation to nimsoft.techpubs@ca.com.

To provide feedback about general CA Technologies product documentation, complete our short customer survey which is available on the support website at http://ca.com/docs.

# Documentation Changes

This table describes the version history for this document.

| Version | Date | What's New? |
|---|---|---|
| 8.0 | September 2014 | Added Time Over Threshold section. |
| 7.6 | June 2014 | General Probe Administration and Interface Overview sections have been updated. |
| 7.5 | March 2014 | How to Add a Hub License section has been updated. |
| 7.1 | December 2013 | Robot selection section has been updated. |
| 7.0 | September 2013 | Configurable HTTP/HTTPS communication between Admin Console and NMS.<br>Simplified deployment of self-signed SSL certificates. |
| 1.0 | March 2013 | Initial release of Admin Console. |

**Related Documentation**

Documentation for Admin Console compatible probes

Monitor Metrics Reference Information for CA Nimsoft Probes

# Contents

## Chapter 6: Deploy Probes Using Admin Console 31

## Chapter 7: General Probe Configuration 35

## Chapter 8: Time Over Threshold 41

# Chapter 1: Getting Started with Admin Console

This topic describes how to display and view data in the Admin Console. You can access the Admin Console either through the Unified Management Portal (UMP) or in a standalone web page.

UIM System Administrators and users with administrator or superuser permissions can access this application.

The standalone version of the Admin Console is installed during your UIM system installation. The Admin Console portlet is installed during your UMP installation.

The Admin Console application allows you to manage and maintain your hubs, robots, and probes on your CA Unified Infrastructure Management system.

## How to Access Admin Console Using UMP

The Admin Console can run within an UMP portlet. Using Admin Console, you can manage and maintain your hubs, robots, and probes on your UIM system.

Set up the page and portlet by following the procedures in the following section.

## How to Create a Page

You can create custom pages where you control which portlets are displayed and the layout of the page. Two privacy settings are available:

**Private**

Pages display when you first log in. Only you can see private pages.

**Public**

Pages are accessed by choosing Go to, My Public Pages from the menu bar. Anyone on the Internet can see public pages.

**Follow these steps:**

1. Add a page (see page 8).
2. Select a layout (see page 8).
3. Add portlets (see page 9).

### How to Add a Page

**Follow these steps:**

1. Choose Add, Page from the menu bar.
2. Enter a name for the page in the text box that is displayed next to the page tabs.
3. Click the green checkmark next to the text box.
4. Click the tab for the page.

   The new page opens.

### How to Select a Layout

**Follow these steps:**

1. Choose Manage, Page Layout from the menu bar.
2. Select the layout that you want.
3. Click Save.

## How to Add Portlets

**Follow these steps:**

1. Choose Add, Portlet from the menu bar.
2. Click the + sign next to Monitoring.
3. Drag a portlet to the position on the page where you want to display it, or click Add next to the portlet.

To add more portlets to your layout, repeat these steps.

## How to Log in to Admin Console in UMP

**Follow these steps:**

1. Connect to your UMP application in a web browser.
2. Enter a valid UIM user name and password.

   The Unified Management Portal opens to the USM portlet.
3. Click the Admin Console tab.

   **Note:** If the Admin Console tab is not available, see the Add Portlets (see page 9) section to add this portlet.

   The Admin Console screen appears.

Your system is available for configuration.

# How to Access Admin Console Using a Standalone Web Page

The Admin Console is available through a web page. The Admin Console allows you to manage and maintain your hubs, robots, and probes.

## How to Log in to Admin Console in a Standalone Web Page

**Follow these steps:**

1. Enter http://<service_host>:8080/adminconsole in your web browser window.

   **Note:** <service_host> is the system where the service_host probe is installed.
2. Enter a valid UIM username and password.

   The Admin Console application opens.

# Interface Overview

This section introduces you to the Admin Console interface. The main window contains two buttons in the upper left corner to access the list of hubs/robots and the probe archive.

The upper right corner displays the username, help button (?), and link to the CA Marketplace (🛒).

The arrow next to the username in the upper right corner is used to change the password or to logout of Admin Console.

The main window is divided into two sections. The left navigation pane displays the hubs and robots in a tree structure. The right pane displays either the robot or probe information that is based on your selection in the navigation pane.

At the top of each section is a filter to narrow your list. The filters only apply to the appropriate section of the screen.

## Infrastructure Interface Overview

To manage your Hubs, select the Infrastructure button in the Admin Console screen.

The navigation pane displays the hubs and robots in a tree structure. The right side of the screen displays the robot information for the selected hub in the navigation pane.

The right pane displays the robot properties. See How to Modify Robot Properties View (see page 12) for more information.

The ? (Help) icon opens the online help for the Admin Console application.

## Robot Interface Overview

To manage your robots, select the Infrastructure button in the Admin Console screen then select a robot in the navigation pane.

The right pane provides four options for accessing information about your robot:

- Robot Properties
- Probes
- Packages Installed
- The environment variables.

## Robot Properties

This screen displays the properties that are associated with your robot. This screen is a read-only screen and provides the following information for the robot:

**OS Major**

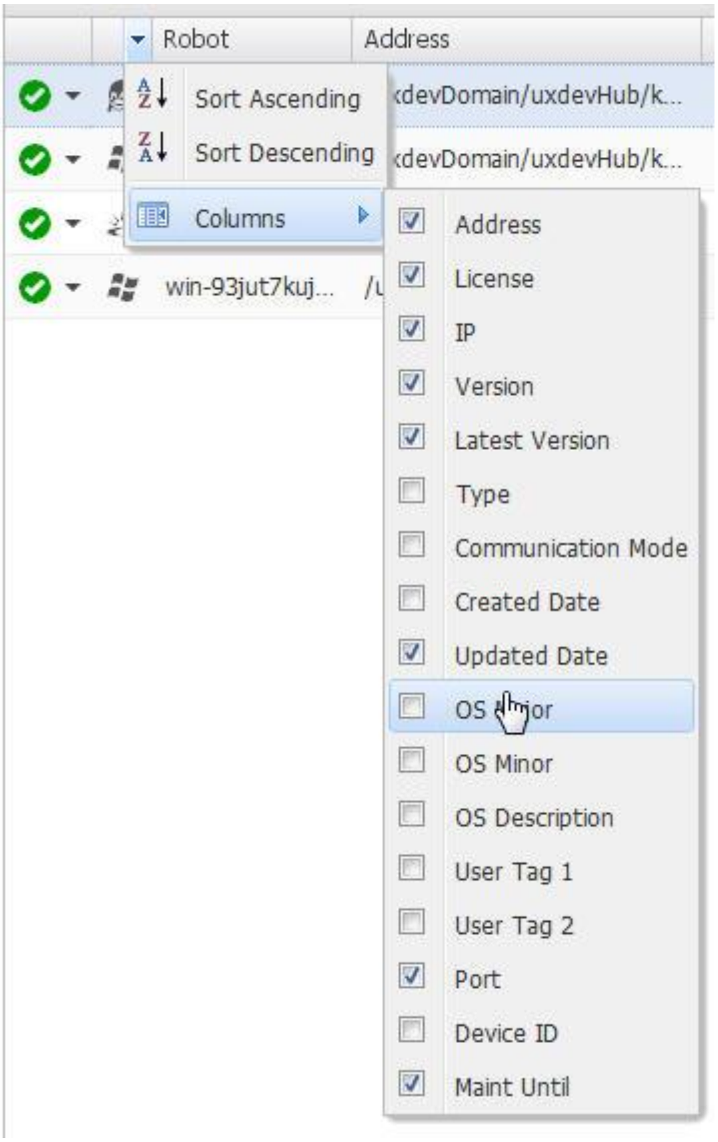
Operating system of the robot.

## How to Modify Robot Properties View

**Follow these steps:**

1. In the right pane, click the arrow next to a column heading.
2. Click **Columns**.

   A list of the available columns appears.



☑ Address
☑ License
☑ IP
☑ Version
☑ Latest Version
□ Type
□ Communication Mode
□ Created Date
☑ Updated Date
□ OS Major
□ OS Minor
□ OS Description
□ User Tag 1
□ User Tag 2
☑ Port
□ Device ID
☑ Maint Until

3. Select the checkbox next to every column you want to display.

## Robot Property Fields

**Robot**

Name of the robot.

**Type**

Type of robot.

**Address**

Path to the robot in /<domain name>/<hub name>/<robot name> format.

**License**

True or False - Indicates whether the license is current for the robot.

**IP**

IP address of the robot.

**Version**

Version number of the robot.

**Latest Version**

Latest version of the robot.

**Communication Mode**

How the robot communications with the hub. The robot can be in one of three modes:

- Passive
- Normal
- None

**Created Date**

Date the robot was created.

**Updated Date**

Date the robot was updated.

**User Tag 1**

A User-defined field.

**User Tag 2**

A User-defined field.

**Port**

Port number for the robot. Default is 48000.

**Maint Until**

Date the robot is scheduled to be returned to active status from maintenance mode.

**Note**: This field only applies to robots that are placed in maintenance mode.

**OS Major**

Operating system the robot is installed on.

**OS Minor**

Version of the operating system running on the robot.

**OS Description**

Brief description of the operating system. Example: Service Pack 1.

**Processor**

Processor on the system.

**Started Time**

Time the robot was started.

**Robot Time**

Time at the point you selected the robot properties.

**Robot Time Zone**

Time zone where the robot system resides.

## Probes

This screen displays the probes that are installed on the robot and is used as the starting point for configuring your probes. The icon next to the probe name provides a drop-down list with tasks related to the probe. The menu includes:

- Activate
- Deactivate
- Restart
- Delete
- Configure
- Raw Configure
- Probe Utility
- View Log

These tasks are covered in the section on General Probe Configuration (see page 35).

### Installed Packages

This screen displays the packages that are installed on your robot.

The fields are:

**Package**

Package that is installed on this robot.

**Version**

Version number of the installed package.

**Build Number**

The build number for the package.

**Sections**

Target platforms for the package.

**Install Date**

Date the package was installed on the robot.

### Environment Variables

This screen displays the environment variables applicable to your robot. This list changes based on the operating system and probes that are installed on your robot.

## Archive Interface Overview

This section describes the local archive, web archive, and distribution activities for the probes on your UIM system.

### Local Archive

This screen displays the probes that reside in your local archive. This archive resides on the hub, therefore the list is the same for all robots that are connected to the hub. The archive lists the packages that have been downloaded to the local archive with the version, category, description, and link to the release notes. There can be more than one version of a package on the local archive.

If a newer version of the package exists on the web archive, an update button (⟳) is displayed on the right side of the screen.

You can deploy, import, group, and can delete probe packages from this screen. See the section titled Deploy Probes Using Admin Console (see page 31) for more information.

## Web Archive

This screen displays the list of probe packages on the support archive. You must have a valid login and password for the support site to download any package. See How to Connect to the Web Archive (see page 16) section for more information.

The archive lists the packages that are currently available for downloading, with the version, category, description, and link to the release notes.

## How to Connect to the Web Archive

**Follow these steps:**

1. Click the **Archive** button at the top of the Admin Console window.
2. Select the **Web Archive** button on the robot archive screen.
3. Click the key (🔑) icon.
4. Enter your username and password for the support site.
5. Click **Save**.

## Distribution Activity

This screen displays a log of your probe package distributions with the status of each distribution. Your packages can be deployed individually or in groups.

# Chapter 2: Manage Licenses

This section describes how to manage your probe licenses. An Administrator typically performs these procedures. The robot licenses are managed from the Settings button in the upper-right corner of the Admin Console screen. The hub licenses are managed by clicking the Configure Hub (⚙) icon next to the hub name in the navigation pane.

This section contains the following topics:

## How to Add a Hub License

**Follow these steps:**

1. Log in to the Admin Console.
2. Click the **Configure Hub** (⚙) icon.
3. Click the **Change** (✎) icon.
4. Cut and paste the hub license into the license field.
5. Click the **Save Changes** icon (💾).

   The hub restarts to update the license information.
6. Click **Yes**.

## How to View Robot Licenses

**Follow these steps:**

1. Log in to the Admin Console.
2. Click the **Settings** button.

   A drop-down list appears.
3. Select **Manage Licenses**.

   A Manage Licenses screen appears and contains a list of the probe licenses on your system.

## License Property Fields

You can customize the columns that appear by selecting the arrow next to any column heading and right-click. To sort either in ascending or descending order, or show or hide each license property field, use the arrow next to each field.

**Product**

Name of the probe.

**Info**

License description.

**Expiration Date**

Date the license expires.

**IP**

IP mask that is used to limit the systems that the probe is licensed to run on. An * indicates that the probe is licensed to run on all systems in this domain.

**Number**

Number of licenses for the probe package.

**Code**

Valid license code for the probe.

# How to Add a License

**Follow these steps:**

1. Log in to the Admin Console.
2. Click the **Settings** button.

   A drop-down list appears.
3. Select **Manage Licenses**.

   A Manage Licenses screen appears and contains a list of the probe licenses on your system.
4. Click the **Add** button.

   The Add Licenses screen appears.
5. Click in the window and cut and paste the license key from the email you received from the support team.

# How to Delete a License

**Follow these steps:**

1. Log in to the Admin Console.
2. Click the **Settings** button.

   A drop-down list appears.
3. Select **Manage Licenses**.

   A Manage Licenses screen appears and contains a list of the probe licenses on your system.
4. Select the check box next to the probe license you want to delete.
5. Click the **Delete** button.

   A confirmation message appears.
6. Click **OK** to delete the probe license.

   The deleted probe license is no longer in the list.

   **Note**: If the screen does not refresh, click the 🔄 (Refresh) button.

# Chapter 3: Manage Users

This section describes how to manage UIM users. A UIM Administrator that has full ACL permissions typically performs these procedures.

This section contains the following topics:

## How to View User Properties

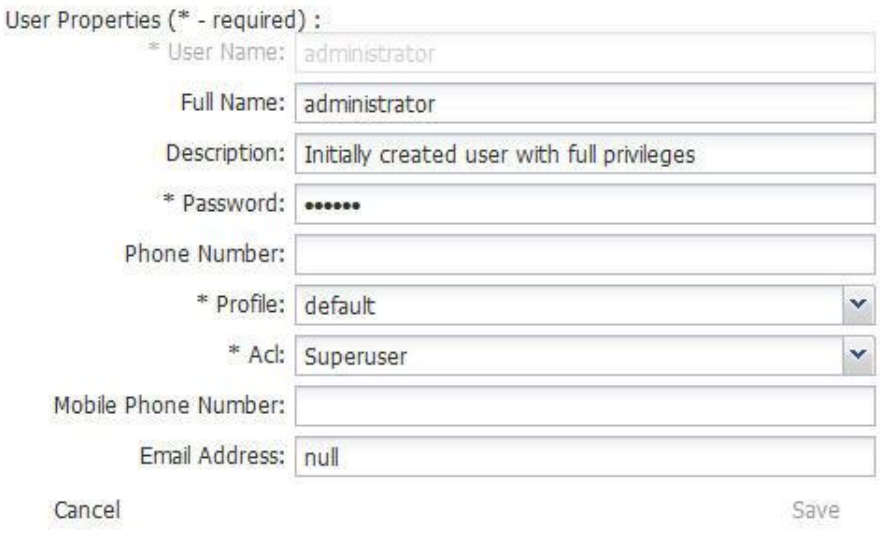
**Follow these steps:**

1. Log in to the Admin Console.
2. Click the **Settings** button.

   A drop-down list appears.
3. Select **Manage Users**.

   A Manage Users dialog appears.
4. Select a user name in the left navigation pane.

   The right pane displays the properties for the selected user.



User Properties (* - required) :

| | |
|---|---|
| * User Name: | administrator |
| Full Name: | administrator |
| Description: | Initially created user with full privileges |
| * Password: | •••••• |
| Phone Number: | |
| * Profile: | default |
| * Acl: | Superuser |
| Mobile Phone Number: | |
| Email Address: | null |

Fields with an * are required fields. See the User Property Fields (see page 22) section for a description of the fields. To refresh the user list, click **Refresh Users** in the upper left corner of the screen.

## User Property Fields

The user property fields are:

**User name**

The UIM user name. This field is read-only.

**Full name**

The full name for the UIM user.

**Description**

A brief description of the user.

**Password**

The password that is associated with the user name. Restrictions are: 6+ characters and cannot equal the user name.

**Phone Number**

The phone number for the UIM user.

**Profile**

The profile that is associated with the UIM user.

**ACL**

The access control list that is assigned to the UIM user.

**Mobile Phone Number**

The mobile phone number for the UIM user.

**Email Address**

The email address for the UIM user.

# How to Add a New User

**Follow these steps:**

1. Log in to the Admin Console.
2. Click the **Settings** button.

   A drop-down list appears.
3. Select **Manage Users**.

   A Manage Users dialog appears.
4. Click **New User**.
5. Complete the fields, then click **Save**.

   For field descriptions, see the User Property Fields (see page 22) section.

# How to Delete a User

**Follow these steps:**

1. Log in to the Admin Console.
2. Click the **Settings** button.

   A drop-down list appears.
3. Select **Manage Users**.

   A Manage Users dialog appears.
4. Select a user in the navigation pane.
5. Click **Delete Selected**.

   A confirmation message appears.
6. Click **Yes** to delete the user.

# How to Modify a User

**Follow these steps:**

1. Log in to the Admin Console.
2. Click the **Settings** button.

   A drop-down list appears.
3. Select **Manage Users**.

   A Manage Users dialog appears.
4. Select a user in the navigation pane.
5. Update the fields, then click **Save**.

# Chapter 4: Change Probe Security

**This section contains the following topics:**

This section describes how to manage security for probes.

## How to View Probe Security Settings

To view a list of the probes that are installed on your system and their respective access permissions, use the following procedure.

**Follow these steps:**

1. Log in to the Admin Console.
2. Click the **Settings** button.

   A drop-down list appears.
3. Select **Probe Security**.

   The Probe Security screen appears. See the Probe Security Access Fields (see page 25) section for more information.

### Probe Security Access Fields

The probe security access fields are:

**Probe**

Name of the probe.

**Access**

Access permissions.

**IP Mask**

The IP addresses of systems the probe is allowed to access. This field allows for the use of regular expressions. A wildcard (*) in this field allows access to all systems within the domain.

# How to Assign Probe Security Access to a Probe

Use this procedure when a probe has not been assigned access permissions. To modify the existing access permissions of a probe, see How to Modify Probe Security Access Levels (see page 26).

**Follow these steps:**

1. Log in to the Admin Console.
2. Click the **Settings** button.

   A drop-down list appears.
3. Select **Probe Security**.

   The Probe Security screen appears.
4. Click the **New** button.

   A pop-up dialog appears.
5. Select the probe name from the drop-down list.

   **Note**: Only probe names without access permissions are listed in this drop-down list.
6. Select the appropriate Access permissions from the drop-down list.
7. Click the **Create** button.

   The security access permissions are now assigned to the probe.

# How to Modify Probe Security Access Levels

**Follow these steps:**

1. Log in to the Admin Console.
2. Click the **Settings** button.

   A drop-down list appears.
3. Select **Probe Security**.

   The Probe Security screen appears.
4. Click the access level next to the probe you want to modify.

   A drop-down list button appears and the field refreshes.
5. Click the drop-down arrow and select the appropriate access level.

   The screen refreshes with the new access level assigned to the probe.

# How to Delete Probe Security Access Levels

**Follow these steps:**

1. Log in to the Admin Console.
2. Click the **Settings** button.

   A drop-down list appears.
3. Select **Probe Security**.

   The Probe Security screen appears.
4. Select the checkbox next to the probe you want to delete the security access.
5. Click the **Delete** button.

   A confirmation message appears.
6. Click **OK**.

   The probe is removed from the list after the screen refreshes.

# Chapter 5: How to Download Probes from Web Archive

The following section describes how to connect to the web archive and download probes.

This section contains the following topics:

## How to Connect to the Web Archive

**Follow these steps:**

1. Click the **Archive** button at the top of the Admin Console window.
2. Select the **Web Archive** button on the robot archive screen.
3. Click the key (🔑) icon.
4. Enter your username and password for the support site.
5. Click **Save**.

## How to Download a Probe

**Follow these steps:**

1. Click the **Archive** button at the top of the Admin Console window.
2. Click **Web Archive**.
3. Select the check box next to the probe you want to download.
4. Click **Download**.

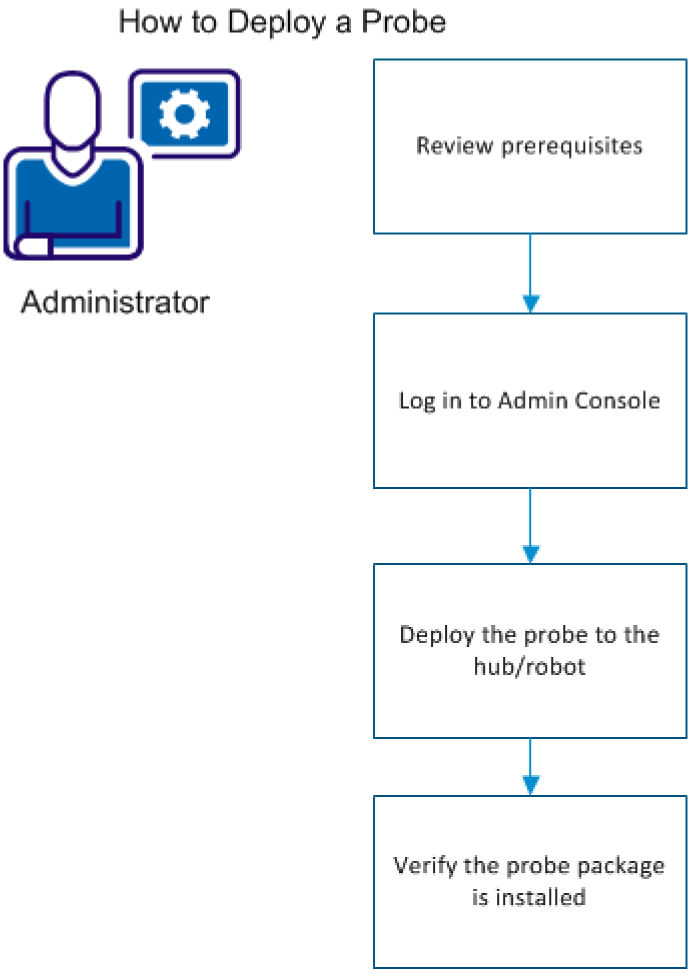
   You receive a confirmation message.

   **Note**:If your credentials are not entered you receive an error message. See the How to Connect to the Web Archive (see page 16) section for more information.
5. Click **Yes**.

The probe package is downloaded to your local archive.

# Chapter 6: Deploy Probes Using Admin Console

As a UIM Administrator, you deploy probes using the Admin Console application. UIM uses probes to monitor your system, send alarms and provide dashboards that display the status of your system. After deploying a probe you will need to configure the probe for your specific monitoring requirements.



This section contains the following topics:

# Review Probe Prerequisites

Before you deploy a probe, review its prerequisites for any environmental issues that may impede probe deployment. Look for probe prerequisite in the individual probe release notes or configuration document.

# Log in to Admin Console

Admin Console can be accessed either through a standalone web page or through UMP. The procedure for accessing your Admin Console application depends on the version of the Admin Console installed on your system.

## How to Log in to Admin Console in UMP

**Follow these steps:**

1. Connect to your UMP application in a web browser.
2. Enter a valid UIM user name and password.

   The Unified Management Portal opens to the USM portlet.
3. Click the Admin Console tab.

   **Note:** If the Admin Console tab is not available, see the Add Portlets (see page 9) section to add this portlet.

   The Admin Console screen appears.

Your system is available for configuration.

## How to Log in to Admin Console in a Standalone Web Page

**Follow these steps:**

1. Enter http://<service_host>:8080/adminconsole in your web browser window.

   **Note:** <service_host> is the system where the service_host probe is installed.

2. Enter a valid UIM username and password.

   The Admin Console application opens.

# Deploy a Probe to the Hub/Robot

**Follow these steps:**

1. Click the **Archive** button at the top of the Admin Console window.
2. Click **Local Archive** or **Web Archive**.

   **Note**: If the probe is not listed in the local archive and you deploy from the Web Archive, the probe will be download to your local archive.

3. Click the arrow button next to the hub name in the navigation pane to display the robots on the hub.
4. Select the check box(es) next to the name of the targeted robot(s) in the navigation pane.

   The right pane displays the probes available on the archive you selected above.

5. Select the check box(es) next to the name of the probe(s) you want to deploy.
6. Click the **Deploy** button at the top of the probe listing.

   You will receive a confirmation message.

7. Click **OK** to deploy the probe to the selected robot.

# Verify the Probe Package Deployed

**Follow these steps:**

1. Click the **Infrastructure** button at the top of the Admin Console screen.
2. Select the name of the robot where you deployed the probe.
3. Select the **Probes** button at the top of the right pane.

   The probe should be listed in the right pane.

The probe is now ready for you to configure.

# Chapter 7: General Probe Configuration

This section describes the general probe administration tasks that you can perform in the Admin Console application. For specific probe configuration information, see the individual probe configuration documents that are included in the Admin Console Probe Catalog.

This section contains the following topics:

## How to Activate a Probe

Activate a probe that has been deactivated from the Infrastructure menu.

**Follow these steps:**

1. Click the **Infrastructure** button.
2. Select the robot in the navigation pane. If you can't see the robot, expand the navigation tree.
3. Click the icon next to the probe name.

   A pop-up menu displays.
4. Select **Activate**.

   The probe is activated.

# How to Deactivate a Probe

**Follow these steps:**

1. Click the **Infrastructure** button.
2. Select the robot in the navigation pane. If you can't see the robot, expand the navigation tree.
3. Click the icon next to the probe name.

   A pop-up menu displays.
4. Select **Deactivate**.

   The probe is deactivated.

# How to Restart a Probe

**Follow these steps:**

1. Click the **Infrastructure** button.
2. Select the robot in the navigation pane. If you can't see the robot, expand the navigation tree.
3. Click the icon next to the probe name.

   A pop-up menu displays.
4. Select **Restart**.

   The probe is restarted.

# How to Delete a Probe

**Follow these steps:**

1. Click the **Infrastructure** button.
2. Select the robot in the navigation pane. If you can't see the robot, expand the navigation tree.
3. Click the icon next to the probe name.

   A pop-up menu displays.
4. Select **Delete**.

   The probe is removed from the robot.

# How to Configure a Probe

The probe must be running to configure it.

**Follow these steps:**

1. Click the **Infrastructure** button.
2. Select the robot in the navigation pane. If you can't see the robot, expand the navigation tree.
3. Click the icon next to the probe name.

   A pop-up menu displays.
4. Select **Configure**.

   The configuration GUI for the probe appears. See the specific probe documentation for more information about probe configuration.

# How to Locate Probe Template Items

The probe configuration GUI contains a left and right navigation pane. The left navigation pane contains a hierarchical representation of the monitoring targets and any configurable elements associated with the probe. The right navigation pane usually contains configuration information based on your selection in the left navigation pane. Refer to the applicable probe guide for more information about specific elements and configuration options.

The left navigation pane contains a filter to help locate items within the probe hierarchy. This filter is especially useful if you must manage multiple probe configuration elements.

Enter your filter criteria in the field at the top of the left navigation pane.

- The names of items that match your filter criteria appear as highlighted bold text.
- Collapsed items that contain child items that match your filter criteria appear as bold text.
- Items that do not match your filter criteria appear as gray text.
- Collapsed items that contain unloaded child items contain a ⊞ icon.

  **Note:** The filter only locates items loaded in the current view. It might be necessary to expand a collapsed item to load any child items.

# How to Configure Dynamic Alarm Thresholds

Dynamic alarm thresholds can be set at the QoS metric level in probes that publish alarms for a QoS metric.

**Important!** In order to create dynamic alarm thresholds, you must have the baseline_engine probe version 2.0 installed on the robot and configured.

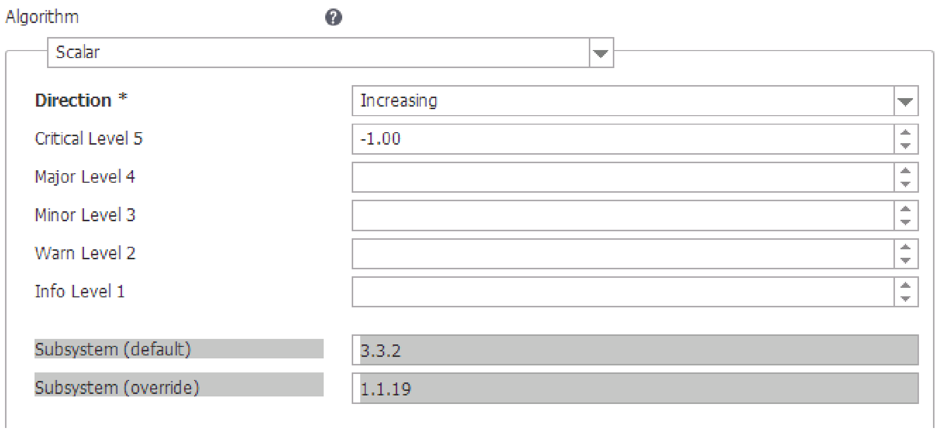
**Follow these steps:**

1. In the probe GUI, select a node in the tree to view any associated monitors and QoS metrics.
2. Select the monitor that you want to modify from the available list.
3. Click the **Publish Data** box.
4. Click the **Compute Baseline** box

   The Dynamic Alarm Thresholds section is enabled.
5. Change the dropdown in the Dynamic Alarm Thresholds section from **None** to **Dynamic**.

   The Dynamic Alarm Threshold section expands and more options become available.
6. Choose an Algorithm to use:
   - **Scalar** - Each threshold is a specific value from the computed baseline.
   - **Percent** - Each threshold is a specific percentage of the computed baseline.
   - **Standard Deviation** - Each threshold is a measure of the variation from the computed baseline. A large standard deviation indicates that the data points are far from the computed baseline. A small standard deviation indicates that they are clustered closely around the computed baseline.
7. Choose a direction for the threshold:
   - **Increasing** - An alarm occurs when the metric increases past the set threshold.
   - **Decreasing** - An alarm occurs when the metric falls below the set threshold.
8. Set the threshold for each alarm state.
9. Save your settings.

If you are using baseline_engine 2.1, you can also change the Subsystem ID using the Subsystem (override) field. This is only required if the Subsystem ID shown in the Subsystem (default) field is not correct for your configuration.



Algorithm

Scalar

| | |
|---|---|
| **Direction** * | Increasing |
| Critical Level 5 | -1.00 |
| Major Level 4 | |
| Minor Level 3 | |
| Warn Level 2 | |
| Info Level 1 | |
| Subsystem (default) | 3.3.2 |
| Subsystem (override) | 1.1.19 |

# How to Configure Static Alarm Thresholds

Static alarm thresholds can be set at the QoS metric level in some of the probes that publish alarms for a QoS metric.

**Important!** In order to create static alarm thresholds, you must have the baseline_engine probe version 2.2 installed on the robot and configured.

**Follow these steps:**

1. In the probe GUI, select a node in the tree to view any associated monitors and QoS metrics.
2. Select the monitor that you want to modify from the available list.
3. Click the **Publish Data** box.

   The Alarm Thresholds section is enabled.
4. Change the dropdown in the Static Alarm Thresholds section from **None** to **Static**.

   The Static Alarm Threshold section expands and more options become available.
5. Choose a direction for the static threshold:
   - **Increasing** - An alarm occurs when the metric increases past the set threshold.
   - **Decreasing** - An alarm occurs when the metric falls below the set threshold.
6. Set the threshold for each alarm state.
7. (Optional) If the Subsystem ID listed in the **Subsystem (default)** field is not correct for your configuration, enter the correct ID in the **Subsystem (override)** field.
8. Save your settings.

# Chapter 8: Time Over Threshold

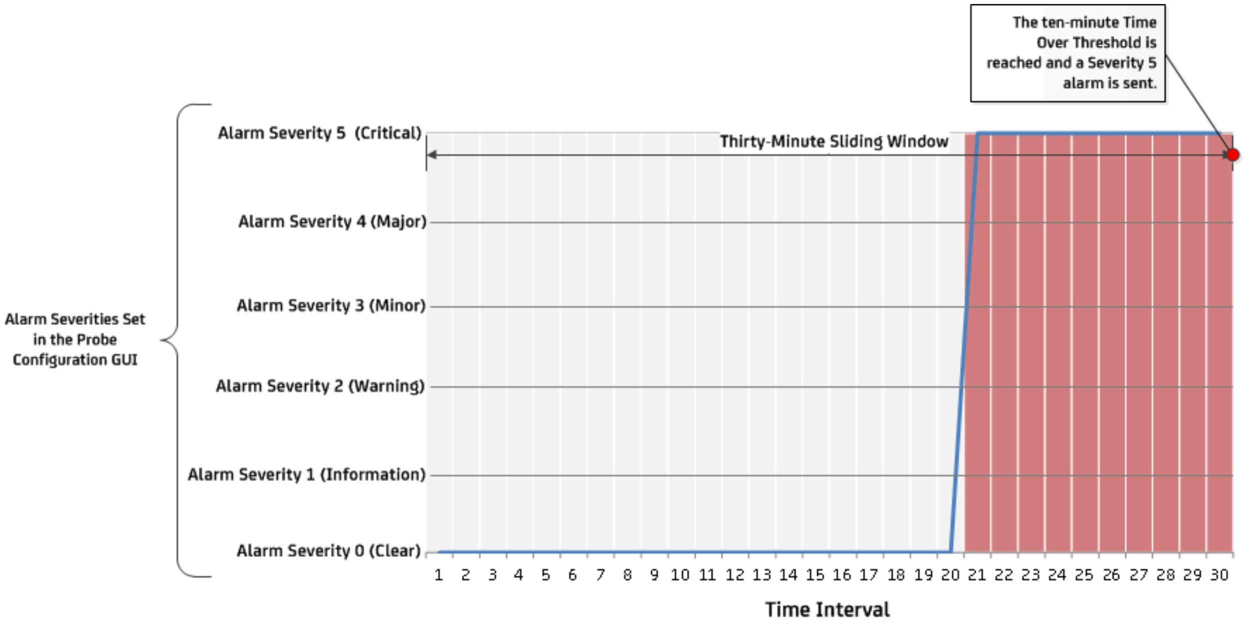
Time Over Threshold (TOT) is an event processing rule that allows you to reduce the number of alarms that are generated when threshold violation events occur. You can use Time Over Threshold to filter out data spikes and monitor problematic metrics over a set period. Instead of sending an alarm immediately after a threshold violation has occurred, Time Over Threshold:

- Monitors the events that occur during a user-defined sliding time window.
- Tracks the length of time that the metric is at each alarm severity.
- Raises an alarm if the cumulative time the metric is in violation during the sliding window reaches the set Time Over Threshold.

### Example: Time Over Threshold in a Consecutive Block

This example uses the following settings:

- **Sliding Window:** 30 minutes.
- **Time Over Threshold:** 10 minutes.
- **Auto-Clear:** Not set.
- **Alarm Severities:** Clear, Information, Warning, Minor, Major, and Critical alarm thresholds are set in the probe GUI.

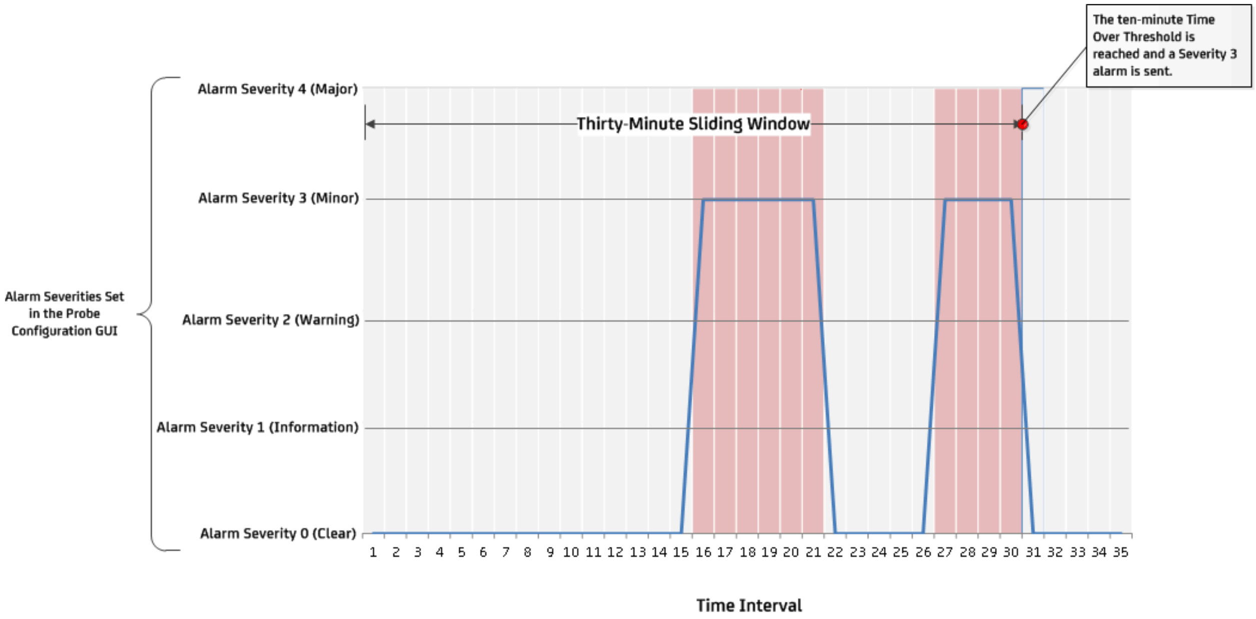


The Time Over Threshold does not have to occur consecutively within a sliding time window. All of the time in a sliding window is counted toward the Time Over Threshold.

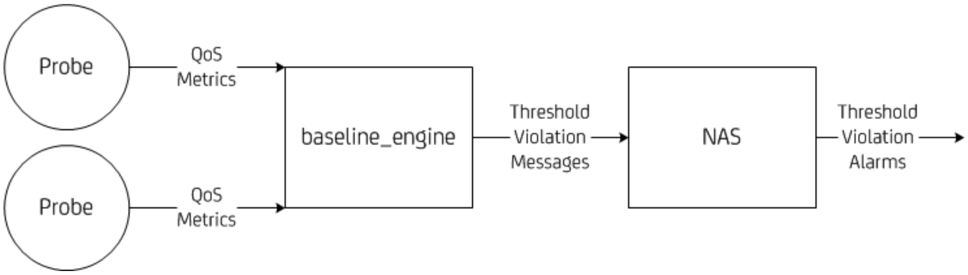
### Example: Time Over Threshold in a Nonconsecutive Block

This example uses the following settings:

- **Sliding Window:** 30 minutes.
- **Time Over Threshold:** 10 minutes.
- **Auto-Clear:** Not set.
- **Alarm Severities Set:** Clear, Information, Warning, Minor, and Major alarm thresholds are set in the probe GUI.



## Time Over Threshold Workflow



1. The baseline_engine probe evaluates QoS metrics from probes against static and dynamic threshold definitions.
2. The baseline_engine probe generates threshold violation messages when thresholds are crossed.
3. The nas probe implements the Time Over Threshold event processing rule to filter out data spikes. This event processing produces a more accurate reflection of threshold violation behavior.

## Alarm Suppression During Time Over Threshold

After a metric reaches a Time Over Threshold state, an alarm is generated for each additional threshold violation. By default, these duplicate alarms will increase the suppression count for the alarm, but will otherwise not be visible. If suppression is turned off, the duplicate alarms are treated as new alarms and will be visible in USM or the nas GUI.

## Alarm Clear Conditions Using Time Over Threshold

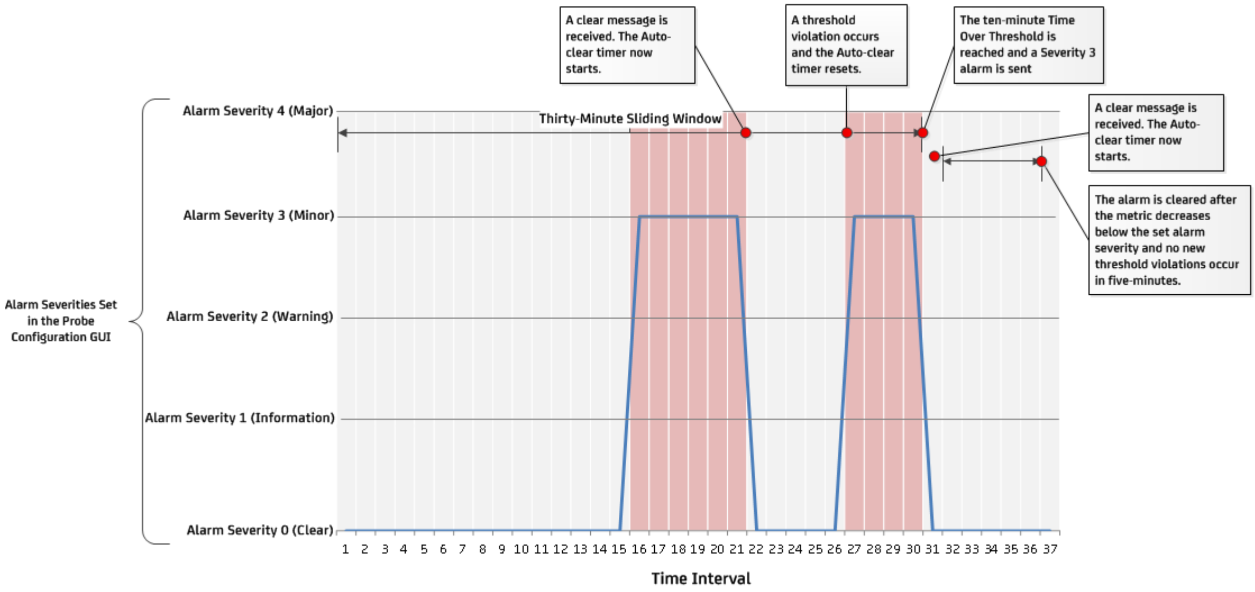
Auto-clear is an optional setting that clears a Time Over Threshold alarm when there are no new threshold violation events for the defined time period. If auto-clear is turned on, a timer begins after a clear event is received. If no subsequent threshold violation events arrive in the auto-clear window after the clear event is received, the alarm is automatically cleared (set to level 0). The arrival of a threshold violation event resets the clear rule, which waits for the next clear event to arrive before the timer starts again.

An auto-cleared Time Over Threshold alarm can be automatically acknowledged (and closed) using the Accept automatic 'acknowledgment' of alarm option in the nas probe GUI, which is enabled by default. If this option has been disabled, alarms will remain in the alarm history with Clear (green) Severity and must be manually acknowledged.

### Example: Time Over Threshold Using Auto-Clear

This example uses the following settings:

- **Sliding Window:** 30 minutes.
- **Time Over Threshold:** 10 minutes.
- **Auto-Clear:** 5 minutes
- **Alarm Severities:** Clear, Information, Warning, Minor, and Major alarm thresholds are set in the probe GUI.



## Alarm Severity Changes During Time Over Threshold

Time Over Threshold is evaluated at each user-defined event severity. This means that a metric must be at an elevated alarm severity for the defined Time Over Threshold before the severity changes. The new alarm severity level is then set to match cumulative event severity in the Time Over Threshold Window.

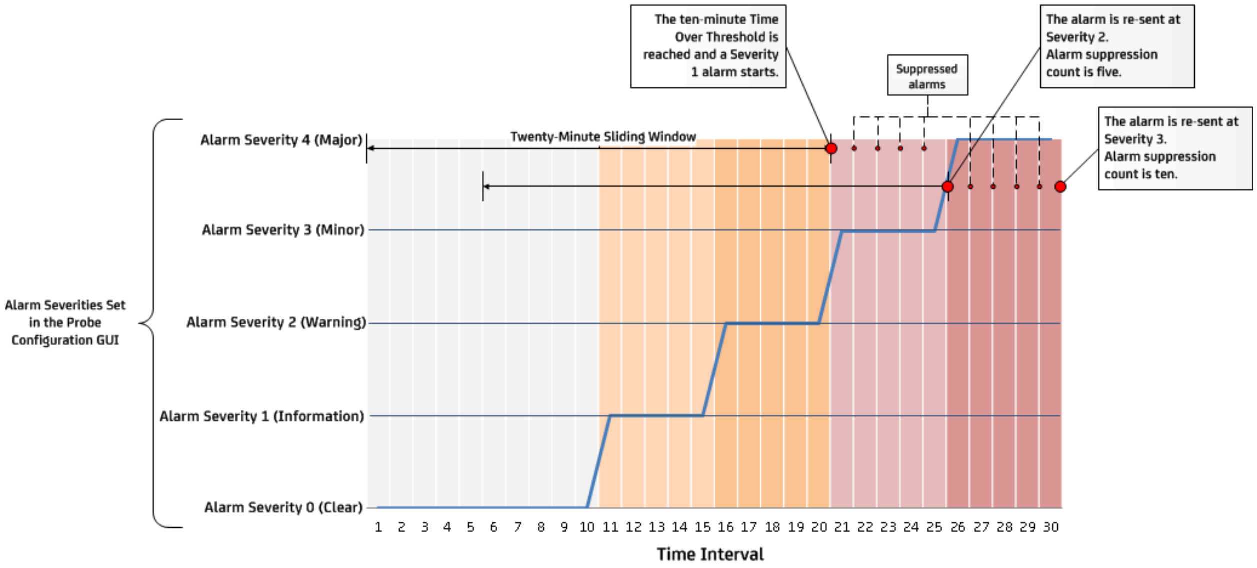
Each time a threshold violation event arrives, the Time Over Threshold alarm severity is determined as follows:

1. The cumulative time of the threshold violation events within the sliding window with Critical severity is calculated. If that time exceeds the defined Time Over Threshold, the alarm severity is set to Critical and rule processing is complete.
2. The cumulative time of threshold violation events within the sliding window with a severity that is Major or greater is calculated. If that time exceeds the defined Time Over Threshold, the alarm severity is set to Major and rule processing is complete.
3. The cumulative time of threshold violation events within the sliding window with a severity that is Minor or greater is calculated. If that time exceeds the defined Time Over Threshold, the alarm severity is set to Minor and rule processing is complete. Otherwise, the algorithm continues in this pattern for the remaining severity levels.

### Example: Time Over Threshold with Increasing Severity

**This example uses the following settings:**

- **Sliding Window:** 20 minutes.
- **Time Over Threshold:** 10 minutes.
- **Auto-Clear:** Not set.
- **Alarm Severities:** Clear, Information, Warning, Minor, and Major alarm thresholds are set in the probe GUI.
- **Alarm Suppression:** On.


The ten-minute Time Over Threshold is reached and a Severity 1 alarm starts.
Suppressed alarms
The alarm is re-sent at Severity 2. Alarm suppression count is five.
The alarm is re-sent at Severity 3. Alarm suppression count is ten.
Twenty-Minute Sliding Window
Alarm Severities Set in the Probe Configuration GUI
Alarm Severity 4 (Major)
Alarm Severity 3 (Minor)
Alarm Severity 2 (Warning)
Alarm Severity 1 (Information)
Alarm Severity 0 (Clear)
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
Time Interval

**In this example:**

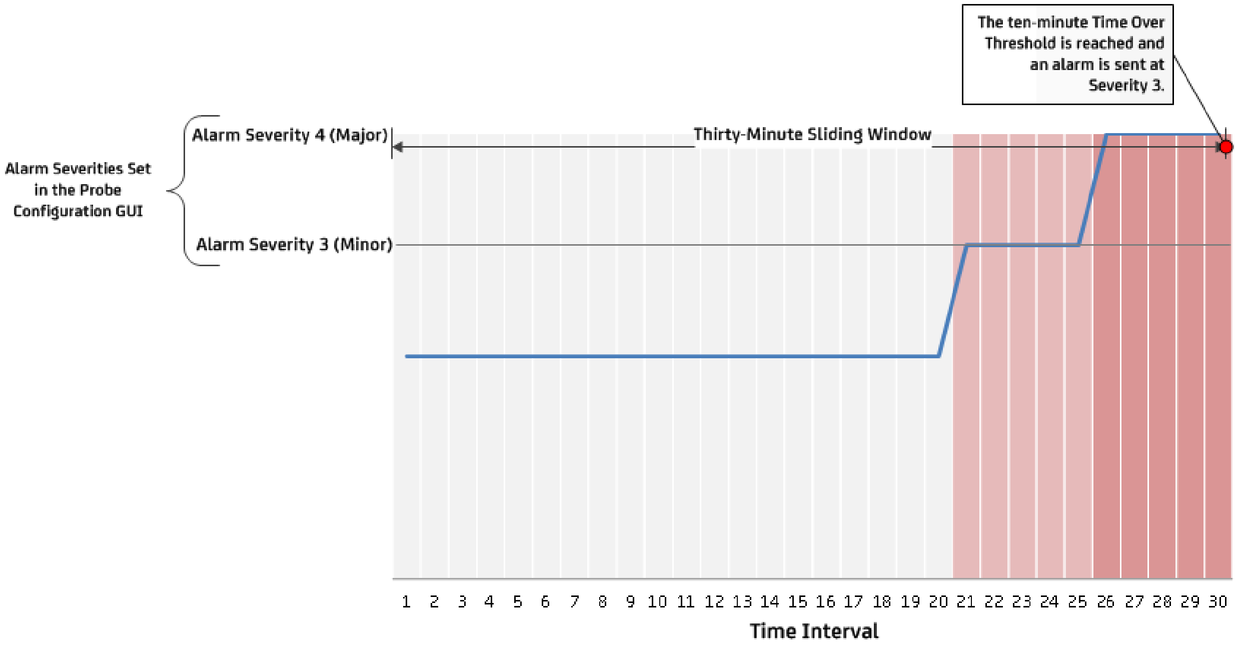
1. **Time 20** - A Time Over Threshold alarm is raised after ten minutes of Time Over Threshold event time is accumulated. The alarm severity is set to 1, because the first Time Over Threshold rule condition that matches is 'event severity is 1 or greater'.
2. **Time 25** - The severity is elevated to 2 because the Time Over Threshold rule condition 'event severity is 2 or greater' is now true
3. **Time 30** - The severity is elevated to 3 because the Time Over Threshold rule condition 'event severity is 3 or greater' is now true.

**Note:** Time Over Threshold only evaluates on alarm severity levels that are set in the probe configuration GUI.

### Example: Time Over Threshold with Two Set Severities

**This example uses the following settings:**

- **Sliding Window:** 30 minutes.
- **Time Over Threshold:** 10 minutes.
- **Auto-Clear:** Not set.
- **Alarm Severities:** Minor and Major alarm thresholds are set in the probe GUI.



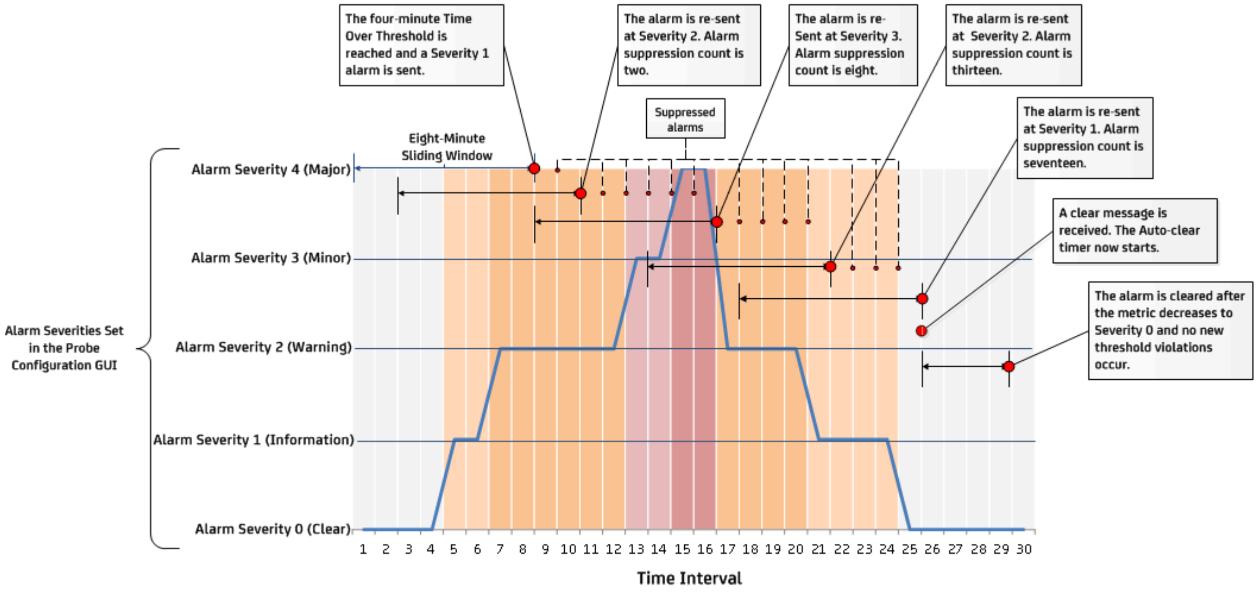
**In this example:**

1. **Time 30** - A Time Over Threshold alarm is raised after ten minutes of Time Over Threshold event time is accumulated. The Time Over Threshold alarm severity is set to 3, because the first Time Over Threshold rule condition that matches is 'event severity is 3 or greater'.

### Example: Time Over Threshold With Multiple Severities

**This example uses the following settings:**

- **Sliding Window:** 8 minutes.
- **Time Over Threshold:** 4 minutes.
- **Auto-Clear:** 4 minutes.
- **Alarm Severities:** Clear, Information, Warning, Minor, and Major alarm thresholds are set in the probe GUI.
- **Alarm Suppression:** On.



The four-minute Time Over Threshold is reached and a Severity 1 alarm is sent.

The alarm is re-sent at Severity 2. Alarm suppression count is two.

The alarm is re-Sent at Severity 3. Alarm suppression count is eight.

The alarm is re-sent at Severity 2. Alarm suppression count is thirteen.

The alarm is re-sent at Severity 1. Alarm suppression count is seventeen.

A clear message is received. The Auto-clear timer now starts.

The alarm is cleared after the metric decreases to Severity 0 and no new threshold violations occur.

**In this example:**

1. **Time 8** - A Time Over Threshold alarm is raised after four minutes of Time Over Threshold event time is accumulated. The alarm severity is set to 1, because the first Time Over Threshold rule condition that matches is 'event severity is 1 or greater'.
2. **Time 10** - The severity is elevated to 2 because the TOT rule condition ‘event severity is 2 or greater’ is now true.
3. **Time 16** - The severity is elevated to 3 because the TOT rule condition ‘event severity is 3 or greater’ is now true.
4. **Time 21** - The alarm severity decreases to 2 because there are no longer 4 minutes or more of severity 3 or greater within the 8-minute sliding window, but there are 4 minutes or more of severity 2 or greater
5. **Time 25** - The alarm severity decreases to 1 because there are no longer 4 minutes or more of severity 2 or greater within the 8-minute sliding window, but there are 4 minutes or more of severity 1 or greater
6. **Time 30** - The alarm is cleared because no new violations occur for four-minutes and the auto-clear condition is met.

## Supported Threshold Types

The following threshold limit types are currently supported with Time Over Threshold:

**Static** -No alarms are sent until sufficient alarms meeting the time requirements have exceeded the threshold.

> **Note:** A static threshold is effectively a high pass filter with extra averaging.

**Dynamic**- A dynamic threshold is calculated on variance from the calculated static baseline with no averaging. Variances can be set to one of the following algorithms:

- **Scalar** - A set value past the calculated baseline.
- **Percent** - A set percent past the baseline.
- **Standard Deviation** -A set standard deviation past the baseline.

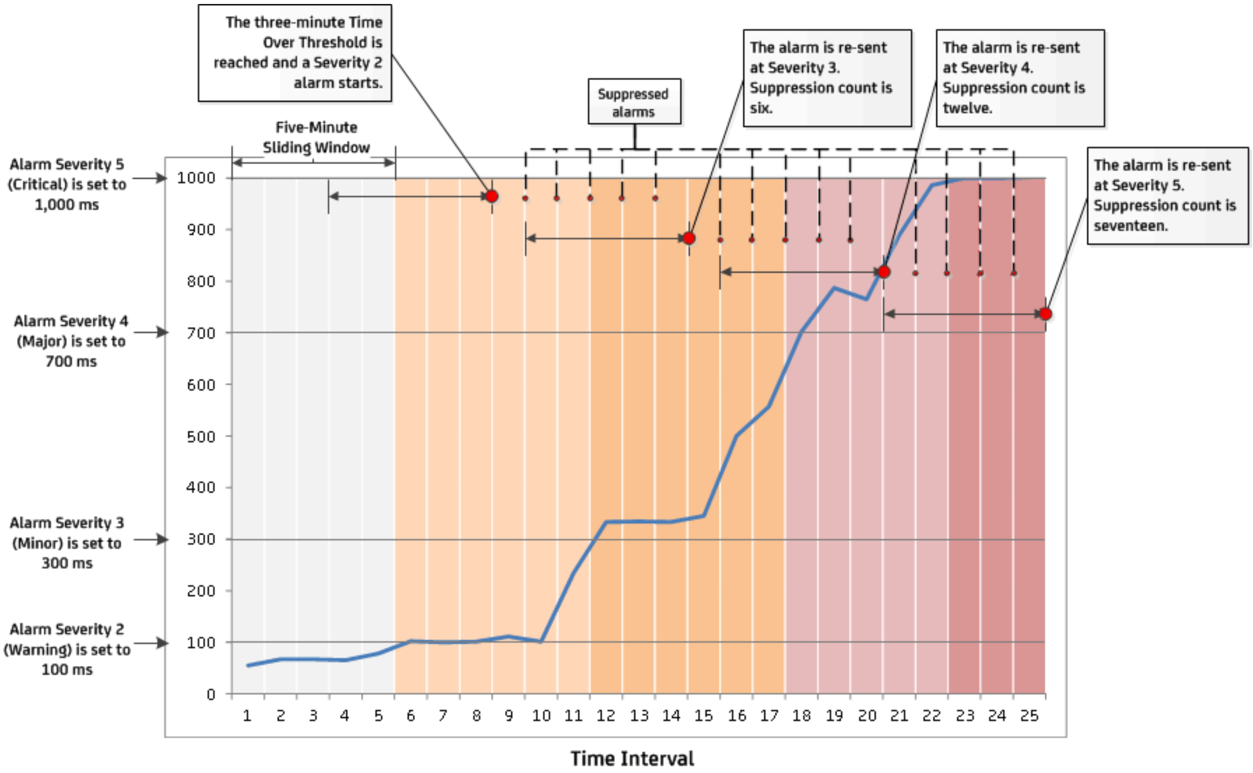
## Additional Time Over Threshold Scenarios

The following examples show extra Time Over Threshold scenarios using specific probe metrics.

### Example: URL_response Probe Metric Time to First Byte

**This example uses the following settings:**

- **Sliding Window:** 5 minutes.
- **Time Over Threshold:** 3 minutes.
- **Auto-Clear:** Not set.
- **Alarm Severities:**
  - Alarm Severity 2 is set to 100 ms.
  - Alarm Severity 3 is set to 300 ms.
  - Alarm Severity 4 is set to 700 ms.
  - Alarm Severity 5 is set to 1,000 ms.
- **Alarm Suppression:** On.


The three-minute Time Over Threshold is reached and a Severity 2 alarm starts.

Suppressed alarms

The alarm is re-sent at Severity 3. Suppression count is six.

The alarm is re-sent at Severity 4. Suppression count is twelve.

The alarm is re-sent at Severity 5. Suppression count is seventeen.

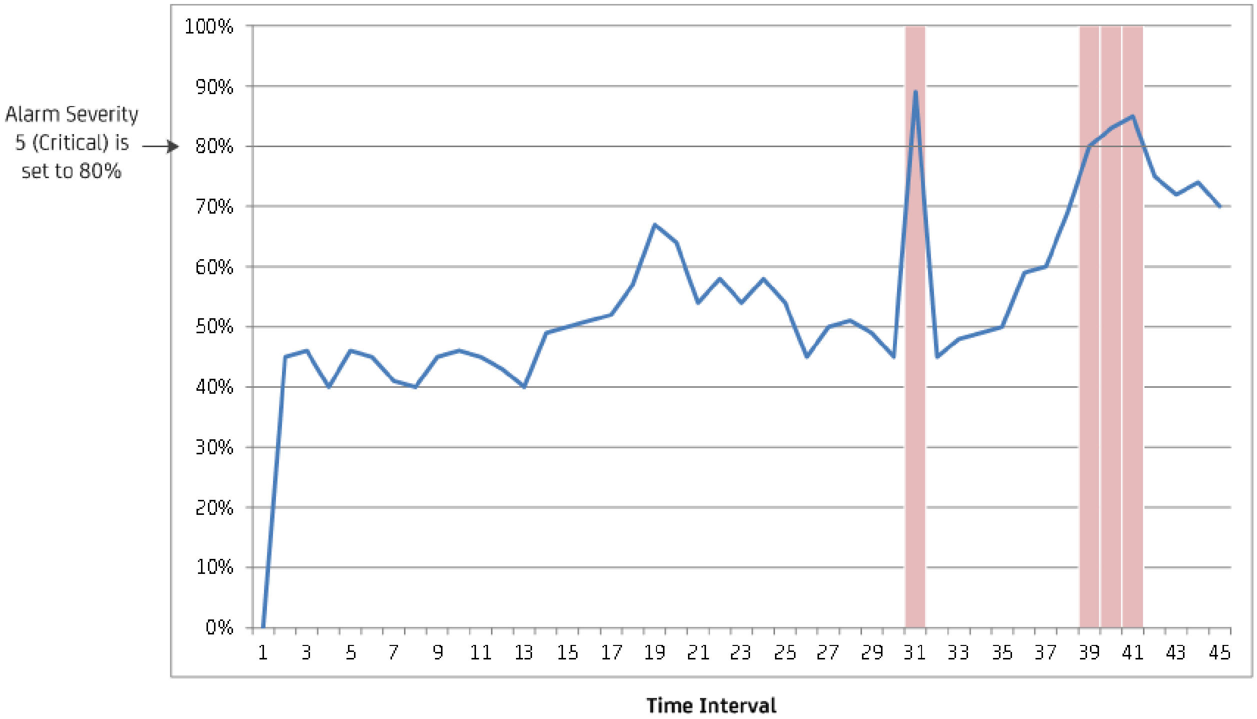
**In this example:**

1. **Time 8** -Three-minutes of time to first byte of 100 ms or greater is observed in the sliding window and an alarm of severity 2 is sent.
2. **Time 14** - Three-minutes of time to first byte of 300 ms or greater is observed. The alarm increases to severity 3.
3. **Time 20** - Three-minutes of time to first byte of 700 ms or greater is observed. The alarm increases to severity 4.
4. **Time 25** - Three-minutes of time to first byte of 1000 ms or greater occurs. The alarm increases to severity 5.

### Example: CDM Probe Metric Disk Usage

**This example uses the following settings:**

- **Sliding Window:** 45 minutes.
- **Time Over Threshold:** 5 minutes.
- **Auto-Clear:** Not set.
- **Alarm Severities:** The Critical alarm threshold is set to 80% in the probe GUI.



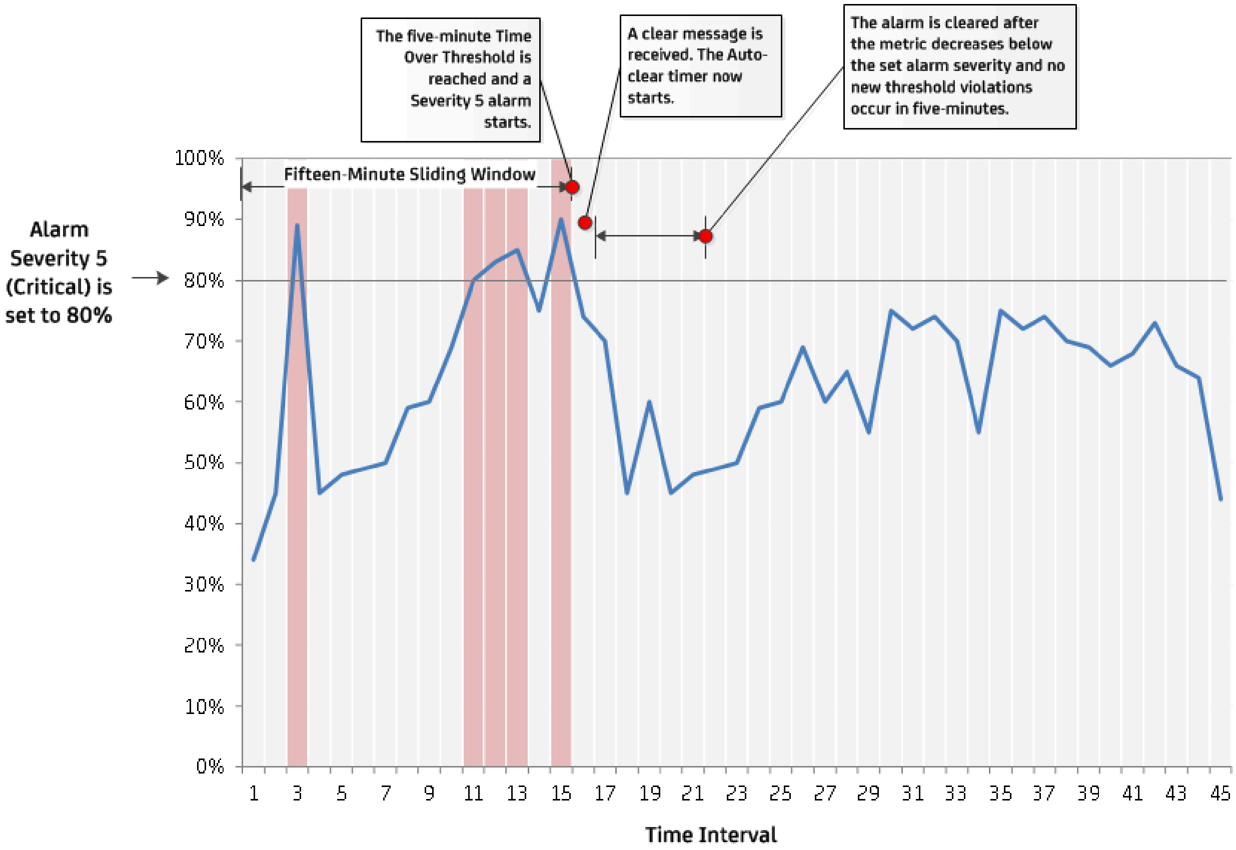
**In this example:**

1. Time Over Threshold only occurs for four-minutes and no alarm is sent.

### Example: CDM Probe Metric Disk Usage (Modified to Send a Time Over Threshold Alarm)

**This example uses the following settings:**

- **Sliding Window:** 15 minutes.
- **Time Over Threshold:** 5 minutes.
- **Auto-Clear:** 5 minutes.
- **Alarm Severities:** The Critical alarm threshold is set to 80% in the probe GUI.



1. **Time 15** -Five-minutes of disk usage at 80% or greater is observed in the sliding window and an alarm of severity 5 is sent.
2. **Time 21** - The alarm is cleared after five-minutes of time below the set severity level.

## Best Practices for Time Over Threshold

Observe the following best practices when using Time Over Threshold:

- Set Time Over Threshold only if you need an averaged or leveled-out alarm state, in which case you will see fewer alarms. If you must see every alarm coming from a system, do not activate Time Over Threshold for that monitored system.
- Be aware that Time Over Threshold can hide the sudden transition of alarms states (alarm spikes).
- Set the Auto-clear window to a longer interval than the Time Over Threshold. Setting a smaller Auto-clear window results in an excessive number of alarms due to rapid Auto-clears.
- Set the Time Over Threshold to a longer interval than the sample period for the QoS metric. Setting a smaller Time Over Threshold produces the same results as leaving the Time Over Threshold rule disabled.
- Evaluate your monitored system and determine the appropriate values for both the sliding window and Time Over Threshold. Values that are too large for your system can result in the suppression of alarms you may need to be aware of.

## Configure Time Over Threshold

Time Over Threshold is set at the QoS metric level in some of the probes that publish alarms for a QoS metric.

In order to create static alarm thresholds, you must have the following probe versions installed :

- baseline_engine 3.0
- ppm 2.38
- nas 4.38

### Configure the Threshold Type

Before setting the Time Over Threshold parameters, you must enter the threshold settings for either a dynamic (see page 54) or static (see page 55) threshold.

## Configure a Dynamic Alarm Threshold

**Follow these steps:**

1. In the probe GUI, select a node in the tree to view any associated monitors and QoS metrics.
2. Select the monitor that you want to modify from the available list.
3. Click the **Publish Data** box.
4. Click the **Compute Baseline** box

   The Dynamic Alarm Thresholds section is enabled.
5. Change the dropdown in the Dynamic Alarm Thresholds section from **None** to **Dynamic**.
6. Choose an Algorithm to use:
   - **Scalar** - Each threshold is a specific value from the computed baseline.
   - **Percent** - Each threshold is a specific percentage of the computed baseline.
   - **Standard Deviation** - Each threshold is a measure of the variation from the computed baseline. A large standard deviation indicates that the data points are far from the computed baseline. A small standard deviation indicates that they are clustered closely around the computed baseline.
7. Choose a direction for the threshold:
   - **Increasing** - An alarm occurs when the metric increases past the set threshold.
   - **Decreasing** - An alarm occurs when the metric falls below the set threshold.
8. Set the threshold for each alarm state.
9. (Optional) If the Subsystem ID listed in the **Subsystem (default)** field is not correct for your configuration, enter the correct ID in the **Subsystem (override)** field.

## Configure a Static Alarm Threshold

**Note:** As of current release, only the following probes support static alarm thresholds with Time Over Threshold:

- aws 2.01
- ICMP 1.0
- websphere_mq 1.0

**Follow these steps:**

1. In the probe GUI, select a node in the tree to view any associated monitors and QoS metrics.
2. Select the monitor that you want to modify from the available list.
3. Click the **Publish Data** box.
4. Change the dropdown in the Static Alarm Thresholds section from **None** to **Static**.
5. Choose a direction for the static threshold:
   - **Increasing** - An alarm occurs when the metric increases past the set threshold.
   - **Decreasing** - An alarm occurs when the metric falls below the set threshold.
6. Set the threshold for each alarm state.
7. (Optional) If the Subsystem ID listed in the **Subsystem (default)** field is not correct for your configuration, enter the correct ID in the **Subsystem (override)** field.

## Set the Time Over Threshold Parameters

After an alarm threshold is set, the Time Over Threshold parameters will become available.

**Follow these steps:**

1. Click the **Enable Time Over Threshold** box.
2. Enter values for the following parameters:

   **Time Over Threshold <TOT>**

   The length of time a metric must remain over threshold before an alarm is sent.

   **Sliding Time Window <TW>**

   The length of time in the sliding window in which metrics are monitored for threshold violations.

   **Time Units for <TOT> and <TW>**

   The unit of measurement used by the **Time Over Threshold** and **Time Window** parameters. Limited to minutes, hours, or days.

   **Automatically Clear Alarm**

   Enables the Auto-clear (see page 43) functionality.

   **Clear Delay Time**

   The length of time used in the Auto-clear timer. If no alarms are sent in the set time period, the alarm is automatically cleared.

   **Time Units for <TC>**

   The unit of measurement used by the Auto-clear. Limited to minutes, hours, or days.
3. Save your changes.

# Raw Configure Utility

Many probes have their own custom configuration utility. For the probes that do not, Admin Console presents the probe configuration data in an editor similar to regedit.

Raw configure lets you add, delete, and modify the nodes in the configuration file, and the variable name/value elements.

**Note**: You can use this method for any probe.

## How to Use Raw Configure

**Follow these steps:**

1. Click the **Infrastructure** button.
2. Select the robot in the navigation pane. If you can't see the robot, expand the navigation tree.
3. Click the icon next to the probe name.

   A pop-up menu displays.
4. Select **Raw Configure**.

   The Raw Configure screen appears.

### How to Add Keys

1. In the Raw Configure Menu, click on the folder you want to add the key in.
2. Click on the New Key Menu item.
3. Enter the Key Name in the Add key window, click **Add.**

   The new key appears in the list of keys with a blank value.
4. Click in the Value column for the newly created key and enter the key value.
5. Repeat this process for all of the required keys.
6. Click **Apply**.

# Probe Utility

Using the Probe utility allows you to run a probe command set and view the output in the right pane for debugging purposes.

## How to Use Probe Utility

**Follow these steps:**

1. Click the **Infrastructure** button.
2. Select the robot in the navigation pane. If you can't see the robot, expand the navigation tree.
3. Click the icon next to the probe name.

   A pop-up menu displays.
4. Select **Probe Utility**.

   The probe utility screen appears.
5. To execute the command, select a command from the drop-down list then click the **green arrow** button.

   The results are displayed in the right pane.

# Probe Log Files

Each probe has a log file. This file contains information about the probe and is used for debugging purposes. A default of 500 lines displays in the Log viewer window. You can set this value to any number from 100 through 10,000 lines.

## How to View a Probe Log File

**Follow these steps:**

1. Click the **Infrastructure** button.
2. Select the robot in the navigation pane. If you can't see the robot, expand the navigation tree.
3. Click the icon next to the probe name.

   A pop-up menu displays.
4. Select **View Log**.

   The Log Viewer screen appears.

## How to Download a Log File

**Follow these steps:**

1. Click the **Infrastructure** button.
2. Select the robot in the navigation pane. If you can't see the robot, expand the navigation tree.
3. Click the icon next to the probe name.

   A pop-up menu displays.
4. Select **View Log**.

   The Log Viewer screen appears.
5. Select the **Download Log** (⤓) icon.

   The download starts.

## How to Clear a Log File

**Follow these steps:**

1. Click the **Infrastructure** button.
2. Select the robot in the navigation pane. If you can't see the robot, expand the navigation tree.
3. Click the icon next to the probe name.

   A pop-up menu displays.
4. Select **View Log**.

   The Log Viewer screen appears.
5. Click the **Clear** (◆) icon.

   The log file is cleared.