Iris Alarms

Version 7.13.2

NOTE

The content in this document is a subset of the Iris online help and user guides. Not all links within the document are active. Refer to the Iris online help and user guides for access to complete information about a feature.

Tektronix communications

Copyright

Tektronix Communications
3033 W President George Bush Highway
Plano, TX 75075 USA
+1 469-330-4000 (voice)
www.tekcomms.com

992-0472-08-001-140228

Table of Contents

What's New in Iris Alarms 7.13.2

The following sections describe changes in Alarms version 7.13.2

Feature ID	Description	Section
F-01940	SNMP Handshake Alarm This feature provides support to send a test SNMP trap to an external SNMP trap receiver at a configurable interval. This enables the user to more quickly determine if there is an issue with the SNMP receiver.	System Alarms Tab
F-02567	Support for Alarming Based on Cause Code This feature adds support for creation of IPI alarm policies per specific response codes. Alarming on cause value can pinpoint a specific network failure and lead to faster resolution times for the user.	Creating an IPI Policy Based on Response Codes Condition and Assignment Editor Window Iris Application Policies and Alarms

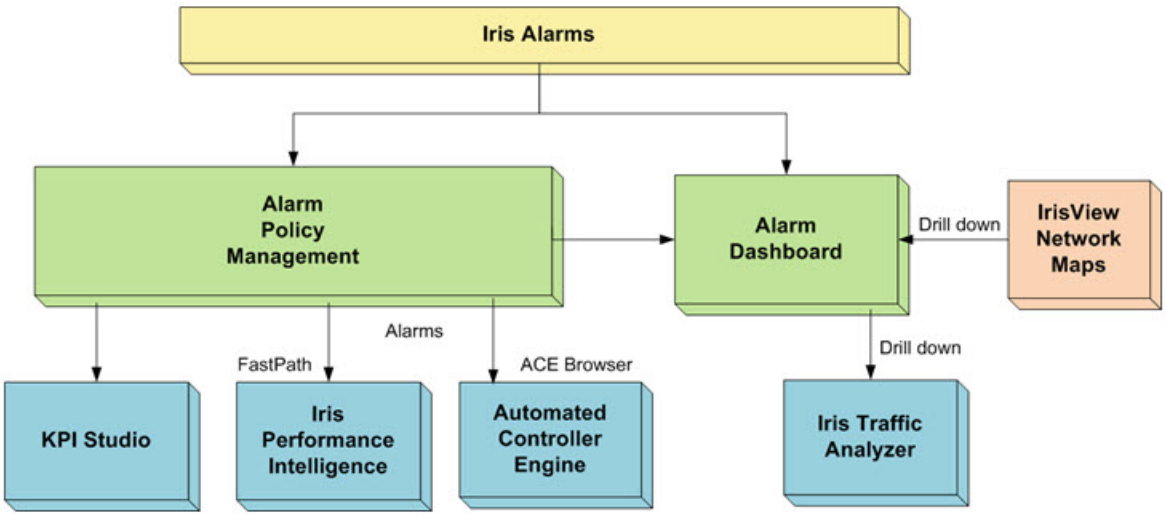
Iris Alarms Components

The Iris Alarms application enables you to manage the following tasks:

- Define and apply Alarm Policies that set performance thresholds for network entities (ITA), services (IPI, KPI Studio), or initiating tests (ACE).
- Configure severity and threshold levels for G10 system-level alarms.
- Monitor the status of network elements and services when they exceed a set policy threshold and generate alarms.
- Monitor and view details on system-generated alarms.

Iris Alarms Components

Click on any of the following Iris Alarms components to view a detailed description workflow for each component.



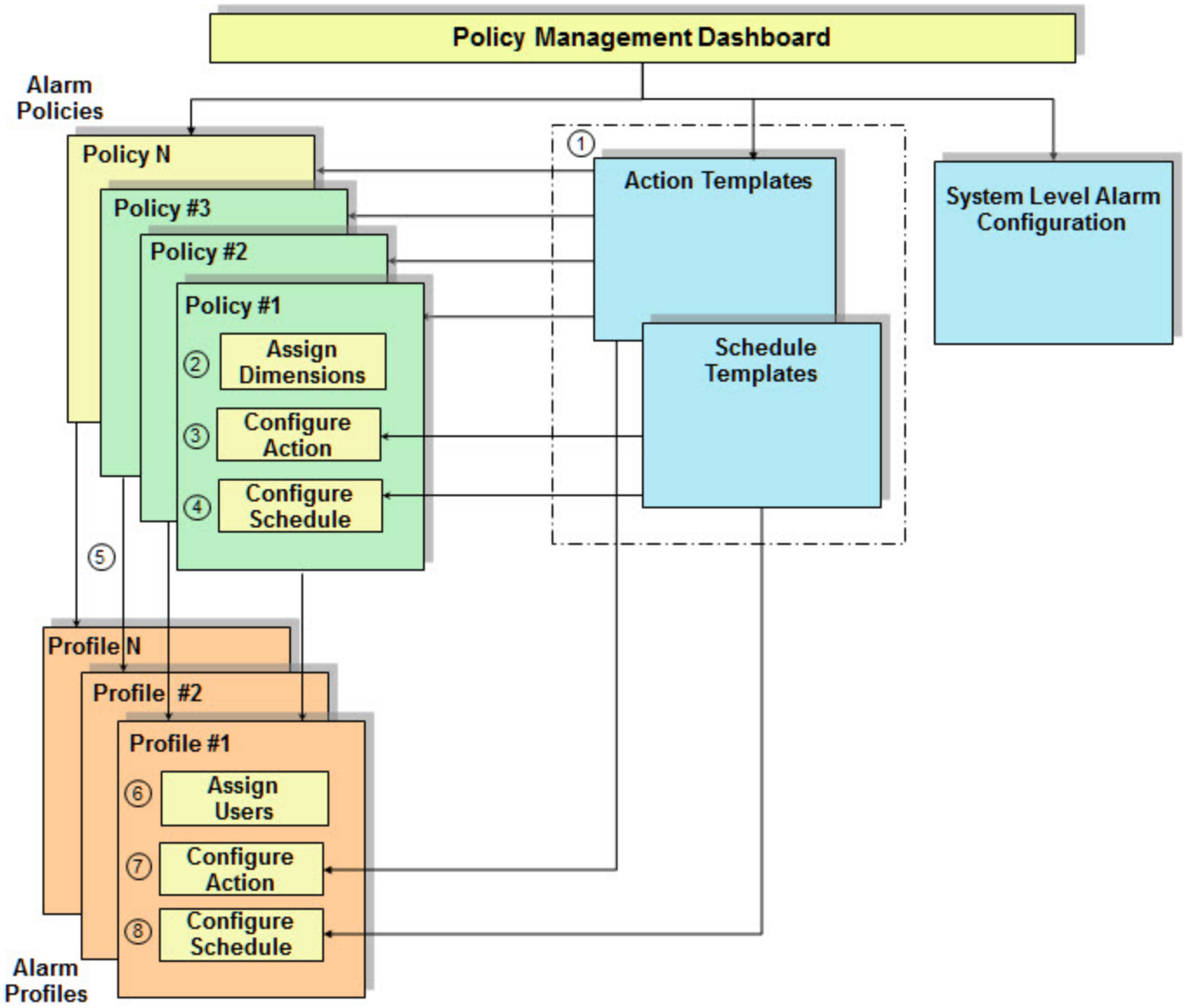
Policy Management Workflow

The Policy Management dashboard enables you to perform the following tasks:

- Create and manage alarm policies for specific Iris applications.
- Create and manage templates:
  - Action Templates - to configure actions to take when an alarm is breached
  - Schedule Templates - to configure time periods when alarm policies and alarm profiles are active
- Create and manage alarm policies to evaluate threshold breaches on complex combinations of KPIs and KQIs
- Create and manage alarm profiles for grouping alarms.
- Generate alarms to display in the Alarm browser, generate email notification on the alarm, initiate a test, or forward alarms using SNMP.
- Configure severity and threshold levels for G10 system alarms and forward using SNMP.
- Send test traps to SNMP destinations to help detect outages.

Policy Management Components

Click on any of the following components to see an overview of each component.



Policy Management Workflow

The following steps describe the Policy Management workflow.

1. Create Action and Schedule templates to assign to new policies and profiles.
2. Create a new policy, assign one or more dimensions to the new policy, and enable the policy.
3. Apply an action template that controls what action to take when the alarm threshold is breached.
4. Apply a schedule template to control when the alarm policy is active.

Optionally, you can group policies into profiles that you can assign to users having the same functional responsibilities. Profiles enable you to control what alarms specific users can view.

5. Add a new profile and assign to it one or more policies. A policy can only be assigned to one profile.
6. Assign users who you want to view the alarms for this profile.

7. Apply an action template for the profile.
8. Apply a schedule template for the profile.

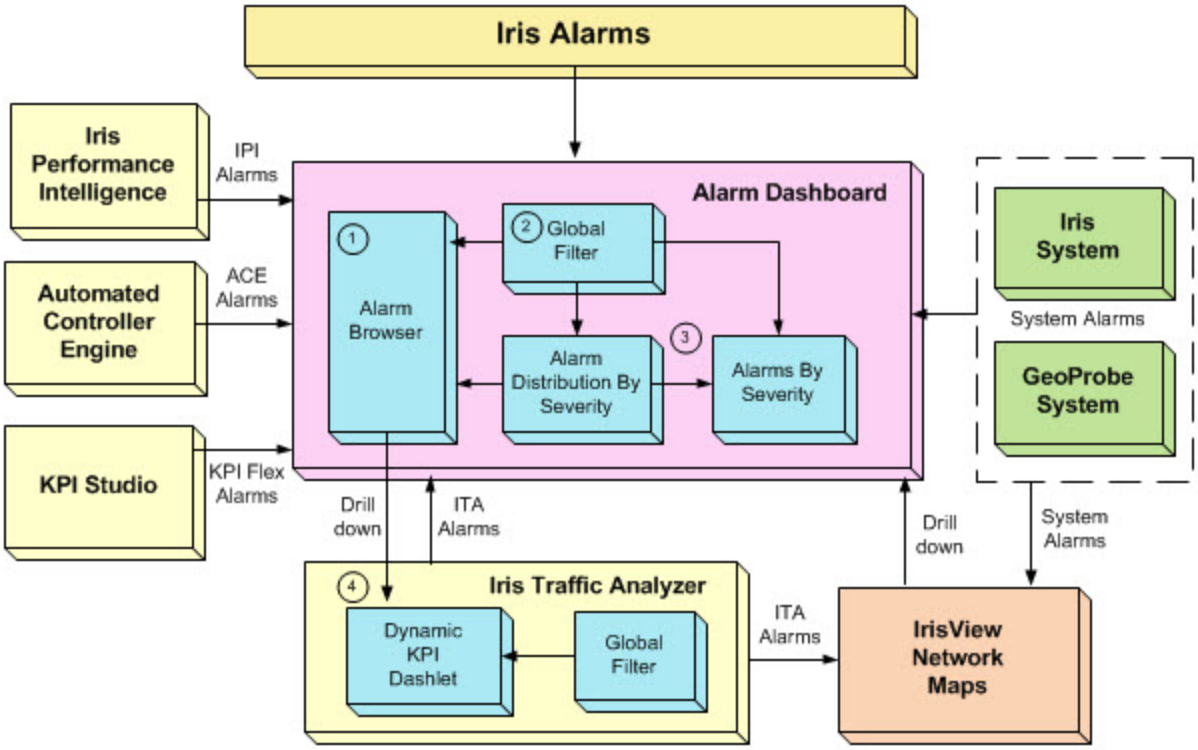
Alarm Dashboard Workflow

The Iris Alarm Dashboard enables you to manage the following tasks:

- Monitor the status of network elements and services when they exceed a set policy threshold and generate alarms.
- Monitor and view details on system-generated alarms.

Alarm Dashboard Components

Click on any of the following Iris Alarms components to view a detailed description of each component.



Alarm Dashboard Workflow

The following steps describe the Iris Alarm Dashboard workflow. You must first configure alarm policies for the applications for which you want to generate alarms.

1. Monitor Iris application and system-level alarms using the Alarm Browser on the Alarm Dashboard.
2. Set global filters to define alarm views as needed.
3. Analyze alarm distribution using the Alarm Distribution KPI dashlets. View pie and bar charts showing alarm distribution by status: Minor, Major, Critical, or Informational.
4. For some ITA alarms, drill down from the Alarm Browser to view a KPI dashlet associated with the alarm and analyze ITA KPIs using a global filter.

Iris Alarms Use Cases

The following use cases are provided as examples of how to use Iris Alarms to troubleshoot problems.

- Setting Up Alarm Thresholds for Link Utilization Use Case
- Creating an IPI Network Service Policy Use Case
- Analyzing Critical Alarms Using the Alarm Dashboard
- Using IPI to Detect One-Way Audio
- Using Email Notification to Drill Down on Alarm Elements
- Creating an IPI Policy Based on Response Codes

Setting Up Alarm Thresholds for Link Utilization

This use case illustrates how you can set thresholds on the Link Utilization KPI, which Iris monitors.

Background

You want to generate an alarm if the link utilization on a group of links exceeds 50% to ensure that you have enough resources to handle the current traffic load. You can use the Iris Policy Management to configure a policy and then apply it to a group of elements. The Alarm dashboard provides a snapshot of all threshold violations, as well as any system-level alarms raised.

To Set Up an Alarm Threshold for Link Utilization

1. To access the Alarms Policy page, click **Alarms** in the IrisView toolbar and select **Policy Management** from the submenu. The Policy Management dashboard appears displaying the Policies tab.
2. Click the **Policies** tab to display the Policy List pane.
3. Click **Add** and select **ITA** at the prompt to display a blank form in the Policy Details pane.
4. Enter a name and optional description for the new policy.
5. Select the severity: Critical, Major, Minor, or Informational.
6. Change the aggregation window and a sample interval, as needed.
7. Then select the Interface from available options.

Configure Policy KPI Conditions

1. In the Policy Details Pane Conditions area, click the **Add** button to open the Condition and Assignment Editor.
2. In the Category field, select **Link**.
3. Select **Link Utilization Downlink** from the KPI/KQI drop-down menu. For details, see ITA KPIs.
4. From the Alarm Type drop-down menu, select **Absolute** and then select **>** from the Condition drop-down menu. For details, see Configuring Relative and Absolute Alarms.
5. In the Threshold field, enter **50** to set a 50% threshold for Link Utilization Downlink.
6. From the Dimension drop-down menu, select **Link;** then select All or Choose a specific element.
7. Click **Save** in the Condition and Assignment Editor to save the condition and close the window.

8. Click the **Add** button again to add a new condition, and repeat the previous steps, this time selecting **Link Utilization Uplink** in step 1.
9. Click **Save** to add the new policies to the Policy List pane.

Create a Link Policy Using the Link Template

1. Click the **Policies** tab, click **Add**, and then select **ITA** at the prompt, to add a new ITA policy.
2. Enter a name and brief description and then select the template you just created.
3. Click the **Enabled** check box and click **Save**. The new policy appears in the Policy List pane.

Assign Other Dimensions to the Link Policy

1. Select the new Link policy in the Policy List pane to view its details in the Policy Details pane.
2. In the **Assignments** area, two areas appear, one for each KPI threshold you had previously set.
3. In the Link Utilization Downlink area, select **Choose** and then select the target links in your group. The default is All links.
4. From the Other Dimensions pull-down menu, select **VLAN**. The All option is selected by default.
5. Repeat steps 3-4 in the Link Utilization Uplink area.
6. Click **Save** to save the changes to your new Link Utilization policy.

Follow-up Tasks

- In the Alarm dashboard, monitor for new alarms caused by excess link utilization.
- To filter on the newly created policy, enter the policy name in the Policy Filter, which is one of the Alarm filters in the Global Filter.

Creating an IPI Network Service Policy

This use case illustrates how to create an IPI alarm policy using values defined in Policy and Action templates.

Prerequisites

- Before you can assign an Email action to a policy, an outbound email server needs to be already configured.

To Create a Policy

1. Hover over the **Alarms** button on the IrisView toolbar and then select **Policy Management** from the submenu to access the dashboard.
2. Click the **Policies** tab and then click the **Add** button in the Policy List pane. At the prompt, select **IPI** as the application and then click **OK**. A blank form appears in the Policy Details pane.
3. Enter a name for the new policy and, optionally, a brief description.
4. Select the severity: Informational, Minor, Major, or Critical.
5. Change the aggregation window and a sample interval, as needed.
6. Select the **Service** option to indicate the type of IPI alarm, and then select from a list of predefined IPI network services.
7. In the Conditions area, click the **Add** button near the bottom to open the Condition and Assignment Editor.

8. Select the KPI category for this policy: **Accessibility**, **Others**, **Performance**, or **Retainability**.
9. Select a **KPI/KQI**, a **Dimension**, an **Alarm Type**, and a **Condition** (logical operator). For more details, see IPI KPIs and Configuring Relative and Absolute Alarms.
10. For a relative alarm, select from **Average over** the number of periods to use for calculating an average. If you select 1 period, no averaging will take place.
11. In the **Trigger Threshold** field, enter a threshold value for triggering the alarm.
12. For Volume KPIs, there is an additional Trigger field, **Minimum Samples**, where you can enter the minimum number of samples required before triggering the alarm.
13. If you selected the **Auto Clear** check box in the Policy Details, you can also enter in the **Clear** fields a threshold for autoclearing the alarm and the minimum number of samples required before automatically clearing the alarm.
14. Click the **Save** button to save the configuration and return to the Policy tab.
15. To add more conditions, click **Add** and repeat these steps to add as many conditions as needed.
16. In the Actions area, select one or more available Action templates for this policy.
17. In the Schedules area, select one or more available Schedule templates for this policy.
18. Click **Save** in the Policy Details pane to save the policy. Once you save, the new policy is added to the Policy List pane.
19. Click the **Enabled** check box to enable the policy.

To Create an Action Template

1. Click the Action Templates tab to display the Action Templates window, and then click **Add**. A blank form appears in the Action Template Details pane.
2. Enter a name for the Action.
3. From the Action Type drop-down menu, select **Email** or **SNMP**.
4. Enter parameters for the action and then click **Save**. The action template is added to the Action Template List.

Follow-Up Tasks

- Hover the cursor over the Alarms button and select **Alarm Dashboard** from the submenu to display the Alarm Browser, which lists all the alarms triggered in the last 180 days.
- Use the Global Filter and alarm dashlets to find any IPI alarms triggered by threshold violations for your policy. It may take a few minutes to see the alarms.
- Monitor the alarms in the Alarm Browser.

Creating a Low Data Volume Alarm Policy

This use case illustrates how you can create an LDV alarm policy to trigger an alarm when certain elements or network dimensions (such as HVAs, VLANs, URLs, and APNs) have sent low or zero traffic during a certain time period.

LDV alarms are useful to detect faults in network elements when equipment is down or locked up in a “silent mode” and not sending any messaging. Both IPI and ITA support LDV alarms.

Background

You want to generate an alarm if specific GGSNs experience LDV. The average traffic of the server is 50-70 calls per minute at its very lowest, and the volume should never be 0 over a 15 minute period. You can use the Iris Policy Management to configure a policy and then apply it to specific GGSNs. The Alarm dashboard provides a snapshot of all threshold violations, as well as any system-level alarms raised.

To Set Up an Alarm for LDV

1. To access the Alarms Policy page, click **Alarms** in the IrisView toolbar and select **Policy Management** from the submenu. The Policy Management dashboard appears, displaying the Policies tab.
2. Click the **Policies** tab to display the Policy List pane.
3. Click **Add** and select **IPI** at the prompt to display a blank form in the Policy Details pane.
4. Enter a name and optional description for the new policy.
5. Perform one of the following to indicate the type of IPI alarm:
   - Select the **Service** option, and then select from a list of predefined IPI network services.
   - Select the **Interface** option, and then select from a list of predefined interfaces.
6. Select the severity: Critical, Major, Minor, or Informational.
7. Change the aggregation window and a sample interval, as needed. For this example, you could choose an aggregation window of 15 minutes with a sample interval of 5 minutes.

Configure Policy KPI Conditions

1. In the Policy Details Pane Conditions area, click the **Add** button to open the Condition and Assignment Editor window.
2. Select the KPI category for this policy: **Accessibility**, **Others**, **Performance**, or **Retainability**.
3. Select an appropriate KPI/KQI from the drop-down menu. For details, see IPI KPIs.
4. From the Alarm Type drop-down menu, select **Low Data Volume** and then select **<** from the Condition drop-down menu. For details, see Configuring Relative and Absolute Alarms.
5. In the **Trigger Threshold** field, enter a threshold value for triggering the alarm. For this example you could enter 50 to trigger an alarm if the data volume was less than 50.
6. From the Dimension drop-down menu, select **GGSN**.
7. Click **Save** in the Condition and Assignment Editor window to save the condition and close the dialog box.
8. Click **Save** to add the new policy to the Policy List pane.

Assign GGSNs to the Policy

1. Select the new LDV policy in the Policy List pane to view its details in the Policy Details pane.
2. In the **Assignments** area, an area appears for each KPI threshold you had previously set.
3. In the **Select GGSN** area, select **Choose** and then select the GGSNs you want to assign to this LDV alarm.
4. Click **Save** to save the changes to your new Link Utilization policy.

Follow-up Tasks

- In the Alarm dashboard, monitor for new alarms caused by LDV.
- To filter on the newly created policy, enter the policy name in the Policy Filter, which is one of the Alarm filters in the Global Filter.

Analyzing ITA Critical Alarms Using the Alarm Dashboard

The Alarm Browser dashlet provides a default view of the state of all monitored elements with associated alarms. The system generates alarms when monitored elements exceed a set policy threshold. You can view alarm results by severity in a Pie chart and a Bar chart provided in the Alarm Dashboard.

Prerequisites

- ITA alarm policies with Critical severity need to be configured in Policy Management.
- There must be some Critical ITA alarms in the system, triggered when user-defined thresholds for ITA were breached.

To Analyze Critical Alarms Using the Alarm Dashboard

1. To access the Alarm Browser, hover over the **Alarms** button on the IrisView toolbar and then select **Alarm Dashboard** from the submenu. The Alarm Dashboard appears displaying the Alarm Browser and two dashlets.
2. Click the Show/Hide **Global Filter** button at the top right of the window next to the scroll bar to display the Global Filter pane.
3. In the Global Filter pane, click the **Automatic Refresh** check box to clear it and then set a specific time window in the Time Filter area. It cannot be more than 180 days. Then click **Apply**.
4. In the Alarm Filters area, select **Critical** from the Severity drop-down menu and then select **ITA** from the Application drop-down menu. You can also click the Critical alarms pie area in the Alarm Distribution by Severity dashlet.
5. From the Cleared and Acknowledged drop-down menus, select **All** and click **Apply**. All ITA Critical alarms, regardless of status, are now listed in the Alarm Browser and displayed in the other two dashlet.
6. To examine specific alarms in a narrower time window, in the Global Filter change the start and end dates and click **Apply** to view a different time window. You can only view alarms in the past 180 days.
7. To narrow down the number of alarms in the browser, complete one or both of the following tasks and click **Apply**:
   - Enter a policy name for a policy with a critical severity. The policy names are listed in the Policies tab view in the Policy Management dashboard.
   - Enter keywords from the policy description in the Description field. The policy descriptions are also listed in the Policies tab view.
8. In the Alarm Browser, click the Expand button **(+)** in the first column to view detailed information about the alarm, such as the time when it was first triggered and alarm description.

Follow-up Tasks

- If the alarm has a Drill link at the bottom of the row, click on **Drill** to launch ITA.
- Examine traffic data in the corresponding KPI dashlet.

Creating an IPI Policy Based on Response Codes

This use case illustrates how you can set up an IPI policy to generate alarms based on specific response codes. This type of alarm is used to proactively notify you about certain network errors. Configuration of policy conditions based on response codes is only applicable to interface based policies.

Alarms generated for response codes appear in the Alarms Dashboard and contain links to drill to the Cause Code Analysis (CCA) Dashboard in IPI for further analysis. Emails generated for response code alarms also contain links to drill to the CCA Dashboard.

To Create a Policy

1. Hover over the **Alarms** button on the IrisView toolbar and then select **Policy Management** from the submenu to access the dashboard.
2. Click the **Policies** tab and then click the **Add** button in the Policy List pane. At the prompt, select **IPI** as the application and then click **OK**. A blank form appears in the Policy Details pane.
3. Enter a name for the new policy and, optionally, a brief description.
4. Select the severity: Informational, Minor, Major, or Critical.
5. Change the aggregation window and sample interval, as needed.
6. In the **Policy Type** drop-down menu, select **Interface**.
7. In **Interface** drop-down menu, select the interface for the alarm.
8. In the Conditions area, click the **Add** button near the bottom to open the Condition and Assignment Editor.

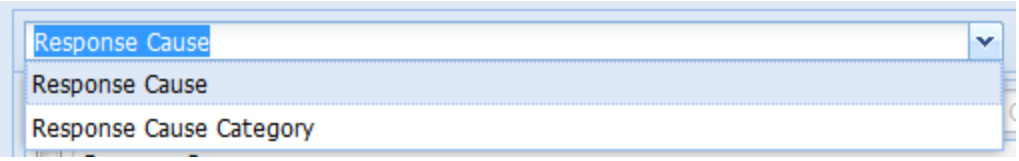
To Create Response Code Conditions

1. Open the Condition and Assignment Editor for the policy.
2. Select **Response Code** as the KPI category for this policy.
3. Select one of the following KPI/KQIs:
   - Number of Occurrences
   - Percent Occurrence of All Cause Codes
   - Percent Occurrence of Failure Cause Codes
   - Percent Occurrence of Success Cause Codes
   - Percent Occurrence of Timeout Cause Codes
4. Select an **Alarm Type** and a **Condition** (logical operator). For more details, see IPI KPIs and Configuring Relative and Absolute Alarms.

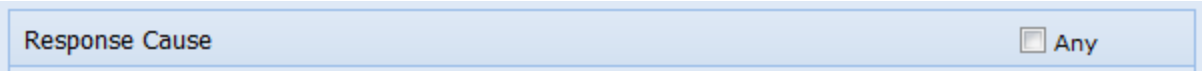
   Note: Only absolute and relative alarm types are supported for alarms based on response code.
5. For a relative alarm, select from **Average over** the number of periods to use for calculating an average. If you select 1 period, no averaging will take place.
6. In the **Trigger Threshold** field, enter a threshold value for triggering the alarm.
7. For Volume KPIs, there is an additional Trigger field, **Minimum Samples**, where you can enter the minimum number of samples required before triggering the alarm.
8. If you selected the **Auto Clear** check box in the Policy Details, you can also enter in the **Clear** fields a threshold for autoclearing the alarm and the minimum number of samples required before automatically clearing the alarm.

To Create Response Code Policy KPI Dimensions

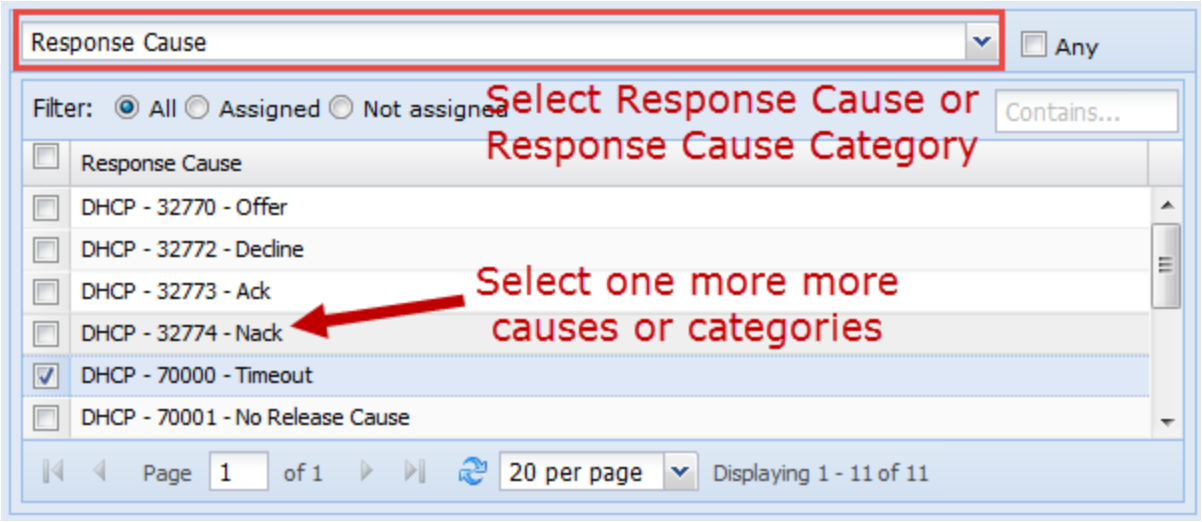
1. In the Dimensions area of the Condition and Assignment Editor, select a protocol, procedure, and optionally an attribute for the dimension.
2. Select an Response Code procedure for the dimension.
3. Select the Reponse Causes or Response Cause Categories that should apply for this policy.
   - If the KPI/KQI for this policy is either Number of Occurrences or Percent Occurrences for All Cause Codes, you can select either Response Cause or Response Cause Category.



- If the KPI/KQI is Percent Occurrence of Failure, Success, or Timeout cause codes, then only Response Cause is available.



4. Select one or more individual response causes or categories that apply for the policy.



5. Select the dimensions and elements within each dimension (if required).
6. Add more dimensions as necessary.
7. Click **Ok** to save the condition. The details of the condition appear in the Condition and Assignments Details area in the Policy Details pane.
8. You can add more than one condition. Conditions can have an "or" or "and" relationship. The default relationship is "or."

Follow-Up Tasks

- Hover the cursor over the Alarms button and select Alarm Dashboard from the submenu to display the Alarm Browser, which lists all the alarms triggered in the last 180 days.
- Use the Global Filter and alarm dashlets to find any IPI alarms triggered by threshold violations for your policy. It may take a few minutes to see the alarms.
- Expand the alarm to view details about it. Click the link to drill to the Cause Code Analysis Dashboard in IPI.

Alarms User Interface

The Alarms GUI enables you to configure alarm policies and monitor alarms. You open the Alarms main window when you click the Alarms button in the IrisView toolbar.

Alarms Toolbar

Policy Management Option	Open the Policy Management dashboard to configure alarm policies for supported Iris applications.
Alarm Dashboard Option	Open the Alarm Dashboard to monitor supported alarms.

Policy Management Dashboard

Policies Tab	Create new policies, define severity, interface, conditions, and KPIs, assign them dimensions and actions, and then enable the policies.
Action Templates Tab	Create templates that define the action to take when a threshold is breached: send email, notify ACE, and send notifications through SNMP.
Schedule Templates Tab	Create templates that define specific time frames when alarm policies and alarm profiles generate alarms.
Profiles Tab	Create alarm profiles to which you can assign alarm policies, schedules, actions, and users.
Users to Profiles Tab	View users and their assigned profiles, and modify profile assignments per user.
System Alarms Tab	Configure severity, thresholds, and SNMP details for G10 system-level alarms.

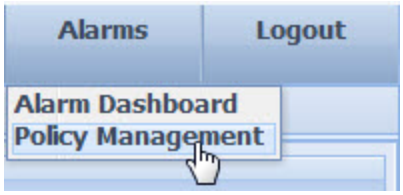
Policy Management Dialog Boxes

Import Policy Data Dialog Box	Import alarm policy configurations contained in an XML file.
Condition and Assignment Editor	Create or edit alarm conditions for a policy.

Alarm Dashboard

Alarm Browser	Click the Alarm Dashboard tab to display these dashlets: • Alarm Browser • Alarms by Severity (bar chart) • Alarm Distribution by Severity (pie chart)
Alarm Distribution by Severity Dashlet	
Alarm Distribution Dashlet	
Global Filter Pane	Click the Global Filter button to show or hide the Global Filter pane.
Time Slider Window	Time Slider window appears near the bottom of the Alarm Dashboard.

Alarm and Policy Management Dashboards

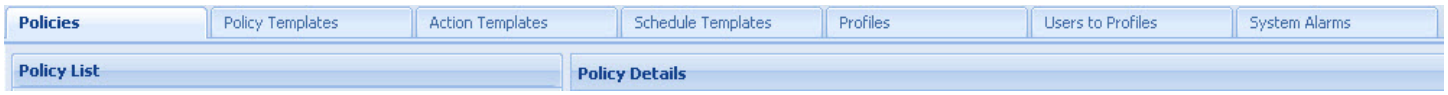


Alarm Dashboard	Monitor supported alarms in the Alarms browser and analyze data in alarm distribution dashlets.
Policy Management	Configure alarm policies using policy and action templates.

Alarm Dashboard

Refresh Button	Manually refresh the data displayed in the Alarm dashboard. You can also set an Automatic Refresh in the Time Filter area of the Global Filter. ⚠ Do not use the Refresh button provided in your Internet browser, as this will cause all your pages to reload and discard any changes you have not saved.
Save Button	Save the content of the Alarm dashboard in graphical form to a PDF file. The Alarm Browser and the two alarm distribution dashlets also include this button.

Policy Management Dashboard



Policies Tab	Create new policies, define severity, interface, conditions, and KPIs, assign them dimensions and actions, and then enable the policies.
Action Templates Tab	Create templates that define the action to take when a threshold is breached: send email, notify ACE, and send notifications through SNMP.
Schedule Templates Tab	Create templates that define specific time frames when alarm policies and alarm profiles generate alarms.
Profiles Tab	Create alarm profiles to which you can assign alarm policies, schedules, actions, and users.
Users to Profiles Tab	View users and their assigned profiles, and modify profile assignments per user.
System Alarms Tab	Configure severity, thresholds, and SNMP details for G10 system-level alarms.

Alarm Dashboard

You can use the Alarm Dashboard to monitor Iris application and system-level alarms. You access this window by clicking the Alarm button and then selecting Alarm Dashboard from the submenu.

Alarm Browser	Contains a table listing all supported Iris application and system-level alarms that have occurred in the last 180 days. You can drill down from some ITA alarms to the related ITA KPI dashlet and from IPI alarms to the related IPI KPI dashboard.
Alarm Distribution by Severity Dashlet	Contain pie chart and bar graph representations of the alarms raised during the time window you specified in the Global Filter pane or the Time Slider window.
Alarms by Severity Dashlet	
Global Filter pane	Contains a Time filter and an Alarms filter to control the information displayed in the dashlets and the Alarm Browser. The Time filter can be used in conjunction with the Time Slider window.
Time Slider Window	Grab and drag either handle with your mouse to change settings. The slider, near the bottom of the dashboard, enables you to add more granularity to your view of the Alarms by Severity dashlet and the Alarm Browser. This window is used in conjunction with the Global Time Filter.

Time Filter Values

Filter Type	Maximum	Comment
Global Time Filter	180 days	If the Global Time Filter is set for more than six hours, the Time Slider window is not visible.
Time Slider Window	6 hours	

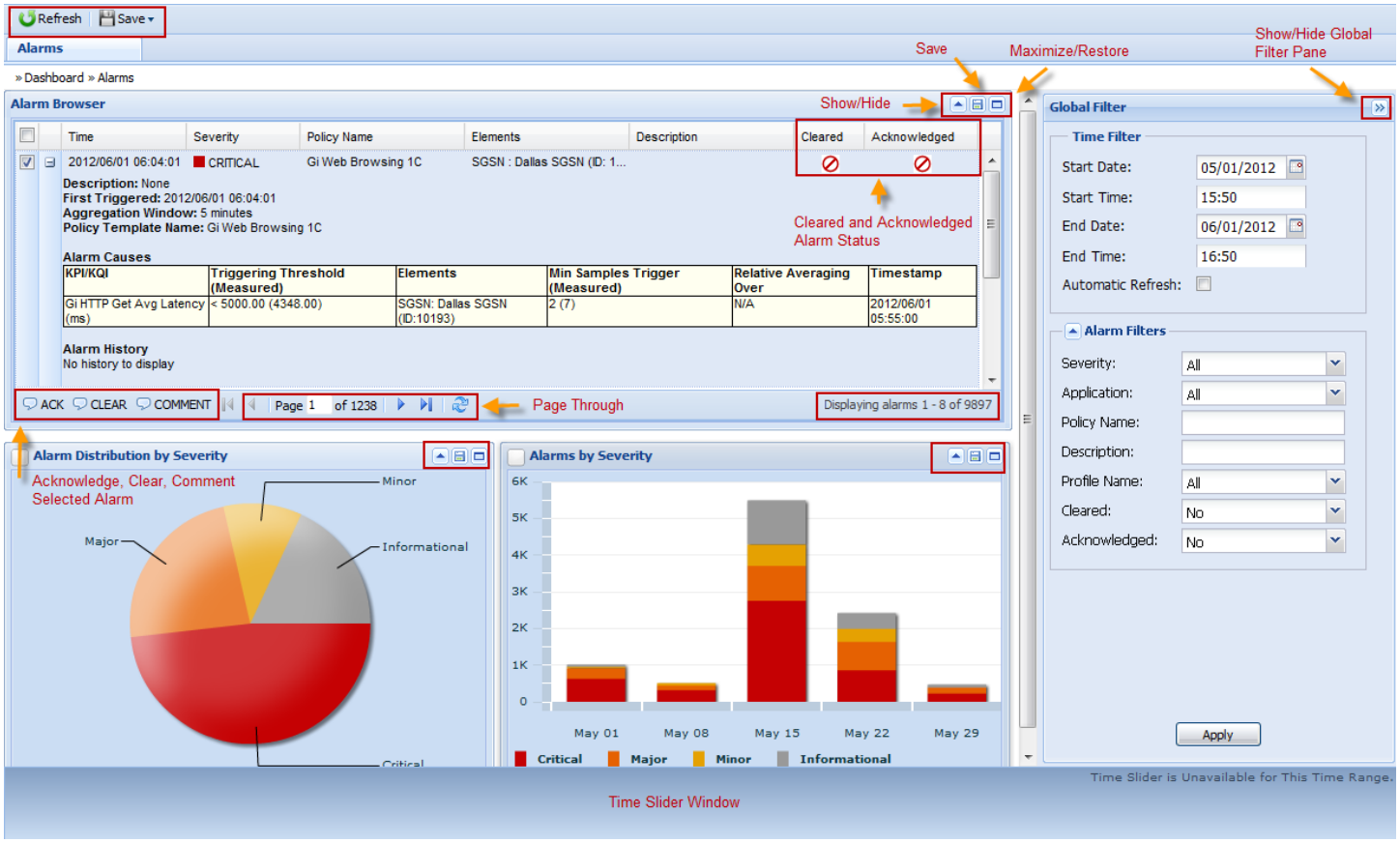
Common Pane Controls

Show / Hide Button	Hide or show the dashlet content below the toolbar. This button disappears when you maximize a dashlet.
Save Button	Save the content of the dashlet in graphical form to a PDF file. You can also save the content of all dashlets in the window using the Save button in the Alarm Dashboard toolbar.
Maximize / Restore Buttons	Maximize the dashlet to span the entire window; the Show/Hide button disappears. Click the Restore button to return the dashlet to its default form and location in the window.
Drag / Drop	Drag a dashlet to any location within the dashboard. Hover over the dashlet toolbar until the drag icon is visible, click and hold the left mouse button down while you move the dashlet to a different location, and then release the mouse button.
Hover Over	Hover your cursor over a pie piece or a bar to display details about the alarm: severity, count, and percentage as compared with other alarms of different severity.

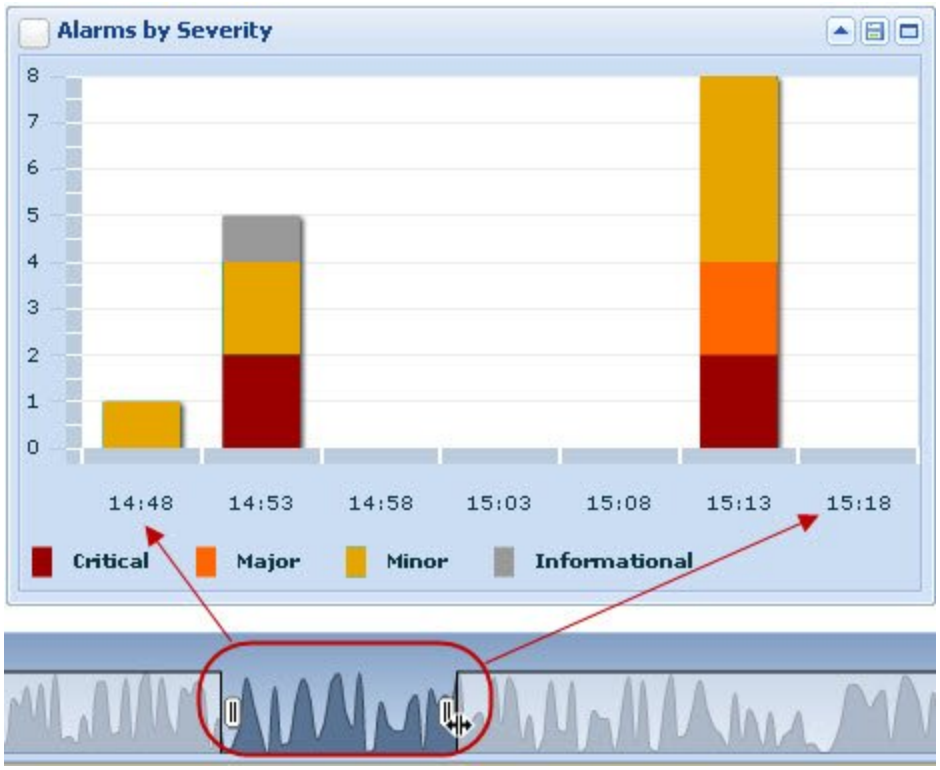
Alarm Dashboard Toolbar

Refresh Button	Manually refresh the data displayed in the Alarm dashboard. You can also set an Automatic Refresh in the Time Filter area of the Global Filter. ⚠ Do not use the Refresh button provided in your Internet browser, as this will cause all your pages to reload and discard any changes you have not saved.
Save Button	Save the content of the Alarm dashboard in graphical form to a PDF file. The Alarm Browser and the two alarm distribution dashlets also include this button.

Alarm Dashboard



Time Slider Window



Alarm Browser

You use the Alarm Browser to monitor supported Iris application alarms, as well as system-level alarms. You access this dashlet by hovering over the Alarms button in the IrisView toolbar and selecting Alarm Dashboard from the submenu.

Columns	• View system-level and user-defined alarms, status, and detailed description.
Column Filters	• Use filter controls to sort column data or show or hide the Policy Name, Elements, and Description columns.
ACK Button	• Click the ACK button to acknowledge one or more selected system-level or user-defined alarms. • To activate the ACK button you must select at least one unacknowledged alarm; you must have the Alarm Acknowledge privilege to view the button.
CLEAR Button	• Click on the CLEAR button to clear one or more selected system-level or user-defined alarms. • To activate the CLEAR button, you must select at least one uncleared alarm; you must have the Alarm Clearing privilege to view the button.
COMMENT Button	• Click on the COMMENT button to add a comment to selected system-level or user-defined alarms. • To activate the COMMENT button, you must select one or more alarms; you must have the Alarm Acknowledge privilege to view the button. • You can add comments to alarms that have the Cleared or Acknowledged status or that already have comments.
Paging	• If there are more alarms than can be displayed in one page of the browser, they appear in multiple pages. Paging controls are provided to navigate the data. • The Refresh button enables you to manually refresh the browser with the content of the database. • A total count of the alarms displayed in the current page and the overall number of alarms is shown in the bottom right corner.
Browser Toolbar	• The Alarm Browser toolbar enables you to hide the dashlet and redisplay it, maximize or restore it to its original size, and save its content to a PDF file.

Columns

Check Box Column	You must have the Alarm Clearing or Alarm Acknowledge privilege to view this column. Select the check box in the column heading field to select or deselect all alarms in the browser. Select a row check box to select the corresponding alarm for acknowledgment, clearing, or commenting. When you select or expand an alarm, the Automatic Refresh check box in the Time Filter is immediately cleared and a popup message indicates that automatic refresh is disabled; this action prevents the system from updating the data while you are working with an alarm.
Expand/Collapse Column	Contains individual expand (+) or collapse (-) buttons to view an expanded description for the alarm. When you select or expand an alarm, the Automatic Refresh check box in the Time Filter is immediately cleared and a popup message indicates that automatic refresh is disabled; this action prevents the system from updating the data while you are working with an alarm.
Time	The most recent time the alarm occurred.

Severity	Alarm severity: Critical, Major, Minor, or Informational.
Policy Name	For user-defined alarms, name of the policy associated with the alarm that was triggered. For system-level alarms, it shows a system-level alarm identifier; for more details, see the Iris Admin help.
Elements	For user-defined alarms, Iris application dimension that triggered the alarm. For system-level alarms, network, hardware, or software element that triggered the alarm.
Description	Description of impacted network element or service. When you click the Expand (+) button for that row, the description expands to reveal additional details.
Cleared	Contains an icon indicating whether the alarm has been cleared. When you clear an alarm using the CLEAR button or the alarm clears automatically, the icon in this column changes to a green check mark. For more details, see Iris Alarm Clearing.
Acknowledged	Contains an icon indicating whether the alarm has been acknowledged. When you acknowledge an alarm using the ACK button, the icon in this column changes to a green check mark. For more details, see Iris Alarm Acknowledgement..

Description Fields

Description Column	View brief description for the alarm: • For policy-based alarms, this column shows the data entered in the Description field in the Policies tab of the Policy Management dashboard. If the Description field is blank, the Description field in the Alarm Browser will also be blank. • For system-level alarms, this column shows the description that is configured in the system.
Expanded Description Area	The expanded description area is an expansion of the Description column and includes the following information: • The precise time when the alarm was triggered and the policy name appear at the top. No policy name is provided for system-level alarms. • The Alarm Causes table provides KPI and measurement information to analyze the causes. For system-level alarms, only the elements involved, such as probe and port, and the timestamp are provided. • The Alarm History table provides a timestamp of when an alarm was acknowledged and by whom, as well as any comments that were made. • The Alarm History table provides a timestamp of when an alarm was cleared and by whom, as well as any comments that were made.
Alarm Causes Table	
Alarm History Table	

Alarm Causes Table

KPI/KQI	For application-based alarms, name of the KPI or KQI that triggered the alarm. For system-level alarms, "System Alarm" is always shown.
Triggering Threshold (Measured)	Actual measurement of the value that triggered the alarm. N/A indicates that a measurement is not applicable. For relative alarms, the column shows the percentage or value of a previous day, week, 4 weeks, or period with which it was compared.

Elements	Network elements where the alarm was triggered. The Drill link is available for some ITA alarms and IPI alarms that are based on response codes. • For ITA alarms, click on the link to open ITA and view the related KPI dashlet. • For IPI alarms based on response codes, click on the link to open IPI and view the Cause Code Analysis dashboard. • For all other IPI alarms, click on the link to open IPI and view the IPI Proactive Element Analysis dashboard.
Min Samples Trigger (Measured)	Actual measurement of the minimum samples value that triggered the alarm. Minimum samples are only applicable for Volume KPIs. N/A indicates that this measurement is not applicable. For relative alarms, the column shows the percentage or value of a previous day, week, 4 weeks, or period with which it was compared.
Relative Averaging Over	For relative alarms, averaging is specified when a condition is created in order to calculate an average over n periods. This column shows the number of periods used in the averaging calculation, if specified.
Timestamp	The timestamp of the data that caused the alarm.

Alarm History Table

Timestamp	Indicates the date and time when an action was taken.: alarm clearing, acknowledgment, or just commenting.
Username	Identifies the user who cleared, acknowledged, or commented on the alarm. For system-level alarms, the username is SYSTEM.
Description	Describes the action that was taken: alarm clearing, acknowledgment, or just commenting. Plain comments, as well as comments made while clearing or acknowledging an alarm also appear in this column. For more details, see Iris Alarm Acknowledgement and Iris Alarm Clearing.

Column Filter Controls

You can only hide these columns: Policy Name, Elements, and Description.

Actions Menu	• To access the actions menu, hover your cursor over a column header until you see a down arrow and then click on it. • Apply a sort filter or select a column to show or hide.
Sort Ascending Button	• Sort table in ascending or descending order using the values in the selected column. • All numbers are sorted together first, then all upper case names are sorted together, and finally all lower case names are sorted together.
Sort Descending Button	
Columns Menu	• Select columns you want to show in the table and remove the checkmark from columns you want to hide. At least one column must remain visible.

Paging Controls

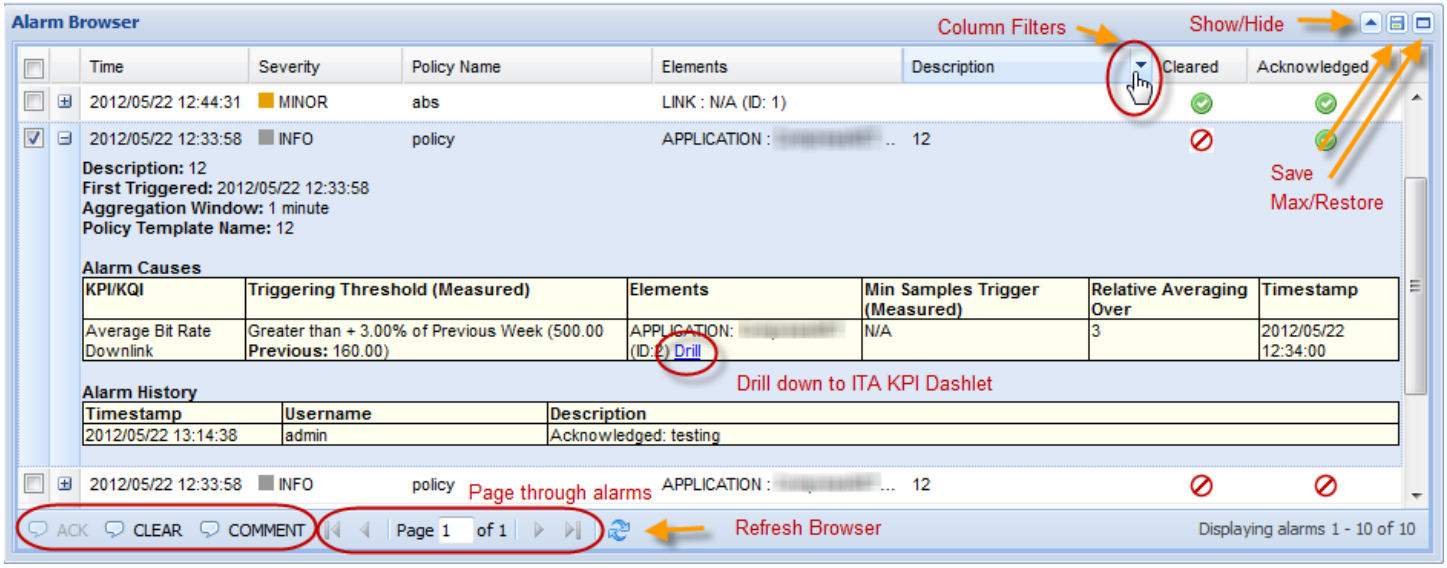
Last / Next Page Buttons	Navigate to view items in multiple pages.
First / Last Page Buttons	Go to the first or last page of data.
Page Count	View the page number and the total number of pages.

Refresh Button	Manually refresh the data displayed in the Alarm Browser. ⚠ Do not use the Refresh button provided in your Internet browser, as this will cause all your pages to reload and discard any changes you have not saved.

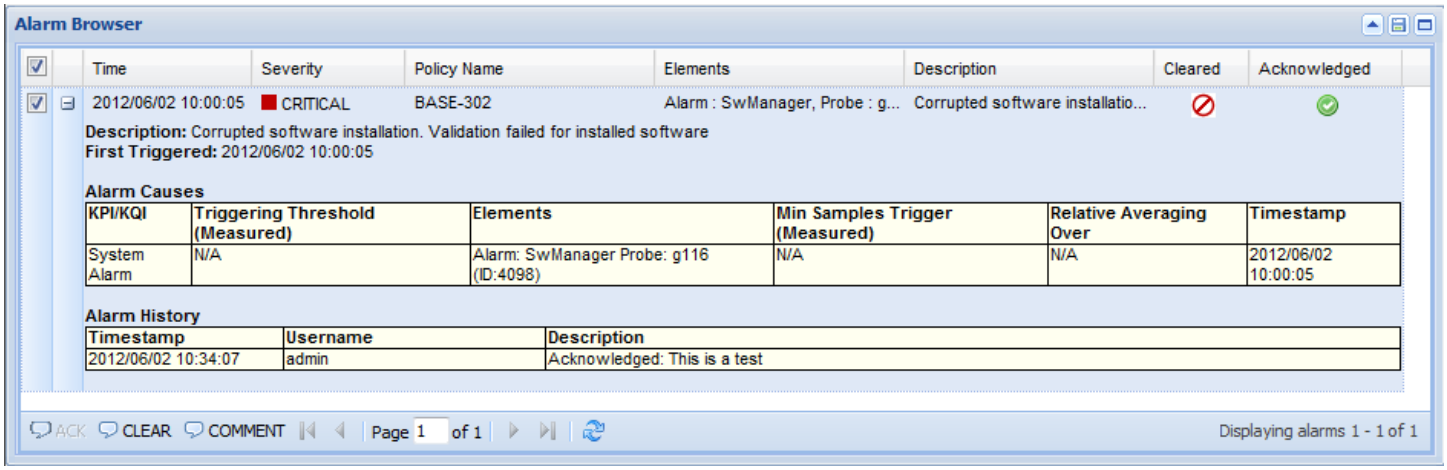
Dashlet Toolbar Controls

Show / Hide Button	Hide or show the dashlet content below the toolbar. This button disappears when you maximize a dashlet.
Save Button	Save the content of the dashlet in graphical form to a PDF file. You can also save the content of all dashlets in the window using the Save button in the Alarm Dashboard toolbar.
Maximize / Restore Buttons	Maximize the dashlet to span the entire window; the Show/Hide button disappears. Click the Restore button to return the dashlet to its default form and location in the window.
Drag / Drop	Drag a dashlet to any location within the dashboard. Hover over the dashlet toolbar until the drag icon is visible, click and hold the left mouse button down while you move the dashlet to a different location, and then release the mouse button.
Hover Over	Hover your cursor over a pie piece or a bar to display details about the alarm: severity, count, and percentage as compared with other alarms of different severity.

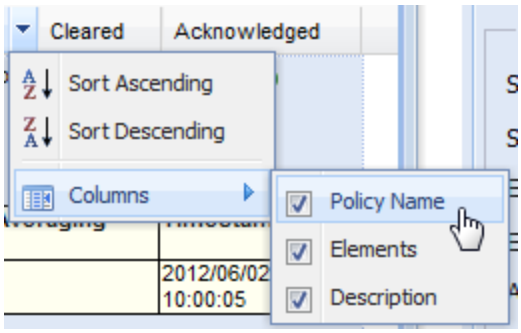
Alarm Browser (ITA Alarms)



Alarm Browser (System-Level Alarm)



Column Filter



Alarms by Severity Dashlets

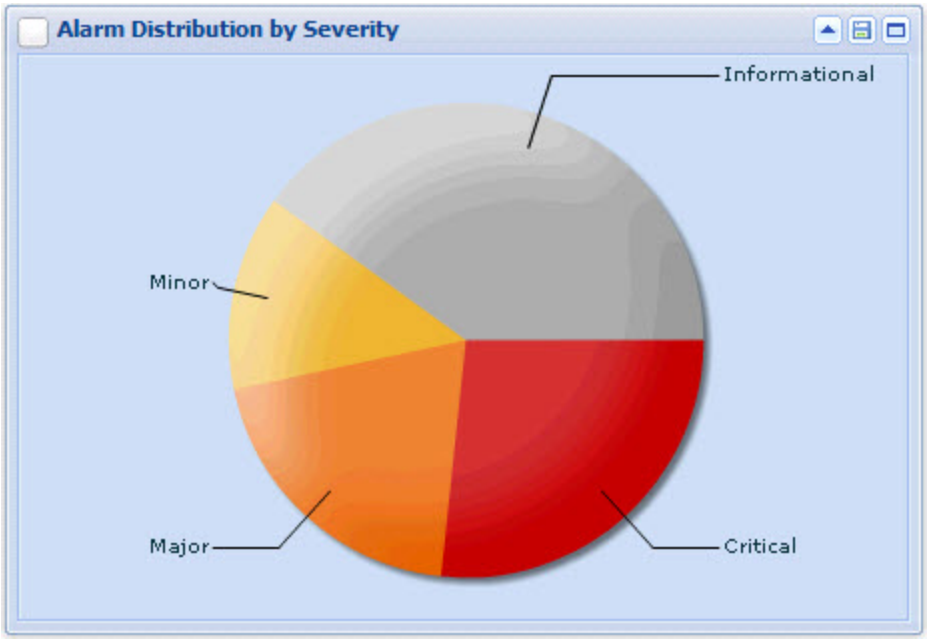
You use the Alarm Distribution by Severity and the Alarms by Severity dashlets to analyze the percentile distribution of alarms by severity. You access these dashlets by clicking the Alarms button in the IrisView toolbar and selecting Alarm Dashboard from the submenu.

Alarm Distribution by Severity Dashlet	A pie chart representation of all alarms that have been raised over the dates specified in the Time Filter. The pie chart is based on an aggregate percentile distribution of alarms by severity. You can click any slice in the pie, and the associated severity data immediately populates the Alarm browser, as well as the Alarms by Severity bar chart.
Alarms by Severity Dashlet	A bar chart representation of alarms over time series and volume. At each time interval, you can view graphically the relative volume of alarms in each severity type.
Alarm Severity	Severity types are Critical, Major, Minor, or Informational. You can choose to view only one severity type by changing the settings in the Alarms filter area of the Global Filter pane.
Alarms Color Coding	Each severity type is associated with a specific color, as shown in the Alarms by Severity pane: Critical = Red; Major = Orange; Minor = Green; Informational = Gray.
Time Axis	You can change the time window for the bar and pie charts by adjusting the handle bars in the Time Slider window or by applying a new time filter in the Global Filter pane.

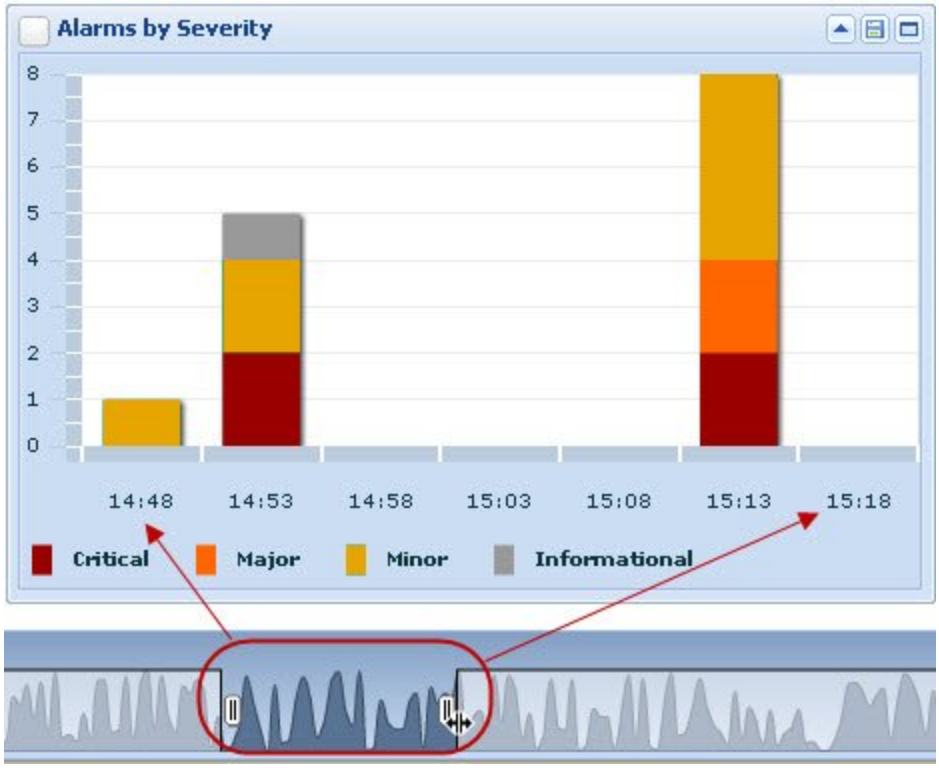
Dashlet Toolbar Controls

Show / Hide Button	Hide or show the dashlet content below the toolbar. This button disappears when you maximize a dashlet.
Save Button	Save the content of the dashlet in graphical form to a PDF file. You can also save the content of all dashlets in the window using the Save button in the Alarm Dashboard toolbar.
Maximize / Restore Buttons	Maximize the dashlet to span the entire window; the Show/Hide button disappears. Click the Restore button to return the dashlet to its default form and location in the window.
Drag / Drop	Drag a dashlet to any location within the dashboard. Hover over the dashlet toolbar until the drag icon is visible, click and hold the left mouse button down while you move the dashlet to a different location, and then release the mouse button.
Hover Over	Hover your cursor over a pie piece or a bar to display details about the alarm: severity, count, and percentage as compared with other alarms of different severity.

Alarm Distribution by Severity



Alarms by Severity and Time Slider



Alarms Global Filter

The Global Filter enables you to define and apply a filter anywhere in the Alarm dashboard. You access the Global Filter by clicking the Alarms button in the IrisView toolbar, selecting Alarm Dashboard from the submenu, and then clicking the Show/Hide button on the right edge of the window. After applying the global filter criteria, only those alarms matching the criteria will appear in the Alarm dashboard.

Time Filter Area	Enter the filter start and end dates and time. These settings affect the Time Slider window settings.The time range filter can be applied to either the first triggered time or the last updated time of an alarm.
Alarm Filters Area	Select different filter criteria such as severity, application where the alarm was triggered, and alarm status.
Drill Filter Area	This area is only visible when you drill down from IrisView Network Maps. In this case, the Alarm dashboard only displays information about the alarms you selected for drilling down. This area enables you to remove that filter and view all alarms in the system that match the filter criteria.
Show / Hide Global Filter Button	Toggle between showing or hiding the Global Filter. The button is located on the top right edge of the window.
Apply Button	Apply the filters defined in this pane to the data displayed in the window.

Time Filter Area

Filter by: Drop Down menu	Select either First Triggered or Last Updated alarms to filter by. For example, you can use the first triggered time to investigate the data that contributed to the firing of an alarm (such as comparing against an IPI dashlet versus analysis). Use the last updated time filter to monitor the last activity on an alarm, such as an acknowledgment.
Start / End Date Field Calendar Button Start / End Time Field	• Enter the filter Start or End Date by changing the value in the field or by selecting it from a calendar. • To open the calendar, click the **Calendar** button and then click the Start or End Date. • Enter the filter Start or End Time in hours and minutes, using an HH:MM format, where HH is 00-23 and MM is 00-59. • You can set the End Date and Time up to 1 day in the future and up to 180 days in the past. This is equivalent to setting automatic refresh on. • These settings can be used in conjunction with the Time Slider window.
Automatic Refresh Check Box	• Set system to automatically refresh the data every minute. You can also do a manual refresh using the Refresh button in the toolbar. • As long as this check box is selected, you cannot edit the other Time Filter settings. • When you expand or select an alarm in the Alarm Browser, the check box is automatically cleared and refresh is disabled. This action prevents the system from updating the data while you are examining an alarm, trying to clear or acknowledge an alarm, or adding a comment.  Do not use the Refresh button provided in your Internet browser, as this will cause all your pages to reload and discard any changes you have not saved.

Time Filter Values

Filter Type	Maximum	Comment
Global Time Filter	180 days	If the Global Time Filter is set for more than six hours, the Time Slider window is not visible.
Time Slider Window	6 hours	

Alarm Filters Area

Select or enter a combination of filter criteria to use with or without a time filter.

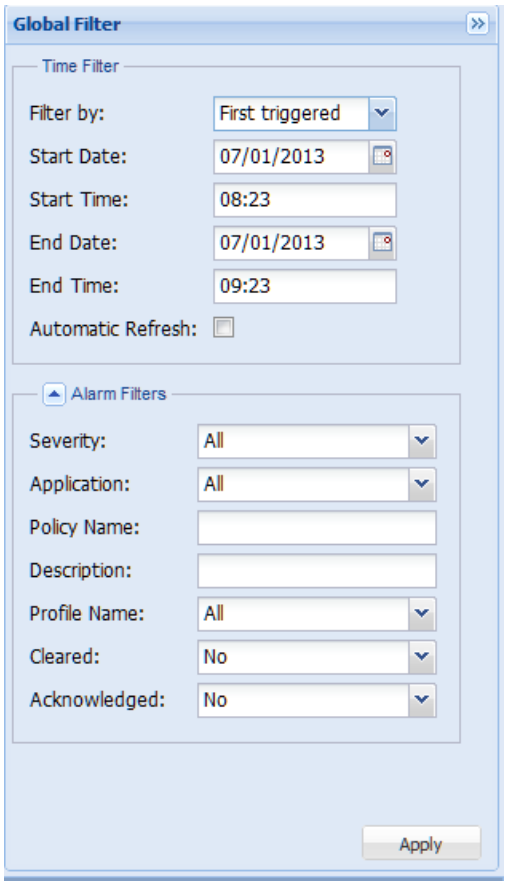
Severity	Select an alarm severity as a filter: Critical, Major, Minor, and Informational alarms or select All to pass all alarms. The default is All. If you drill down from an alarm severity column in Network Maps, this field shows the severity you used for drilling down.
Application	Select one of the following options: • ALL to view all alarm types (ACE, IPI, KPI Studio, ITA applications; GEO; and SYSALARM). This is the default view. • ACE, IPI, KPI Studio, or ITA to view alarms supported by a specific Iris application • GEO to view alarms generated in the GeoProbe system • SYSALARM to view system-level alarms
Policy Name	Enter the full or partial name of one or more policies that are defined in the Policy Management dashboard to use as filters. You can also enter the full or partial name of a system-level alarm.

Description	Enter a string of text in the policy description to use as a filter criteria.
Profile Name	Select the name of a profile to use as a filter. You can select only those profiles that you have been assigned, and the Default profile.
Cleared	Select All to view all cleared alarms, Yes to view only cleared alarms, or No to view only alarms that have not been cleared. When you click the Apply button only alarm data that fits this criteria appears in the Alarm Dashboard dashlets and browser. For more details, see Iris Alarm Clearing.
Acknowledged	Select All to view all acknowledged alarms, Yes to view only acknowledged alarms, or No to view only alarms that have not been acknowledged. When you click the Apply button only alarm data that fits this criteria appears in the Alarm Dashboard dashlets and browser. For more details, see Iris Alarm Acknowledgement.

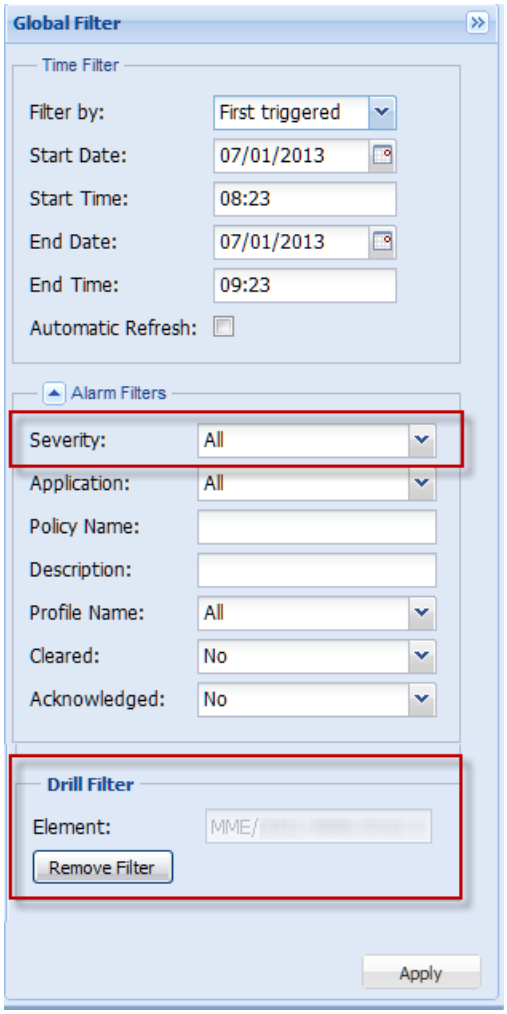
Drill Filter Area

Element Field	View the name of the network element that was used for drilling down.
Remove Filter Button	Clicking this button removes the Drill Filter area and the element filter. Although the Time filter and Alarm filter settings remain the same, the dashboard now displays all alarms in the system that match the filter criteria.

Alarms Global Filter



Alarms Global Filter - After Drilling Down from IrisView Network Maps



Policy Management Dashboard

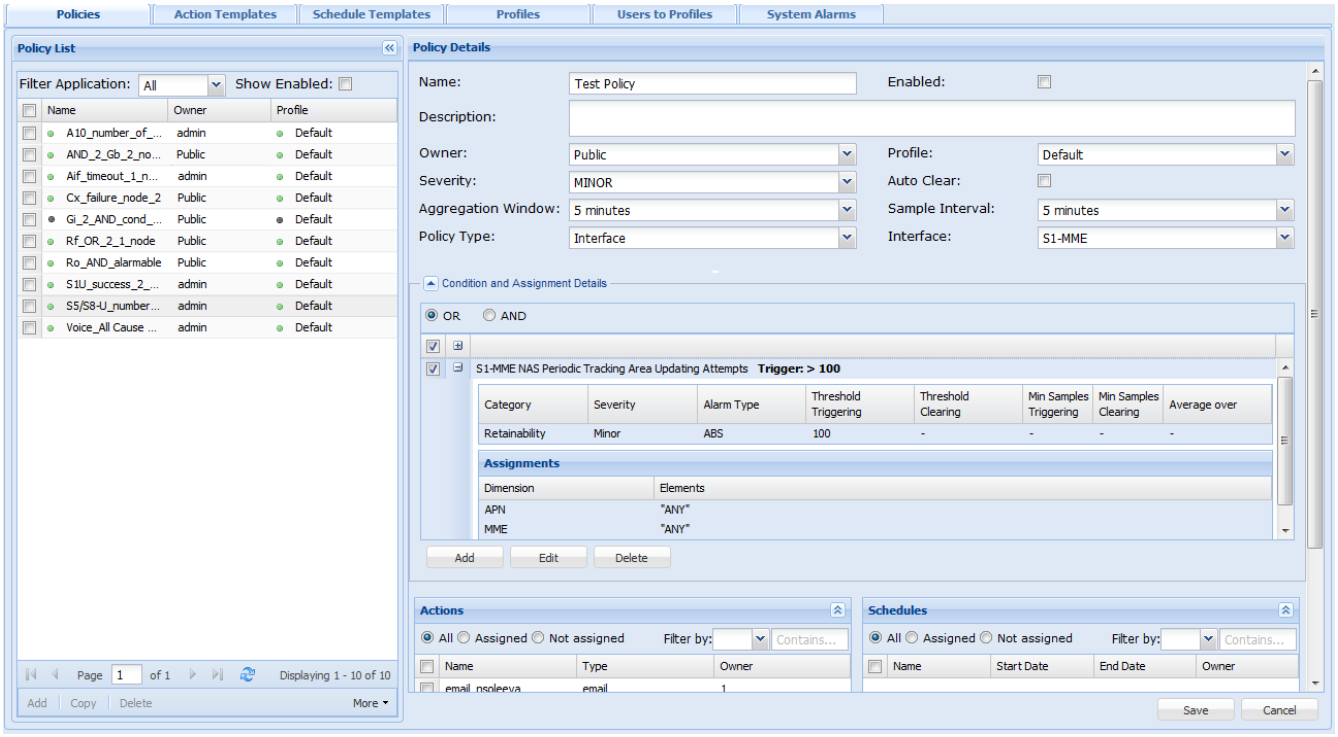
The Policy Management dashboard enables you to create and manage alarm policies for supported Iris applications. You access this dashboard by clicking the Alarms button in the IrisView toolbar and selecting Policy Management from the submenu.

List Pane Details Pane Policy Management Tabs	The Policy Management dashboard has the following components: • Each Policy Management tab view consists of a List pane and a Details pane. • The List pane lists the policies or templates configured in the system for the corresponding tab view and enables you to add, delete, or copy any item you select in the List pane. • The Details pane enables you to configure the properties of any policy or template you select in the List pane.
List Column Filters	Sort the table in the List pane by column data or hide columns from view.

Policy Management Tabs

Policies Tab	Create new policies, define severity, interface, conditions, and KPIs, assign them dimensions and actions, and then enable the policies.
Action Templates Tab	Create templates that define the action to take when a threshold is breached: send email, notify ACE, and send notifications through SNMP.
Schedule Templates Tab	Create templates that define specific time frames when alarm policies and alarm profiles generate alarms.
Profiles Tab	Create alarm profiles to which you can assign alarm policies, schedules, actions, and users.
Users to Profiles Tab	View users and their assigned profiles, and modify profile assignments per user.
System Alarms Tab	Configure severity, thresholds, and SNMP details for G10 system-level alarms.

Policy Management - IPI Example



Policies Tab

The Policies tab view is the main Policy Management window. It enables you to create and manage policies for model-driven applications, such as IPI, ITA, and KPI Studio, using Action, and Schedule templates. The Policies tab consists of a Policy List pane and a Policy Details pane. You can access this tab when you select Alarms in the IrisView toolbar and then click Policy Management in the Alarms toolbar.

Policy List Pane	Lists all the alarm policies you have created for a supported Iris application and the profile to which each policy has been assigned. You can add new policies, delete policies, or copy an existing policy and modify it to create a new policy. When you select a policy in the list, its properties are shown in the Details pane. Each policy name and profile name has an icon to indicate whether it is enabled (green) or disabled (gray).
Policy Details Pane	Shows policy details for the policy you select in the List pane. You can configure policy properties in this pane.

Policy List Pane

Low Data Alarms Enable/Disable Button	Enable or disable all Low Data Volume alarm policies. See Configuring a Low Data Volume Policy Use Case for details. You can disable LDV alarms during times of planned maintenance or if network elements become unavailable. LDV alarms are not supported for KPI Studio.
Filter Application Drop-Down Menu	Select to display in the Policy List pane All policies or only the policies for a supported Iris application.
Show Enabled Check Box	Select to display in the list only policies that have Enabled status.
Add Button	• Open the Select Application dialog box, where you can select from a list of supported Iris applications. • When you click **OK**, a blank form appears in the Policy Details pane.
Copy Button	• Select the check box next to an item on the list and then click **Copy** to generate a copy of an existing item, so you can modify it to create a new one. • When you click **Copy**, `Copy of...` is added in to the front of the item's name, which is displayed in the Details pane. • You can then change the information as needed and click the **Save** button in the Details pane.
Delete Button	• Select the check box next to an item on the list and then click **Delete** to remove the item from the list and from the system.
More Options	• Enable/Disable - Select the checkbox next to one or more items on the list and then select Enable or Disable to change the status of the selected profile(s). • Export Option - Export all policies, action templates, schedule templates, and profiles to an XML file. All policy configurations are exported. This option is available only for users with the Application Alarm Admin privilege. For users with the Application Alarm Configuration privilege, the Export option is disabled. • Import Option - Open the Import Policies dialog box, where you can browse for policy configuration files to import and indicate whether you want to overwrite or synchronize the imported data. The import file includes policies, action templates, schedule templates, and profiles. This option is available only for users with the Application Alarm Admin privilege. For users with the Application Alarm Configuration privilege, the Import option is disabled. • Show XSD Option - Displays the content of the XML schema file, alarm_policies.xsd, within your default Internet browser. This option is available only for users with the Application Alarm Admin privilege. For users with the Application Alarm Configuration privilege, the Show XSD option is disabled.

Policy Details Pane

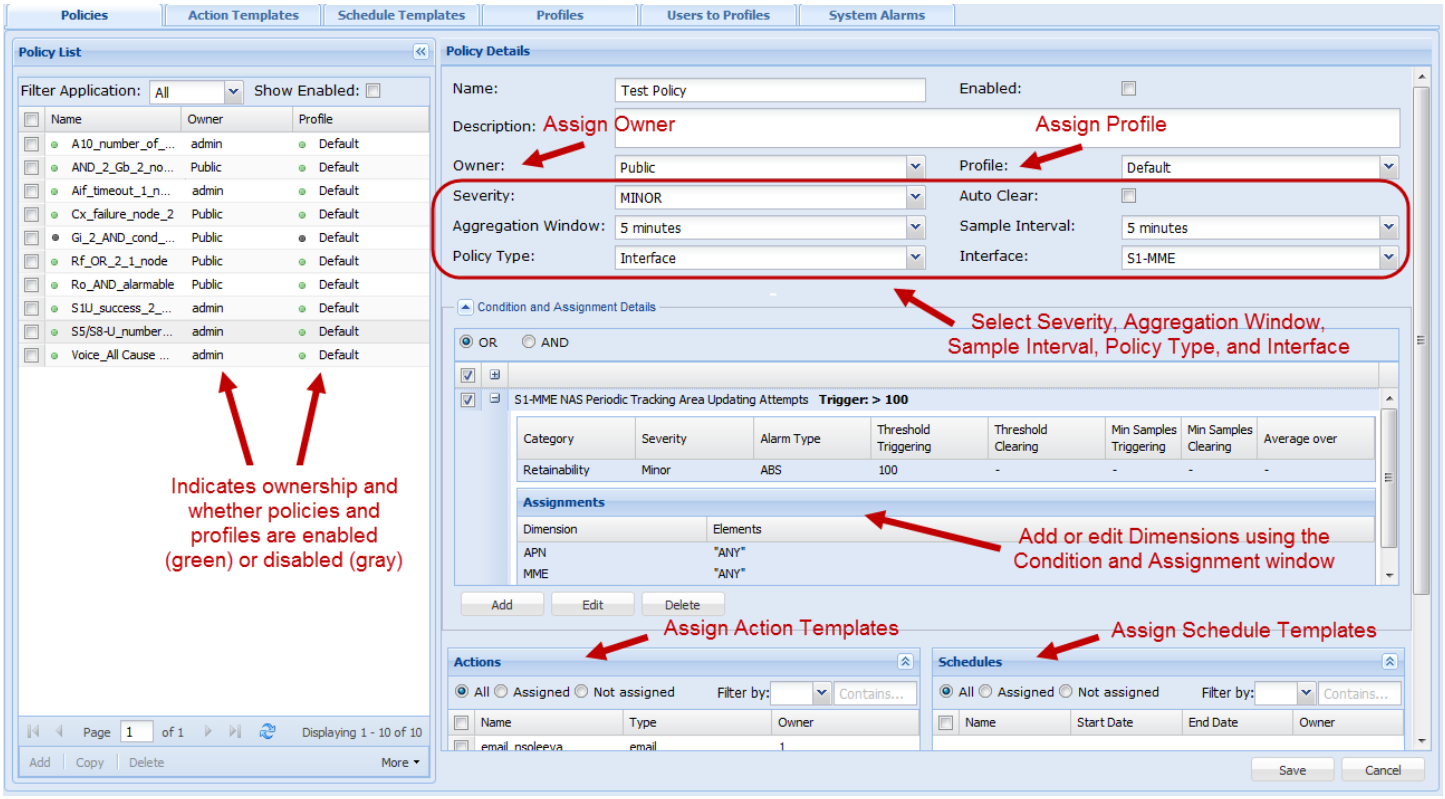
Name Field Description Field	• Enter a name and brief description for the policy. • In the Alarm dashboard, you can filter on policy names and description keywords using the Global Filter Advanced Filters. • The Description field is optional.

Owner Drop-Down Menu	• You can designate a policy for a specific owner or leave it public. Policy administration is based on privileges:
	  • Users with the Application Alarm Configuration privilege can view any policy or template, public or private. They can modify and delete their own policies or templates as well as those designated public.
	  • Users with the Application Alarm Admin privilege can view, modify, or delete any policy or template, public or private.

Profile Drop-Down Menu	• For a new policy, add an Alarm Profile from the list of profiles available for the selected Iris application.
Interface Drop-Down Menu	• Available only for an IPI policy. After selecting Service or Interface, select an interface or service from a list for the Iris application. • A service-based policy only applies to traffic corresponding to the selected Service. Service-based policies drive the FastPath workflow. • An interface-based policy only applies to traffic corresponding to the selected Interface. Alarms generated when an interface-based policy is violated, can only be viewed in the Alarm Browser; they do not appear in the FastPath workflow.
Studio Model	• Lists the available previously define Service Model. Available only for a KPI Studio policy.
Severity Drop-Down Menu	• Select the alarm severity associated with the policy.
Aggregation Window Drop-Down Menu Sample Interval Drop-Down Menu	• First select the length of the aggregation window. • Then select the length of the interval to sample within the aggregation window. Your choices depend on the length of the aggregation window that you selected.
Condition Summary	• View the policy threshold Boolean expression applied to this alarm policy, which is configured in the Condition and Assignment Editor window.
Assignments Area	• Each condition you defined in the Condition and Assignment Editor window appears in this area for you to assign additional dimensions. You can use protocol/application to choose other dimensions for ITA alarms. • Click the Edit button to change some features of the Conditions: Alarm Type, Condition, Average Over, and the selected Dimensions.
OR/AND Radio Buttons	• Use OR or AND logic when adding Conditions. If some Dimension types appear in several conditions, using the AND condition means an alarm will be generated only against the elements selected for all the conditions within that AND group. • A policy with AND Conditions must have the same filter type and the same elements selected for all conditions against all duplication Dimensions. Such Dimensions are considered to be shared. • If you try to select a Dimension which is already used in some other Condition, you will get a warning message letting you know that any changes to the shared Dimension will be applied to all Conditions that use that Dimension.

Actions Area	• Select from templates created in Action Templates tab. • Assign one or more available templates by selecting its check box.
Schedules Area	• Select from templates created in Schedule Templates tab. • Assign one or more available templates by selecting its check box.
Save Button	• Save the item currently displayed in the Details pane.
Cancel Button	• Cancel all changes made in the Details pane and refresh the pane data. • All unsaved changes are discarded.

Policies Tab - IPI Example



Action Templates Tab

The Action Templates tab enables you to create and manage action templates you can assign to individual Iris application policies in the Policies tab view or to alarm profiles in the Profiles tab view. The Action Templates tab consists of an Action Template List pane and an Action Template Details pane.You can access this tab when you click Alarms in the IrisView toolbar, select Policy Management from the submenu, and then click the Action Templates tab.

Action Template List Pane	• Lists all the Action templates you have created, and whether the ownership is Public or assigned to a particular user with either the Application Alarm Admin or Application Alarm Configuration privilege. • You can add new templates, delete templates from the list, or copy an existing template and modify it to create a new template. • When you select a template in the list, its properties are shown in the Details pane. Each template can only have one type of properties. • If you are using ACE, a single action is listed and it cannot be edited nor deleted. No ACE properties show in the Details pane when you select the ACE action template.
Action Template Details Pane	• Contains fields that enable you to configure the properties for a given action template you select in the List pane. • Configure an email template that includes email addresses for notification of threshold breach. • Configure an SNMP template that includes a destination IP and port number for sending alarms over SNMP.
Delete Button	• Select the check box next to an item on the list and then click **Delete** to remove the item from the list and from the system.
Add Button	• Display a blank Email form in the Action Template Details pane. • You can click the SNMP tab to create a new action using that category or just create an Email action.
Copy Button	• Select the check box next to an item on the list and then click **Copy** to generate a copy of an existing item, so you can modify it to create a new one. • When you click **Copy**, `Copy of...` is added in to the front of the item's name, which is displayed in the Details pane. • You can then change the information as needed and click the **Save** button in the Details pane.
More Options	• Export Option - Export all policies, action templates, schedule templates, and profiles to an XML file. All policy configurations are exported. This option is available only for users with the Application Alarm Admin privilege. For users with the Application Alarm Configuration privilege, the Export option is disabled. • Import Option - Open the Import Policies dialog box, where you can browse for policy configuration files to import and indicate whether you want to overwrite or synchronize the imported data. The import file includes policies, action templates, schedule templates, and profiles. This option is available only for users with the Application Alarm Admin privilege. For users with the Application Alarm Configuration privilege, the Import option is disabled. • Show XSD Option - Displays the content of the XML schema file, alarm_policies.xsd, within your default Internet browser. This option is available only for users with the Application Alarm Admin privilege. For users with the Application Alarm Configuration privilege, the Show XSD option is disabled.

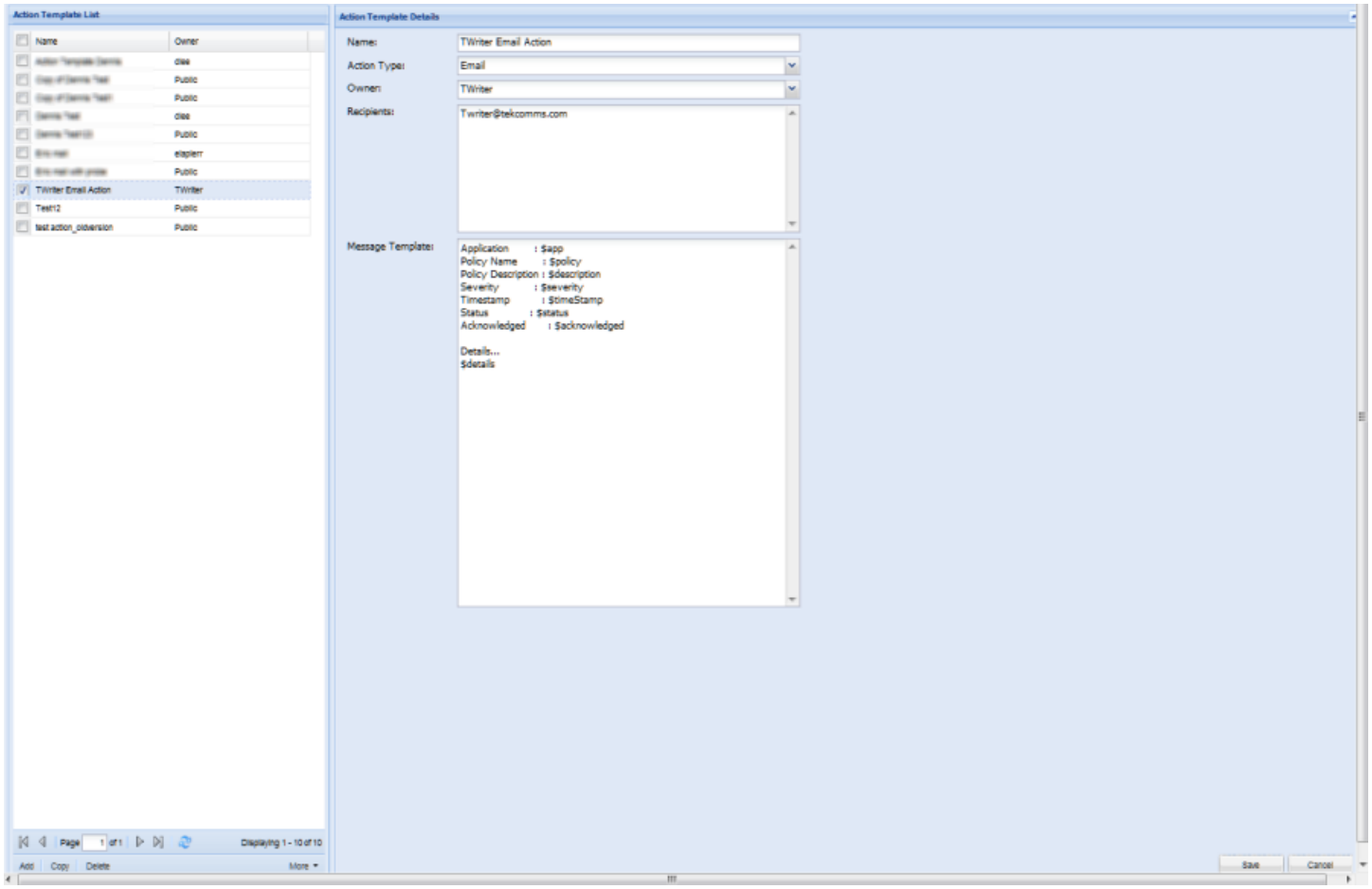
Action Template Details Area

Action Type		Select either Email or SNMP; fields vary depending on your selection.
Owner Drop-Down		You can designate a template for a specific owner or leave it public. Template administration is based on privileges: • Users with the Application Alarm Configuration privilege can view any policy or template, public or private. They can modify and delete their own policies or templates as well as those designated public. • Users with the Application Alarm Admin privilege can view, modify, or delete any policy or template, public or private.
Email	Name	Enter a name for the Email action template. The action templates you create will be available to use when you assign an action to a policy in the Policies window or when you assign email forwarding to a system alarm.
	Recipients	• Enter one or more email addresses, separated by a comma (,), a colon (:), or a semicolon (;), followed by a space. • The system notifies recipients when an alarm policy is violated.
	Message Template	The template enables custom formatting of alarm emails so they can be more SMS readable. The template ensures that pertinent information appears at the top of the email. Following is the default order and bindings supported: • Application : $app • Policy Name : $policy • Policy Description : $description • Severity : $severity • Timestamp : $timeStamp • Status : $status • Acknowledged : $acknowledged • Details... : $details
SNMP	Name	Available only for SNMP actions. The outgoing SNMP needs to be configured for SNMP Forwarding; please contact Customer Support for assistance. • Enter the name of the SNMP action. • Enter the destination IP addresses in IPv4 or IPv6 format. • Enter the destination port. • Enter a customized community string or use the default "public." The string cannot be empty (NULL) and cannot be more than 64 characters.
	Destination IP	
	Destination Port	
	Community String	
Save Button		• Save the item currently displayed in the Details pane.
Cancel Button		• Cancel all changes made in the Details pane and refresh the pane data. • All unsaved changes are discarded.
Show/Hide Button		Show or hide all the tabs in the Action Template Details pane. Tabs are shown by default.

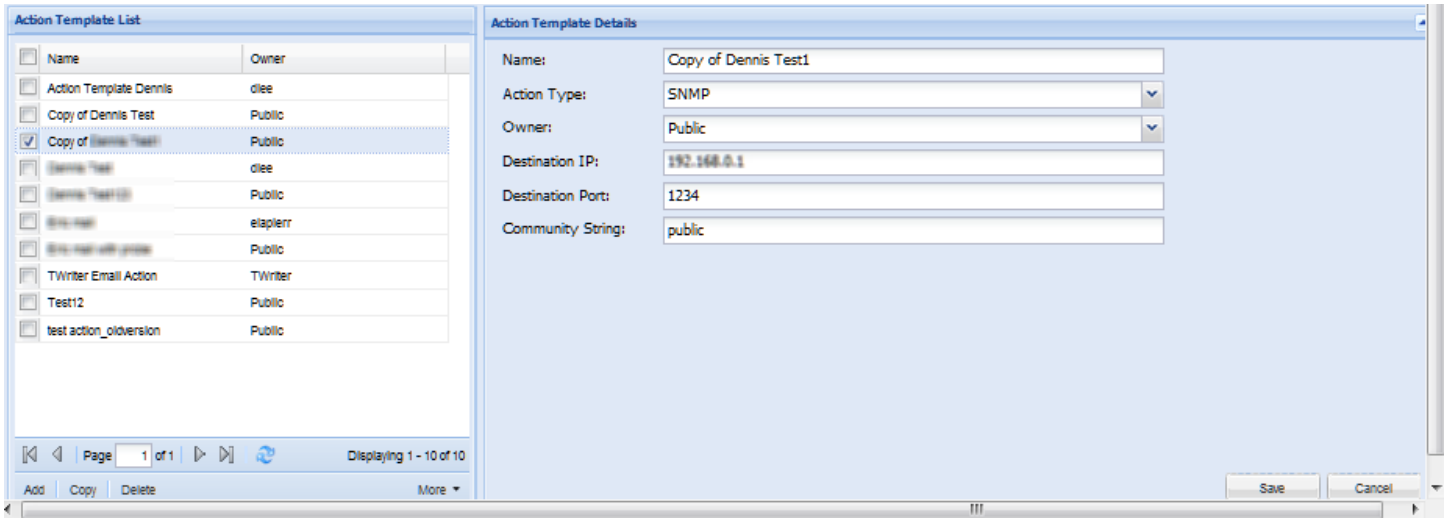
Column Filter Controls

Actions Menu	• To access the actions menu, hover your cursor over a column header until you see a down arrow and then click on it. • Apply a sort filter or select a column to show or hide.
Sort Ascending Button	• Sort table in ascending or descending order using the values in the selected column. • All numbers are sorted together first, then all upper case names are sorted together, and finally all lower case names are sorted together.
Sort Descending Button	
Columns Menu	• Select columns you want to show in the table and remove the checkmark from columns you want to hide. At least one column must remain visible.

Action Templates - Email



Action Templates - SNMP



Schedule Templates Tab

You can create schedule templates to define specific time frames that you want alarm policies and alarm profiles to generate alarms. If a policy or profile is assigned a schedule template, its associated alarms are not generated for a threshold violation unless the violation occurs within the defined schedule times.

The Schedule Templates tab enables you to create and manage schedule templates which you can assign to individual alarm policies in the Policies tab view or to alarm profiles in the Profiles tab view. The Schedule Templates tab consists of a Schedule Template List pane and a Schedule Template Details pane. You can access this tab when you click Alarms in the IrisView toolbar and then select Policy Management from the submenu.

Schedule Templates List Pane	• Lists all the Schedule templates you have created, as well as the Ownership status (public or assigned to a specific owner). • Use the Add, Delete, and Copy buttons near the bottom of the pane to manage new and existing templates. • Use the check box at the top of the list to select or deselect all templates in the list. Use the check box next to each template name to select or deselect individual templates. • When you select the check box next to a template in the list, its properties are shown in the Details pane.
Schedule Template Details Pane	• Configure the properties for a schedule template you select in the List pane.
Delete Button	• Select the check box next to an item on the list and then click **Delete** to remove the item from the list and from the system.
Add Button	• Open the Select Application dialog box, where you can select from a list of supported Iris applications. • When you click **OK**, a blank form appears in the Schedule Template Details pane.

Copy Button	• Select the check box next to an item on the list and then click **Copy** to generate a copy of an existing item, so you can modify it to create a new one. • When you click **Copy**, `Copy of...` is added in to the front of the item's name, which is displayed in the Details pane. • You can then change the information as needed and click the **Save** button in the Details pane.
More Options	• Export Option - Export all policies, action templates, schedule templates, and profiles to an XML file. All policy configurations are exported. This option is available only for users with the Application Alarm Admin privilege. For users with the Application Alarm Configuration privilege, the Export option is disabled. • Import Option - Open the Import Policies dialog box, where you can browse for policy configuration files to import and indicate whether you want to overwrite or synchronize the imported data. The import file includes policies, action templates, schedule templates, and profiles. This option is available only for users with the Application Alarm Admin privilege. For users with the Application Alarm Configuration privilege, the Import option is disabled. • Show XSD Option - Displays the content of the XML schema file, alarm_ policies.xsd, within your default Internet browser. This option is available only for users with the Application Alarm Admin privilege. For users with the Application Alarm Configuration privilege, the Show XSD option is disabled.

Schedule Template Details

Name Field	• Enter a name for the schedule template. The schedule templates you create will be available to use when you create or modify a policy in the Policies tab or a profile in the Profiles tab.

Owner Drop Down	• You can designate a template for a specific owner or leave it public. Template administration is based on privileges:
	  ◦ Users with the Application Alarm Configuration privilege can view any policy or template, public or private. They can modify and delete their own policies or templates as well as those designated public.
	  ◦ Users with the Application Alarm Admin privilege can view, modify, or delete any policy or template, public or private.

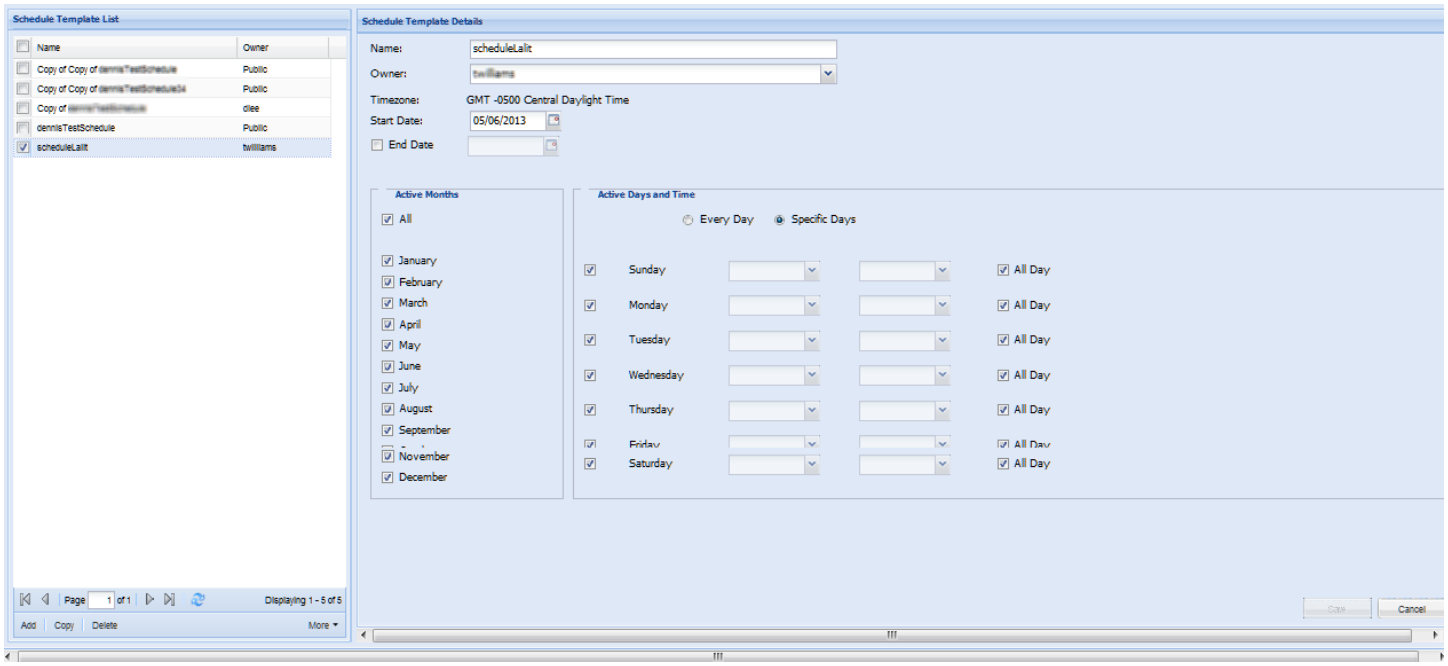
Start Date End Date	• Enter the Start Date by changing the value in the field or by selecting it from a calendar. To open the calendar, click the Calendar button and then click the Start or End Date. • Enter an End Date to deactivate the template (optional).
Timezone	• Displays the server time zone.
Active Months Area	• Select the months you want to generate alarms. • Select All to activate alarms for all months.
Active Days and Time Area	• Select Every Day or the specific days you want to generate alarms. • Select All Day or set a Start Time and End Time for each day. The End Time cannot be set earlier than the Start Time.
Save Button	• Save the item currently displayed in the Details pane.
Cancel Button	• Cancel all changes made in the Details pane and refresh the pane data. • All unsaved changes are discarded.

Column Filter Controls

The following controls apply for the columns in the Schedule Template List.

Actions Menu	• To access the actions menu, hover your cursor over a column header until you see a down arrow and then click on it. • Apply a sort filter or select a column to show or hide.
Sort Ascending Button	• Sort table in ascending or descending order using the values in the selected column. • All numbers are sorted together first, then all upper case names are sorted together, and finally all lower case names are sorted together.
Sort Descending Button	
Columns Menu	• Select columns you want to show in the table and remove the checkmark from columns you want to hide. At least one column must remain visible.

Schedule Templates Tab



Profiles Tab

Optionally, you can group policies into profiles that you can assign to users having the same functional responsibilities. Profiles enable you to control what alarms specific users can view. You can also assign schedule templates and action templates to profiles to further customize alarm views for specific groups. The Profiles tab consists of a Profile List pane and a Profile Details pane. You can access this tab when you select Alarms in the IrisView toolbar and then click Policy Management in the Alarms toolbar.

The Alarms Profile feature provides a Default profile which has the following functionality:

- All new policies are automatically added to Default profile if not assigned to another profile.
- When policies are assigned to user-defined profiles, they are removed from the Default profile.
- When user-defined profiles are deleted, associated policies are reassigned to the Default profile.
- When upgrading to 13.1, all policies will be assigned to the Default profile.

Profile List Pane	• Lists all the profiles you have created. • A green icon next to the profile name indicates it is enabled; a gray icon indicates it is disabled. • Use the Add, Delete, and Copy buttons near the bottom of the pane to manage new and existing profiles. • Use the check box at the top of the list to select or deselect all profiles in the list. Use the check box next to each profile name to select or deselect individual profiles. • When you select the check box next to a profile in the list, its properties are shown in the Details pane. • A read-only Default profile contains all defined policies not assigned to other profiles.
Profile Details Pane	• Contains the Users, Policies, Actions, and Schedules dashlets for configuring the profile you select in the List pane.
Show Enabled Check Box	• Select to display in the list only profiles that have Enabled status.
Add Button	• Open a blank form in the Details pane.
Copy Button	• Select the check box next to an item on the list and then click **Copy** to generate a copy of an existing item, so you can modify it to create a new one. • When you click **Copy**, `Copy of...` is added in to the front of the item's name, which is displayed in the Details pane. • You can then change the information as needed and click the **Save** button in the Details pane.
Delete Button	• Select the check box next to a profile on the list and then click **Delete** to remove the profile from the list and from the system. • All policies assigned to the deleted profile are reassigned to the Default profile. • You cannot delete the Default profile.
More Options	• Enable/Disable - Select the checkbox next to one or more items on the list and then select Enable or Disable to change the status of the selected profile(s). • Export Option - Export all policies, action templates, schedule templates, and profiles to an XML file. All policy configurations are exported. This option is available only for users with the Application Alarm Admin privilege. For users with the Application Alarm Configuration privilege, the Export option is disabled. • Import Option - Open the Import Policies dialog box, where you can browse for policy configuration files to import and indicate whether you want to overwrite or synchronize the imported data. The import file includes policies, action templates, schedule templates, and profiles. This option is available only for users with the Application Alarm Admin privilege. For users with the Application Alarm Configuration privilege, the Import option is disabled. • Show XSD Option - Displays the content of the XML schema file, alarm_policies.xsd, within your default Internet browser. This option is available only for users with the Application Alarm Admin privilege. For users with the Application Alarm Configuration privilege, the Show XSD option is disabled.

Profile Details

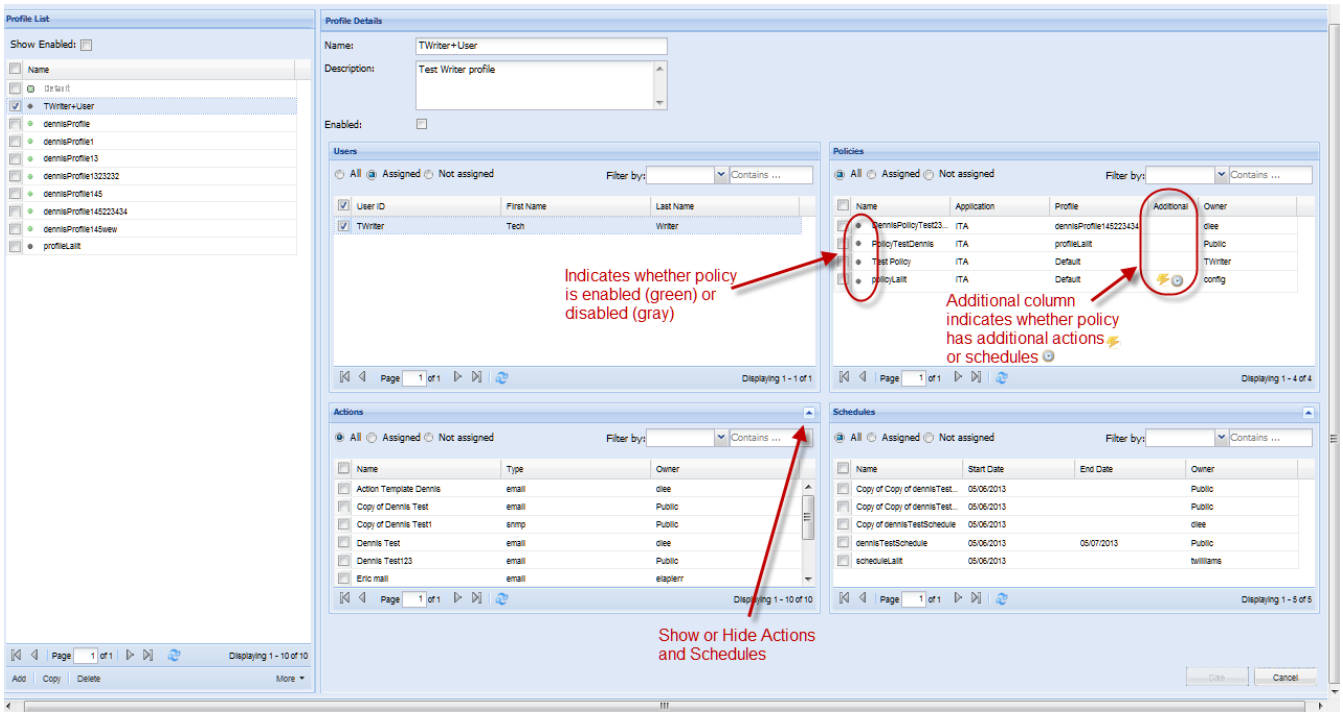
Name	• Enter a name and brief description for the profile. • In the Alarm dashboard, you can filter on profile names and description keywords using the Global Filter Advanced Filters. • The Description field is optional.
Description	
Enabled Check Box	• Click this check box to change the status of the alarm profile from enabled to disabled. By default, all profiles are disabled.
Dashlet Controls	• Use the All, Assigned and Not Assigned radio buttons and the Filter by menu to filter the list. • Use the check box at the top of the list to select or deselect all items in the list. • Sort columns using the Column Filter Controls (not applicable to the Policies dashlet Additional column)
Users Dashlet	• Select the users you want to assign to the profile. • Only alarm users are listed in the dashlet.
Policies Dashlet	• Assign policies to the profile by clicking the check box next to each policy name. You can assign policies from different supported Iris applications to the same profile. • **A policy can only be assigned to one profile.** If you select a policy that is currently assigned to another profile, it is assigned to the current profile, and unassigned from the other profile. • A green icon next to the policy name indicates it is enabled; a gray icon indicates it is disabled. You can control a policy's status in the Policies tab. • The Additional column shows icons indicating whether the policy has additional actions or schedules. A policy's schedules and actions complement the profiles actions and templates. Refer to Profile Action Template Example and Profile Schedule Example for details.
Actions Dashlet	• Assign action templates to the profile by clicking the check box next to each name. • A policy's action templates complement the profile's action templates. Refer to Profile Action Template Example for details.
Schedules Dashlet	• Assign schedule templates to the profile by clicking the check box next to each name. • A policy's schedule templates complement the profile's schedule templates. Refer to Profile Schedule Example for details.
Save Button	• Save the changes made in the Details pane.
Cancel Button	• Cancel all changes made in the Details pane and refresh the pane data. • All unsaved changes are discarded. • Unsaved changes to policy assignments are identified by a red triangle in the upper left corner of the cell in the Profile column.

Column Filter Controls

Actions Menu	• To access the actions menu, hover your cursor over a column header until you see a down arrow and then click on it. • Apply a sort filter or select a column to show or hide.

Sort Ascending Button	• Sort table in ascending or descending order using the values in the selected column. • All numbers are sorted together first, then all upper case names are sorted together, and finally all lower case names are sorted together.
Sort Descending Button	
Columns Menu	• Select columns you want to show in the table and remove the checkmark from columns you want to hide. At least one column must remain visible.

Profiles Tab



Profile Schedule Template Example

The Profile schedule templates have an OR relationship with their associated policies' schedule templates. The following example shows alarm behavior when both a profile has been assigned a schedule and its associated policies have been assigned separate schedule templates.

Profile A
Profile Schedule Mon-Fri 12pm-8pm

Policies in Profile A	Policy Schedule	Alarms Triggered
Policy 1	Mon-Fri 8am-5pm	Mon-Fri 8am to 8pm
Policy 2	Tue-Thur 11am-3pm	Mon 12pm-8pm Tues-Thurs 11am-8pm Fri 12pm-8pm
Policy 3	Sat-Sun 12pm-12am	Mon-Fri 12pm-8pm Sat-Sun 12pm-12am

Profile Action Template Example

If a profile shares the same action template as one of its policies, then only one action is performed when an alarm is triggered. However, if the same action is defined in two separate templates (one for profile and one for policy), then two

actions are performed. The following example shows alarm behavior when both a profile has been assigned actions and its associated policies have been assigned separate action templates.

Profile A
Profile Actions SNMP Destination X and Z
Profile Actions Email Persons A, B, C, D

Policies in Profile A	Policy Actions	Actions Performed when Alarm Triggered
Policy 1	SNMP Destination X and W	SNMP to Destination X, W, and Z. • If Destination X is defined in the same action template, then only one SNMP trap is sent. • If Destination X is defined in two separate action templates (1st assigned to profile, 2nd to policy) with the same destination (IP address and port), then two traps will be sent to this destination when alarm is triggered. Email to Persons A, B, C, and D
Policy 2	Email Persons B, C, E, F	SNMP Destination X and Z Email Persons A, B, C, D, E, F • If mail recipients B and C are defined in the same action template, then only one email is sent. • If mail recipients B and C are defined in two separate action templates (1st assigned to profile, 2nd to policy), then two traps will be sent to this destination when the alarm is triggered.
Policy 3	SNMP Destination Y	SNMP to Destination X, Y, and Z Email Persons A, B, C, D

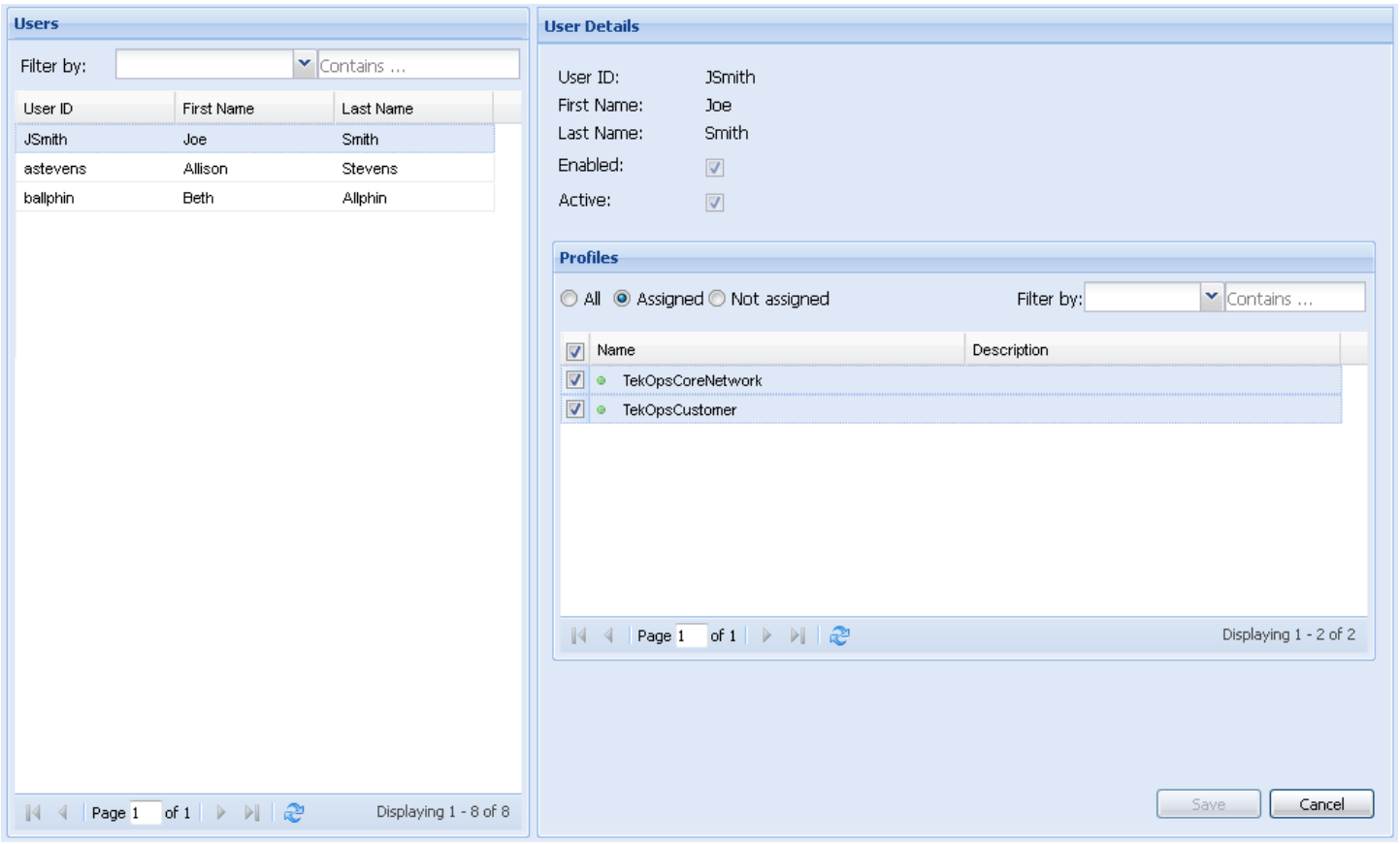
Users to Profiles Tab

The Users to Profiles tab lists all users defined in the system and the profiles assigned to them. You can modify user profile assignments from this window. The Users to Profiles tab consists of a Users List pane and a User Details pane. You can access this tab when you select Alarms in the IrisView toolbar and then click Policy Management in the Alarms toolbar.

User List Pane	• Lists all the users defined in the system. • You can filter the list by User ID, first name, last name.
User Details Pane	• View defined user details and user-enabled and active status. User status is managed in UUMS. • Only alarm users are listed in the dashlet.

Profiles Dashlet	• Assign profiles to the selected user by clicking the check box next to each profile. You can also assign users to profiles on the Profiles Tab. • Use the All, Assigned and Not Assigned radio buttons and the Filter by menu to filter the list. • Use the check box at the top of the list to select or deselect all items in the list.
Save Button	• Save the changes in the Details pane.
Cancel Button	• Cancel all changes made in the Details pane and refresh the pane data. • All unsaved changes are discarded. • Unsaved changes are identified by a red triangle in the upper left corner of the cell.

Users to Profiles Tab



System Alarms Tab

The System Alarms tab displays all the G10 alarms along with their details such as application, description, severity, thresholds, and SNMP details. You can access this tab when you click Alarms in the IrisView toolbar, select Policy Management from the submenu, and then click the System Alarms tab.

Note: *The System Alarms Tab is applicable for most system-level alarms. However, some system alarms are not accessible from this tab and cannot be modified (such as IFC alarms).*

The System Alarms tab consists of an G10 Alarms window and a Forwarding window.

G10 Alarms window	• The G10 Alarms pane lists all the G10 alarms. • The Alarm Details pane displays details about the selected alarm including application, SNMP or email forwarding indication, description, severity, and thresholds.
Forwarding window	• Use the SNMP pane to enable SNMP forwarding and to specify the severity and action template to use. Create action templates for SNMP forwarding using the Action Templates tab. Additionally use this tab to set up periodic test traps. • Use the Email pane to enable email forwarding and to select a severity and template to associate with email forwarding.

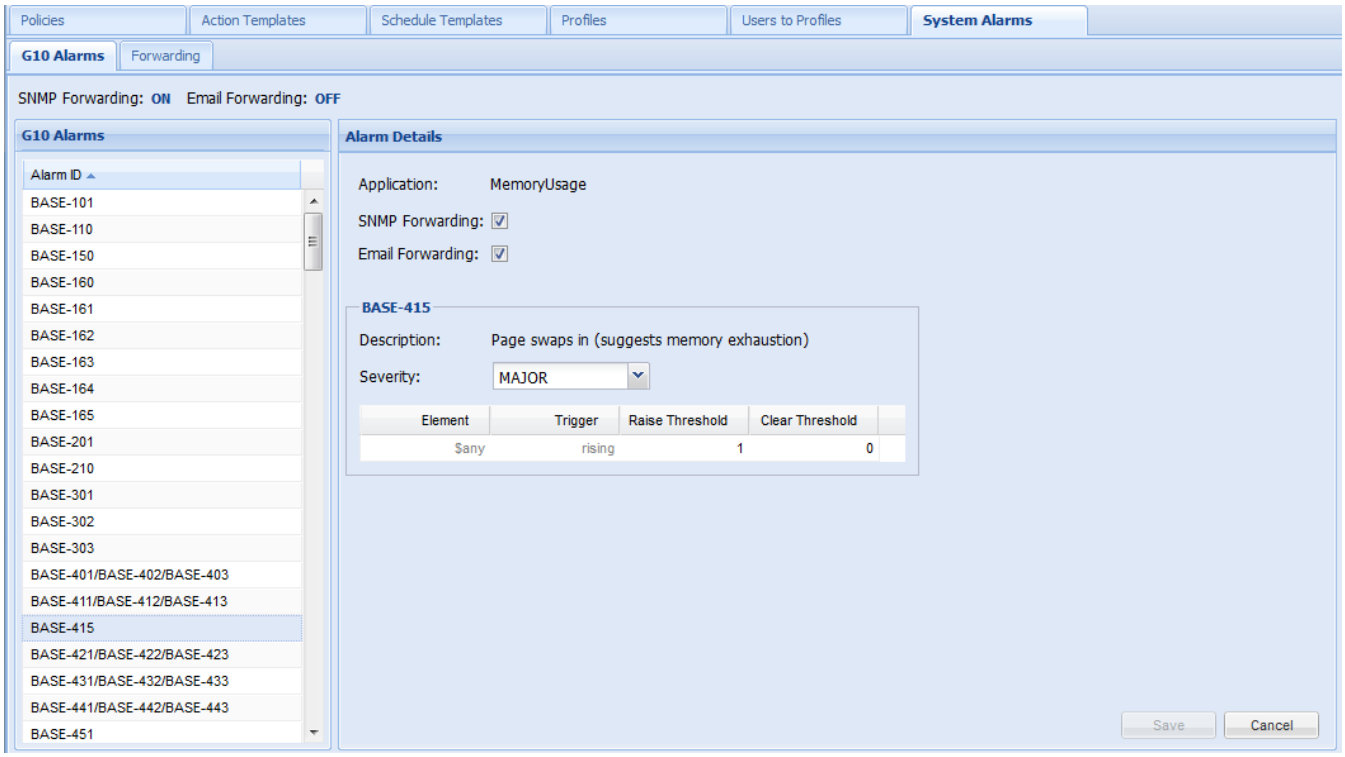
G10 Alarms Window

The G10 Alarms Window displays details for each G10 alarm and allows you to configure aspects of each alarm. You can access the G10 Alarms window from the System Alarms tab.

The first five fields are common to all system-level alarms. Availability of the last four attributes varies depending on the alarm.

Application	Displays the application for the chosen G10 alarm. This field cannot be modified.
SNMP Forwarding	Enable SNMP forwarding for the alarm. This is individual alarm based and it overrides the Enable SNMP Forwarding checkbox in the Forwarding window.
Email Forwarding	Enable Email forwarding for the alarm. This is individual alarm based and overrides the Enable Email Forwarding checkbox in the Forwarding window.
Description	Gives a brief description of the alarm. This field cannot be modified.
Severity drop down box	Modify an alarm severity: Information, Minor, Major, or Critical. **Note:** Some alarms do not have configurable severity.
Element	Shows the alarms element types. This field cannot be modified.
Trigger	Shows the trigger for the particular element type for the alarm. This field cannot be modified.
Raise Threshold	Modify the raise threshold for the alarm element.
Clear Threshold	Modify the clear threshold for the alarm element.

G10 Alarms Window

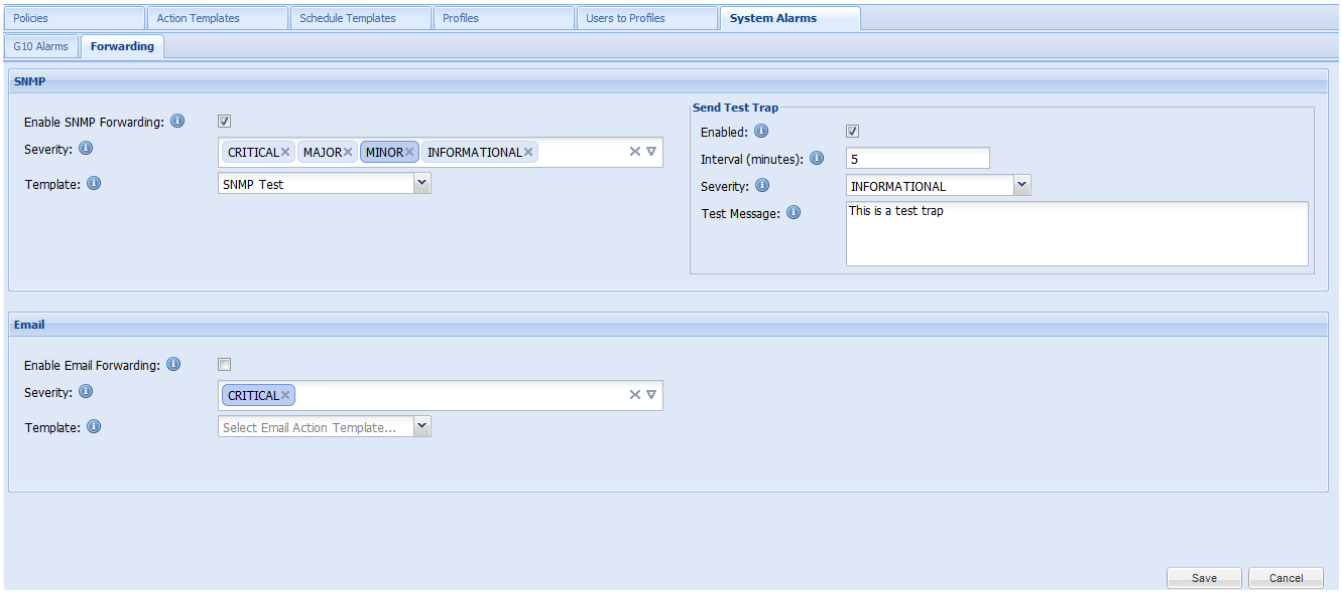


Forwarding Window

The Forwarding window allows you to configure SNMP forwarding, test traps, and email forwarding for system alarms. You can access the Forwarding window from the System Alarms tab.

SNMP Pane	
Enable SNMP Forwarding	Select to globally enable SNMP forwarding. This setting can be overridden at the individual alarm level.
Severity	Select which levels of severity are to be forwarded using SNMP
Template	The action template to associate with SNMP forwarding.
Send Test Trap	
Enabled	Select to send periodic test traps to the configured SNMP receiver.
Interval (minutes)	Select the interval (between 1 and 60 minutes) for test traps to be sent.
Severity	The severity of the test alarms sent to the SNMP receiver.
Test Message	The trap message to send to the SNMP receiver.
Email Pane	
Enable Email Forwarding	Select to globally enable email forwarding. This setting can be overridden at the individual alarm level.
Severity	Select which levels of severity are to be forwarded using email.
Template	The action template to associate with email forwarding.

Forwarding Window



Condition and Assignment Editor Window

The Condition and Assignment Editor window enables you to configure the alarm policy conditions and dimensions for the supported Iris applications. There are some differences in the Condition and Assignment Editor window for KPI Studio.

Category Drop-Down Menu	Select the KPI category corresponding to the Iris application.
KPI/KQI Drop-Down Menu	Select the KPI or KQI for which you are setting the alarm; values in this list depend on the Category selected.
Alarm Type Drop-Down Menu	Select the Alarm Type: • Absolute • Relative % - Previous Day • Relative % - Previous Week • Relative % - Previous 4 Weeks • Relative % - Previous Period • Relative Value - Previous Day • Relative Value - Previous Week • Relative Value - Previous 4 Weeks • Relative Value - Previous Period See Relative Percentage Example for more information on how to configure Relative Percentage alarms.

Condition Drop-Down Menu	Select the alarm trigger criteria for the policy : • Greater than • Greater than or Equal to • Less than • Less than or Equal to • Outside of +/- • Outside of or Equal to +/-
Average Over Drop-Down Menu	This value is only available for relative alarms and shows the number of periods that will be used in the averaging calculation. If the value is 1 period, no averaging will be performed. Options are: • 1 period (no averaging) • 2 periods • 3 periods • 4 periods
Alarm Trigger area	The Alarm Trigger area has different values based on the severity and conditions set. In the example provided, the alarm is Minor Condition is Greater than.
Threshold triggering	Shows the threshold value that will be used to trigger the alarm.
Threshold clearing	Shows the threshold value that will be used to automatically clear the alarm. This value is only available when the Auto Clear check box has been selected and a value has been provided.
Min samples triggering	Shows the minimum number of samples required before the alarm can be triggered.
Min samples clearing	Shows the minimum number of samples required before the alarm can be automatically cleared. This value is only available when the Auto Clear check box has been selected and a value has been provided.
Save Button	Save the information currently displayed in the Condition and Assignment Editor window. The Save button is not active until all required fields have values. Required fields have a red box until a valid value is selected.
Cancel Button	Cancel all changes made in the Condition and Assignment Editor window and return to the Policies tab window. All unsaved changes are discarded.

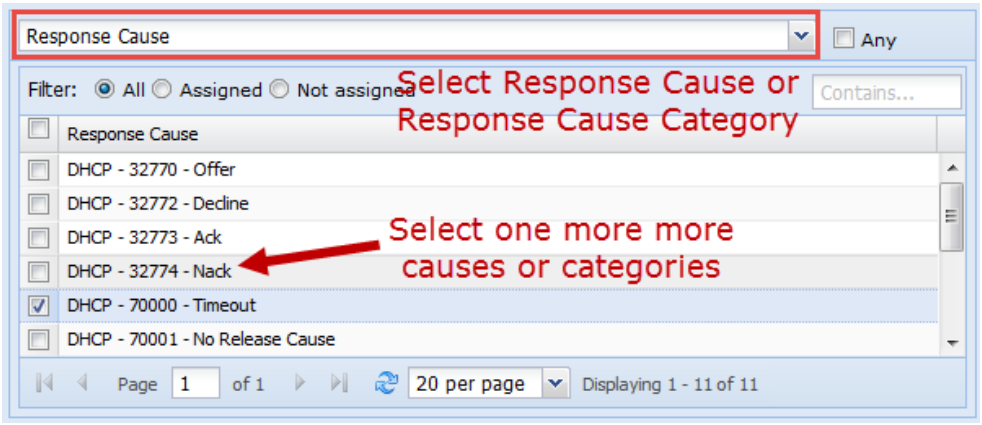
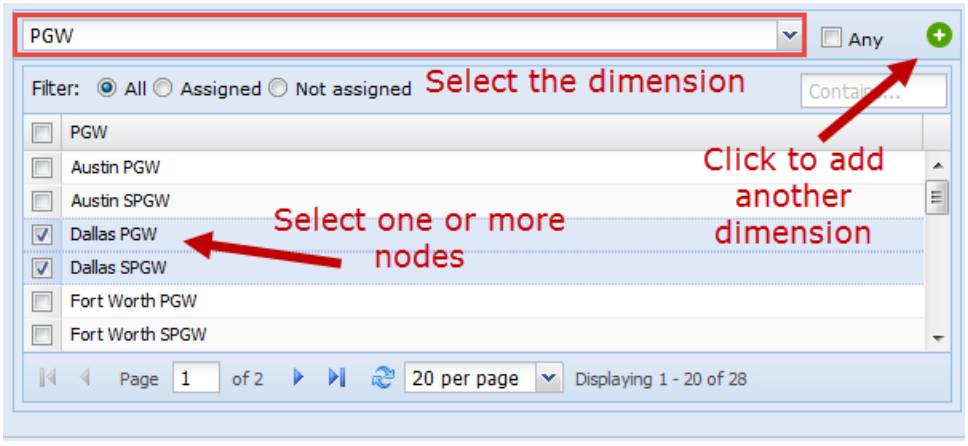
Dimensions Area

Note: Refer to the next section, Dimensions Area for IPI Response Code Category for the dimension area details for IPI alarms triggered by response codes.

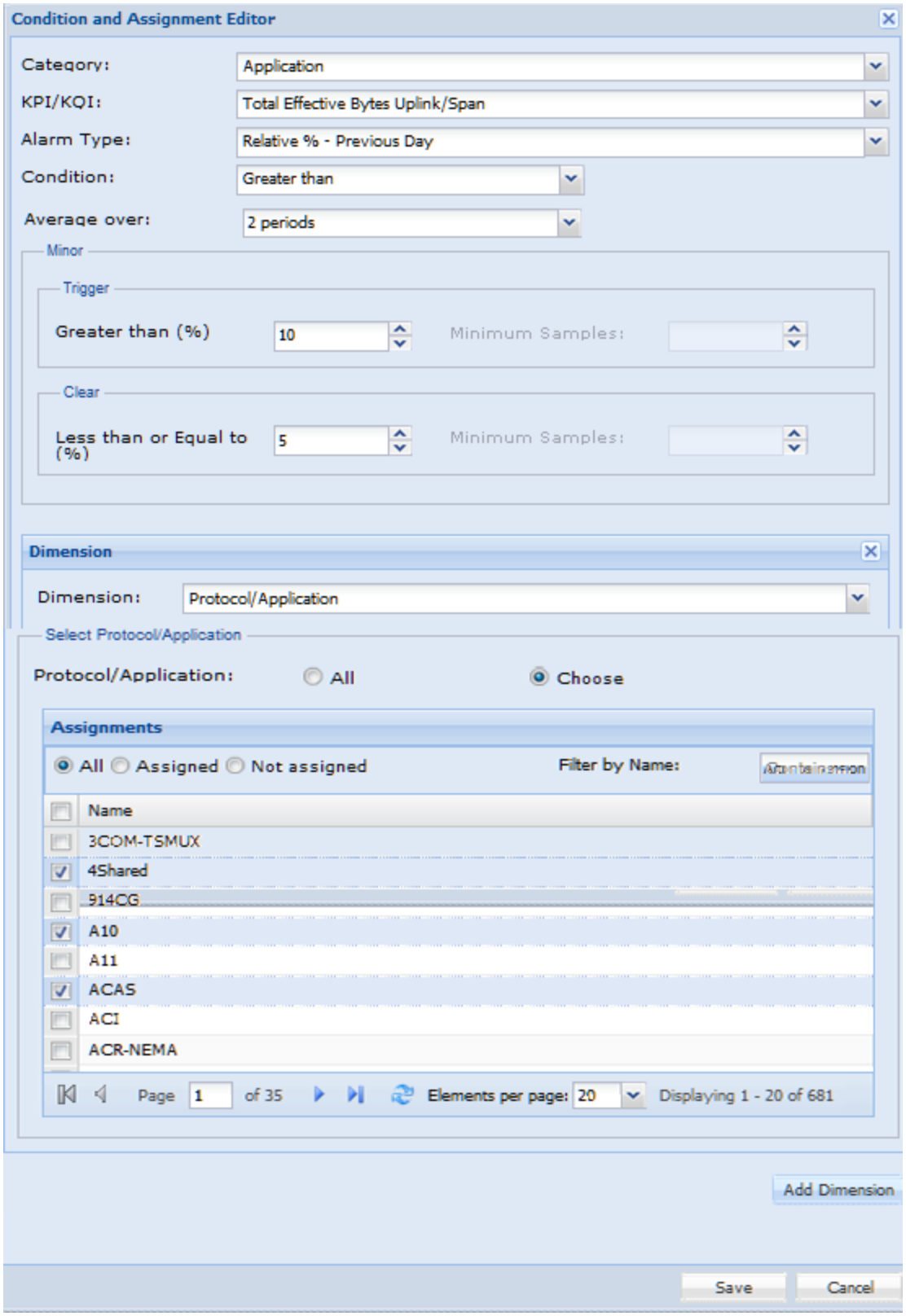
Dimension Drop-Down Menu	Select the Dimension category, corresponding to the supported Iris application.
Select Dimension	Select the Dimension, based on the Dimension category selected. You can select All, or click the Choose radio button to display a list of Assignments.
Assignments	Shows all of the Assigned and Not assigned elements to choose for Dimensions.
Filter by Name	Filter the list of Dimensions by entering a name, partial or whole.
Add Dimension Button	Use the Add Dimension button to add more Dimensions to this policy.

Dimensions Area for IPI Response Code Category

The following dimension area details appear for IPI alarms triggered by response code.

Protocol Drop-Down Menu	Select the protocol to use for the Dimension.
Procedure Drop-Down Menu	Select the procedure to use for the Dimension. The available procedures depend on the protocol selected. Not all combinations of procedures and protocols are supported for a Dimension. An error message appears if you attempt to select an invalid combination.
Attribute Multi-Select Box	The Attribute field only appears for certain protocol/procedure combinations. Select the attribute or attributes that apply.
RC Protocol Drop-Down Menu	Select the Response Code Protocol that corresponds with the selected protocol and procedure.
Response Cause Multi-Select Box	The Response Cause multi-select box allows you to select the response causes or categories that should apply for this dimension. **Note:** Response Code Category is only available if Number of Occurrences or Percent of All Occurrences was selected as the KPI/KQI. For Failure, Success, or Timeout KPIs, only Response Cause is available. You can specify that any response cause or category should apply (select the Any checkbox), or you can select one or more specific response causes or categories from the list. 
Select Node Dimension Drop-Down Menu	Select a dimension from the list (If only one dimension is availabe, it is preselected). The available nodes for that dimension appear. Select one or more nodes. Click the Plus sign in the corner of the Node Dimension box to add another dimenion. 

Condition and Assignment Editor - ITA Example



Condition and Assignment Editor Window - KPI Studio

The Condition and Assignment Editor window enables you to configure the alarm policy conditions and dimensions for KPI Studio. There are some differences in the Condition and Assignment Editor window for other support Iris applications.

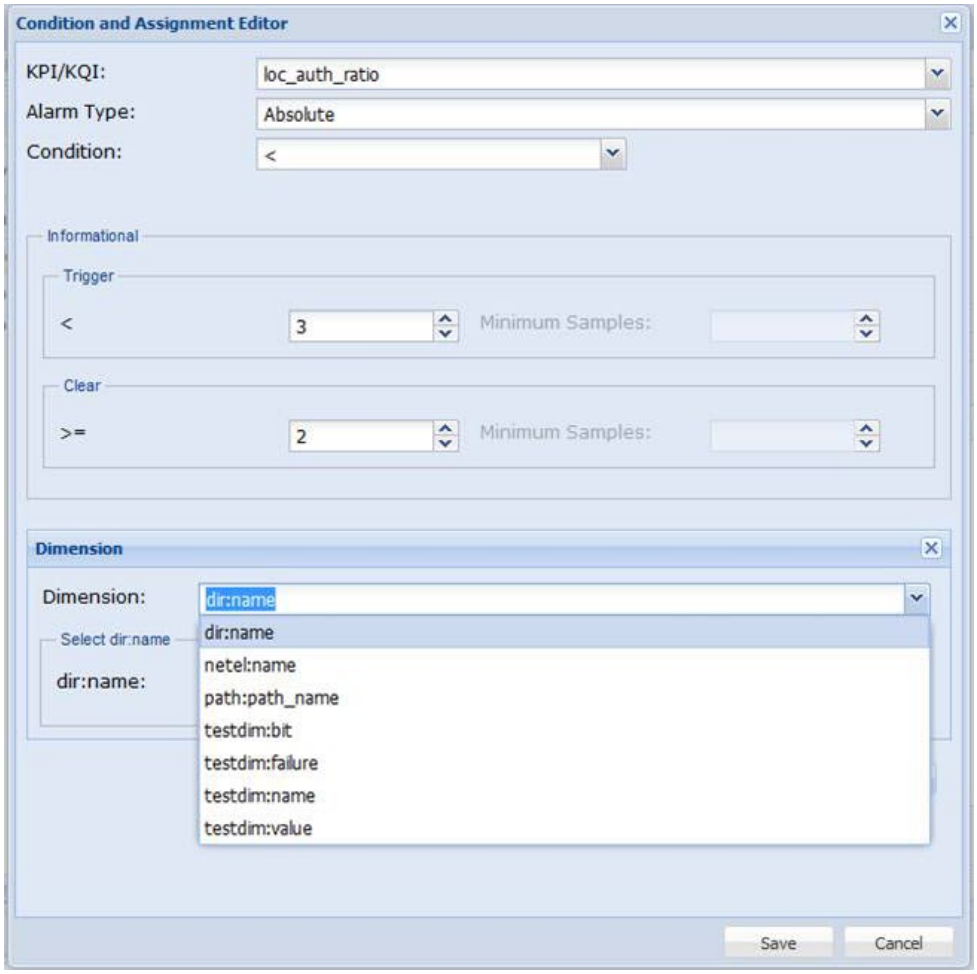
KPI/KQI	Select the KPI or KQI for which you are setting the alarm.
Alarm Type	Select the Alarm Type: • Absolute • Relative % - Previous Day • Relative % - Previous Week • Relative % - Previous 4 Weeks • Relative % - Previous Period • Relative Value - Previous Day • Relative Value - Previous Week • Relative Value - Previous 4 Weeks • Relative Value - Previous Period See Relative Percentage Example for more information on how to configure Relative Percentage alarms.
Condition Drop-Down Menu	Select the alarm trigger criteria for the policy : • Greater than • Greater than or Equal to • Less than • Less than or Equal to • Outside of +/- • Outside of or Equal to +/-
Average Over Drop-Down Menu	This value is only available for relative alarms and shows the number of periods that will be used in the averaging calculation. If the value is 1 period, no averaging will be performed. Options are: • 1 period (no averaging) • 2 periods • 3 periods • 4 periods
Alarm Trigger area	The Alarm Trigger area has different values based on the severity and conditions set. In the example provided, the alarm is Minor Condition is Greater than.
Threshold triggering	Shows the threshold value that will be used to trigger the alarm.
Threshold clearing	Shows the threshold value that will be used to automatically clear the alarm. This value is only available when the Auto Clear check box has been selected and a value has been provided.
Min samples triggering	Shows the minimum number of samples required before the alarm can be triggered.
Min samples clearing	Shows the minimum number of samples required before the alarm can be automatically cleared. This value is only available when the Auto Clear check box has been selected and a value has been provided.

Save Button	Save the information currently displayed in the Condition and Assignment Editor window. The Save button is not active until all required fields have values. Required fields have a red box until a valid value is selected.
Cancel Button	Cancel all changes made in the Condition and Assignment Editor window and return to the Policies tab window. All unsaved changes are discarded.

Dimensions Area

Dimension Drop-Down Menu	Select the Dimension category for KPI Studio.
Select Dimension	Select the Dimension, based on the Dimension category selected. You can select All, or click the Choose radio button to display a list of Assignments.
Assignments	Shows all of the Assigned and Not assigned elements to choose for Dimensions.
Filter by Name	Filter the list of Dimensions by entering a name, partial or whole.
Add Dimension Button	Use the Add Dimension button to add more Dimensions to this policy.

Condition and Assignment Editor - KPI Studio Example

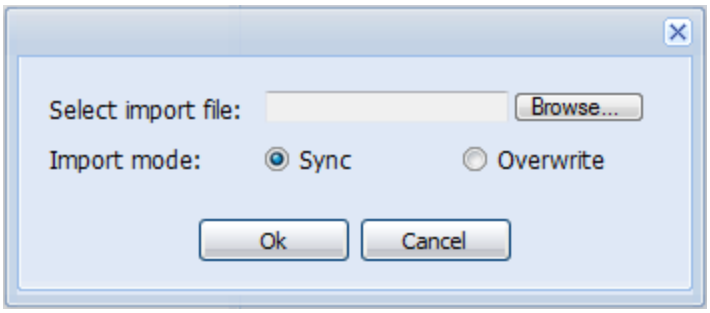


Import Policy Data Dialog Box

Use the Import Policy Data dialog box to import policy configurations contained in an XML file. For details on the import process, limitations, and error, see Exporting and Importing Policy Data. You access this dialog box when you click the More menu then select Import from the Policies, Action Templates, Schedule Templates, or Profiles tabs.

Select import file Field	Enter the path and name of the policy configurations file to import. You can also click the Browse button and then navigate to the file you want to import.
Browse Button	
Import mode Sync Option	Synchronize the data you plan to import with the existing alarm policy configurations. Sync mode means that the configuration item will be saved in the database only if it is missing from the database; otherwise, only the changed items are updated. The system synchronizes imported policy data with the current database based on policy configuration item names. For instance, if an imported policy has the same name as a policy already in the database, the imported policy will be ignored.
Import mode Overwrite Option	Replace the existing policy configurations with the data you plan to import. The Overwrite mode means that the policy configuration currently stored in the database will be replaced with the configuration from the XML file being imported.
OK Button	Import the policy configurations.
Cancel Button	Close the dialog box without importing any data.

Import Policy Data



Iris Alarms References

The following references are provided for Iris Alarms.

- Iris Application Policies and Alarms
- Iris User Privileges
- Iris Entity Support
- Iris Alarm Types
- Iris KPI Studio Alarms
- Configuring Relative and Absolute Alarms
- Relative Percentage Alarm Example
- Configuring Aggregate Alarms
- Iris Alarm Acknowledgement
- Iris Alarm Clearing
- Using Minimum Samples to Cancel Noise
- Configuring Protocol/Application Alarms for ITA KPIs
- Exporting Iris Alarms
- Exporting and Importing Alarm Policy Data
- Iris SNMP Alarm Forwarding
- Updating or Deleting Templates
- IPI Key Performance Indicators
- IPI KPI Bin Count Calculations
- ITA Key Performance Indicators
- IPI Reference Guide

Iris Application Policies and Alarms

The Iris Alarms feature enables you to create or manage alarm policies and analyze alarms for the following Iris applications.

Application	Analyzing Alarms	Managing Alarm Policies
ITA	Monitor and analyze ITA alarms in the Alarm dashboard. From the Alarm Browser, drill down from some ITA alarms to an ITA dashlet. For an ITA alarm drill-down use case, see Analyzing Critical Alarms Using the Alarm Dashboard.	Create and manage ITA policies.
IPI	Monitor and analyze all IPI alarms in the Alarm Dashboard. Monitor and analyze all types of service-based alarms in FastPath.	Create and manage IPI policies.
KPI Studio	Monitor and analyze all KPI Studio alarms in the Alarm Dashboard Monitor.	Create and manage KPI Studio policies.

Application	Analyzing Alarms	Managing Alarm Policies
ACE	Monitor and analyze ACE alarms in the Alarm Dashboard.	Create and manage ACE policies. Also, assign Notify ACE action to any IPI, ITA, or ACE policy.
GEO	Monitor and analyze alarms generated by the GeoProbe system.	GEO alarm policies are created and managed in the GeoProbe system. In IrisView, GEO alarms are treated in similar ways as system-level alarms. When you acknowledge and clear GEO alarms in IrisView, these alarms will not be cleared nor acknowledged in the GeoProbe system.
Iris System	Monitor and analyze system-level alarms in the Alarm Dashboard.	Configure thresholds and severities, and configure SNMP alarm forwarding for system-level alarms on the System Alarms tab.

Policy Configuration

Application	Interface	Aggregation	Conditions
ITA	All interfaces supported by G10 probes	Select the following options to configure Tumbling window or Sliding window: • First, select Aggregation Window • Then, select Sample Interval	• Set one or more conditions using available ITA KPIs
IPI	Select IPI interface from: • Mobile LTE Data • Mobile 2G/3G Data • Mobile 2G/3G Voice • VoIP (Fixed Voice) Or, select an IPI Service		• Set one or more conditions using available IPI KPIs and KQIs • See calculations for Bin Count KPIs
KPI Studio	Select from the following Studio Models:		• Set one or more conditions using available KPI Studio KPIs and KQIs
ACE	• SpIprobe • DirectQuality	Not Applicable	• Set number of Statistical Event Alarms • Set number of Threshold Alarms

IPI-Specific Policy Configuration

Service	FastPath can only display IPI alarms generated from service-based policies. Select a service from: • Network (default) • A list of Voice, LTE, or 2G/3G custom services defined through Customer Support

Condition and Assignment Editor Configuration

Application	KPI Category	Dimensions	Actions
ITA	Select one of the following categories: • Application • Link • Server (Node)	Select from these ITA dimensions: • Applications • Servers • Links • VLANs Select from Other Dimensions: • Application/Protocols • Response Codes and Response Code Types • Transactions and Transaction Types • Message Types (MSRP and TLS only) • VLAN (RTP only)	Assign any of the following actions: • Email • SNMP Forward • Notify ACE
IPI	Select one of the following categories: • Accessibility • Others • Performance • Response Code • Retainability	Select from these IPI dimensions: • Mobile LTE Data • Mobile 2G/3G Data • Mobile 2G/3G Voice • VoIP (Voice)	
ACE	Only one category: • ACE_Event	Select from these ACE dimensions: • Source Probe • Alarm Number • Called Number • DirectQuality Test Type • Originating Probe	

Action Template Configuration

Action	Configuration Parameters
Email	For each action, enter the following: • Name of the Email action • Email addresses of one or more recipients • Custom format of the message using supported bindings, such as Policy Name and Severity, so the email is in SMS readable form

Action	Configuration Parameters
SNMP Forward	For each action, enter the following: • Name of SNMP action • Owner • Destination IP addresses • Destination port • Community String
Notify ACE	No configuration is needed but you must have the ACE license; action is available for IPI, ITA, or ACE policies.

Iris Entity Support

Iris applications support entities configured for G10 probes and also entities configured for SpIprobes. The entities you configure on the Topology Tab in Iris Admin are only used by G10 probes. You configure entities for SpIprobes (14U, 3U, and 2U) on the GeoProbe system network maps. Refer to the GeoProbe documentation for configuration details.

Iris entity support varies for each Iris application and depends on whether the entities were configured for G10 probes using the Iris Topology tab in Iris Admin or configured for SpIprobes using the GeoProbe Network Configuration application.

The following table summarizes entity support for each Iris application and each probe type.

Configured Entities	Iris Application Entity Support									
	Configured for G10[1]						Configured for SpIprobe (SPI)[2]			
	PA	ITA	ISA	Policy Mgmt[3]	IPI	Maps	PA	ISA	IPI	Maps
Physical Links • Defined as a bidirectional Ethernet link • Consists of one or more physical ports • Can only be assigned to a single probe	X	X	X	X						

Configured Entities	Iris Application Entity Support									
	Configured for G10[1]						Configured for SpIprobe (SPI)[2]			
	PA	ITA	ISA	Policy Mgmt[3]	IPI	Maps	PA	ISA	IPI	Maps
Physical Link Groups • Used to group together one or more physical links • Enables aggregated data display - for example, ITA can display KPIs for a set of links instead of one link at a time • Supports a link belonging to multiple groups		X								
Logical Links • Concept of logical-level connections in the network, such as IP paths and SCTP connections • Can be grouped at the user-interface level to provide a level of aggregation						X	X	X		X
Logical Link Groups • Used to group together one or more logical links • Enables aggregated data display Supports a link belonging to multiple groups						X	X			X

Configured Entities	Iris Application Entity Support									
	Configured for G10[1]						Configured for SpIprobe (SPI)[2]			
	PA	ITA	ISA	Policy Mgmt[3]	IPI	Maps	PA	ISA	IPI	Maps
Nodes • Represents various active network elements with IP addresses such as IT Servers, GGSNs, and SGSNs • Iris and GeoProbe servers are not shown on Maps • Supports individual IP addresses or ranges or point codes • An IP address cannot belong to more than one node		X	X	X	X	X	X	X	X	X
Node Groups[4] • Used to group together one or more network nodes. • Enables aggregated data to display - for example, ITA can display KPIs for a set of nodes instead of one node at a time • Supports a node belonging to multiple groups		X	X			X	X	X		
Probes • Represents a G10 probe or SpIprobe			X			X		X		X
Probe Groups • Groups one or more probes of the same type			X			X				

Configured Entities	Iris Application Entity Support									
	Configured for G10[1]						Configured for SpIprobe (SPI)[2]			
	PA	ITA	ISA	Policy Mgmt[3]	IPI	Maps	PA	ISA	IPI	Maps
G10 Protocols and Applications[5] • Can be enabled or disabled for PDU capture • Supports customizing of L7 application protocol port ranges	X	X	X	X	X					
SpIprobe Protocols • Can be enabled or disabled for PDU capture							X	X	X	
Protocol Groups	Not supported in current release						Not supported in current release			

[1]ISA, PA, and IPI applications require access to historical data stored on G10 probe storage arrays.

[2]Policy Management and ITA do not support SpIprobes.

[3]Applies to policies created for ITA using link, node, and application dimensions, and to policies created for ACE using node dimensions.

[4]IPI supports its own node groups; contact Customer Support for more information.

[5]Refer to the Iris Application System Compliance documents for details about protocol support for specific Iris applications for each probe type.

Iris Alarm Types

The IrisView Alarm application provides critical information on the performance of provisioned network elements through the use of Alarm Policies you define for different Iris applications. With Alarm Policies, you can establish a set of guiding principles to manage the KPI threshold configuration to optimize the performance of network elements. You can perform the following tasks:

- Use Policy Management to create templates and configure alarm policies
- Monitor and analyze alarms using the Alarm dashboard

Two types of alarms are visible in the Alarm dashboard: alarms generated when a user-defined threshold is breached and system-level alarms.

System-Level Alarms

The system-level alarms generated by the Iris system are predefined. You can modify threshold levels and severity settings on the System Alarms tab.

User-Defined Threshold Alarms

Alarms are also generated by the Iris system when the threshold conditions specified in an alarm policy are reached. These alarms are generated in response to user-defined conditions, and their name is the one you specify for the policy. You can

create alarm policies for various Iris applications.

Absolute and Relative Condition Alarms

User-defined threshold alarms fall into the following categories, depending on the condition type:

- Absolute Alarms - alarms where the condition is set in absolute terms using Boolean expressions, such as greater than or equal to. For example, if you set a condition of >10%, an alarm is triggered when the KPI value exceeds 10%.
- Relative Alarms - alarms where the condition is set relative to a percentage or value of a previous period, day, week, or 4 weeks. For example, if you set a condition of +/-5% relative to the previous day, a relative alarm is triggered when the KPI value is 5% greater or 5% lower than the previous day. See Relative Percentage Alarm Example for an example of a relative percentage alarm.

Aggregate Alarms

Aggregate alarms enable you to increase the alarming over longer periods than the aggregation period of a KPI. You can configure Aggregate alarms in a Tumbling window mode or in a Sliding window mode.

- Tumbling Window Mode - Enables monitoring alarms every few minutes, hourly, or daily. For instance, if you set an IPI alarm aggregation window to 1 hour and the sample interval to 1 hour, a new measurement will be started every hour and will aggregate for 1 hour. The measurements are contiguous, not overlapping.
- Sliding Window Mode - Enables monitoring alarms over the same fixed time width every aggregation period; the fixed width of time is the sliding window. For example, if you set the aggregation window to 15 minutes and the sample interval to 5 minutes, then every 5 minutes a new measurement will be started and will continue to aggregate for 15 minutes.

Low Data Volume Alarms

You can configure LDV alarms to detect when certain elements or network dimensions (for example, HVAs, VLANs, URLs, and APNs) have sent less than a threshold of data (including zero) traffic during a certain time period. You can also disable these alarms from being triggered, such as during planned network outages; see the Policies tab for details.

Alarm States

You clear and acknowledge alarms in the Alarm Browser. By default, alarms are automatically acknowledged when they are cleared but this setting can be changed by Tektronix to make these alarm states independent of each other.

- Acknowledged - You can acknowledge user-defined and system-level alarms independently of their Cleared status. You cannot acknowledge alarms that have already been acknowledged.
- Cleared - You can clear user-defined and system-level alarms independently of their Acknowledged status. You can set a threshold for user-defined alarms to clear automatically; system-level alarms may clear on their own. You cannot clear alarms that have already been cleared.
- You can add a comment to any alarm, independent of its status, including those that are neither acknowledged nor cleared. The comments are visible in the Alarm History table when you expand an alarm in the Alarm Browser.
- Both user-defined and system-level alarms are automatically removed from the database after 180 days; the length of time is configurable by Tektronix. **Note**: Alarms generated by SNMP test traps are not stored in the database.

Alarm Severity

Each alarm has a severity associated with it. The severity is predefined for system-level alarms. For user-defined alarms, you configure the severity when you define the policy.

- Critical
- Major
- Minor
- Informational

Configuring Relative and Absolute Alarms

Iris enables you to set the following types of Absolute and Relative alarms on the Conditions and Assignment Editor window. Service-based IPI absolute and relative alarms are visible in FastPath and in the Alarm dashboard. For more details, see IPI Alarm Types.

Alarm Type	Condition	Trigger an Alarm when KPI Measurement...
• Absolute	<	Is less than the threshold value or percentage.
	>	Is greater than the threshold value or percentage.
	=	Is equal to the threshold value or percentage.
	<=	Is less than or equal to the threshold value or percentage.
	>=	Is greater than or equal to the threshold value or percentage.
	!=	Is not equal to the threshold value or percentage.
• Relative %- Previous Day • Relative % - Previous Week • Relative % - Previous 4 Weeks • Relative % - Previous Period • Relative Value - Previous Day • Relative Value - Previous Week • Relative Value - Previous 4 Weeks • Relative Value - Previous Period	Greater than	Is greater than the threshold value or percentage of the previous period, day, week, or 4 weeks. The period is equal to the time selected in the Aggregation window.
	Greater than or Equal to	Is greater than or equal to the threshold value or percentage of the previous period, day, week, or 4 weeks.
	Less than	Is less than the threshold value or percentage of the previous period, day, week, or 4 weeks.
	Less than or Equal to	Is less than or equal to the threshold value or percentage of the previous period, day, week, or 4 weeks.
	Outside of +/-	Is outside the threshold value or percentage of the previous period, day, week, or 4 weeks.
	Outside of or Equal to +/-	Is outside or equal to the threshold value or percentage of the previous period, day, week, or 4 weeks.

To Configure Relative or Absolute Alarms

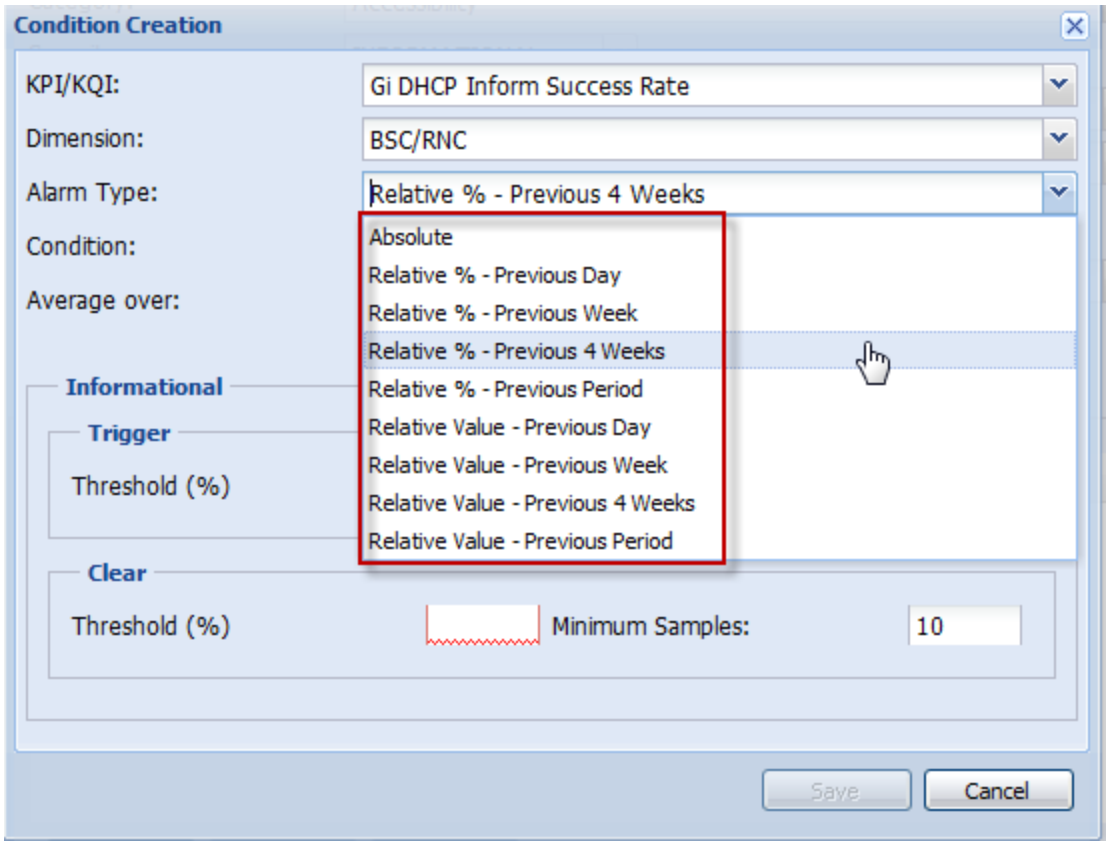
Use the following workflow in the Conditions area to add absolute or relative alarm conditions to an existing or new policy.

1. Click the **Add** button to open the **Condition and Assignments Editor**.
2. Select the **KPI/KQI**. The available KPI/KQI values depend on the Interface you selected for the template.
3. Select the alarm **Type** as Absolute or select one of the relative types; then select a corresponding comparator from the **Condition** menu.
4. If you selected a relative alarm type, select in the **Average over** menu the number of periods to use in the alarm averaging calculation.

5. In the **Trigger Threshold** field, complete one of the following tasks:
   - For an Absolute alarm, enter a value or a percentage depending on the KPI or KQI you selected.
   - For a Relative alarm, enter a value or percentage to use as a measurement against the previous period, day, week, or 4 weeks. If you enter a percentage, use the whole value. For example, if you wish to use 50%, enter 50 instead of .5 in the field. See Relative Percentage Example for more information on Relative Percentage alarm configuration.
6. If you selected a volume KPI for the condition, enter in the Trigger Threshold **Minimum Samples** field the minimum number of samples that must be received before an alarm is eligible for triggering.
7. If you selected the **Auto Clear** option in the Policy Details, complete the following tasks:
   - In the **Clear Threshold** field, enter the threshold for automatically clearing the alarm.
   - In the **Minimum Samples** field, enter the minimum number of samples that must be received before an alarm is eligible for autoclearing.
8. Select the **Dimension** for the condition. The available dimensions depend on the KPI/KQI you selected.
9. To add more conditions, repeat the previous steps; then click the **Save** button to save the changes to the template.

Alarm Policy Conditions Example

The following example shows the available absolute and relative alarm types.



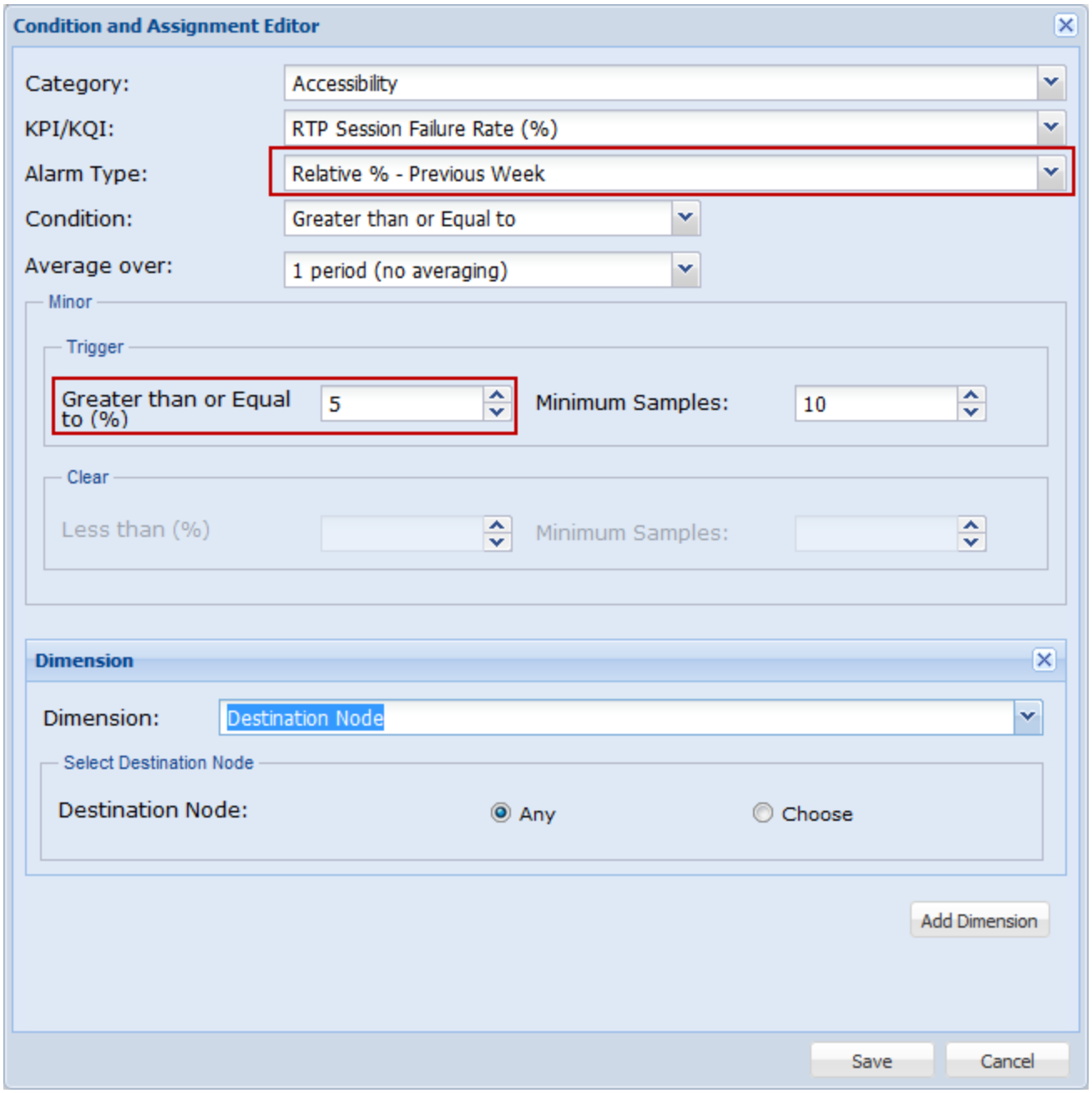
Iris Relative Percentage Alarm Example

Relative Alarms are alarms where the condition is set relative to a percentage or value of a previous period, day, week, or 4 weeks. For example, if you set a condition of +/-5% relative to the previous day, a relative alarm is triggered when the KPI

value is 5% greater or 5% lower than the previous day. When you configure Relative percentage alarms, remember the percentage is relative to the previous period or the same period the previous day, week or month.

For example, in the screen shot below , the Alarm Type is set to trigger when the RTP Session Failure Rate is greater than or equal to 5% relative to the previous week. So if the Failure Rate last week measured at 2%, then measured at greater than or equal to 2.1% this week for the same sample period, the alarm will trigger.

The formula is 2% * trigger (1.05%) = 2.1%.



Configuring Aggregate Alarms

Alarm aggregation enables you to increase the data resolution for ITA and IPI alarms above the entry level so you can support hourly and daily KPIs. Aggregation can help avoid alarms on a single session failure, so that alarms can be used to identify outages that affect many users and sessions. You configure alarm aggregation in the Policies tab of the Policy Management dashboard using the Aggregation Window and Sample Interval options.

Aggregate Alarm Modes

You can configure Aggregate alarms in a Tumbling window mode or a Sliding window mode.

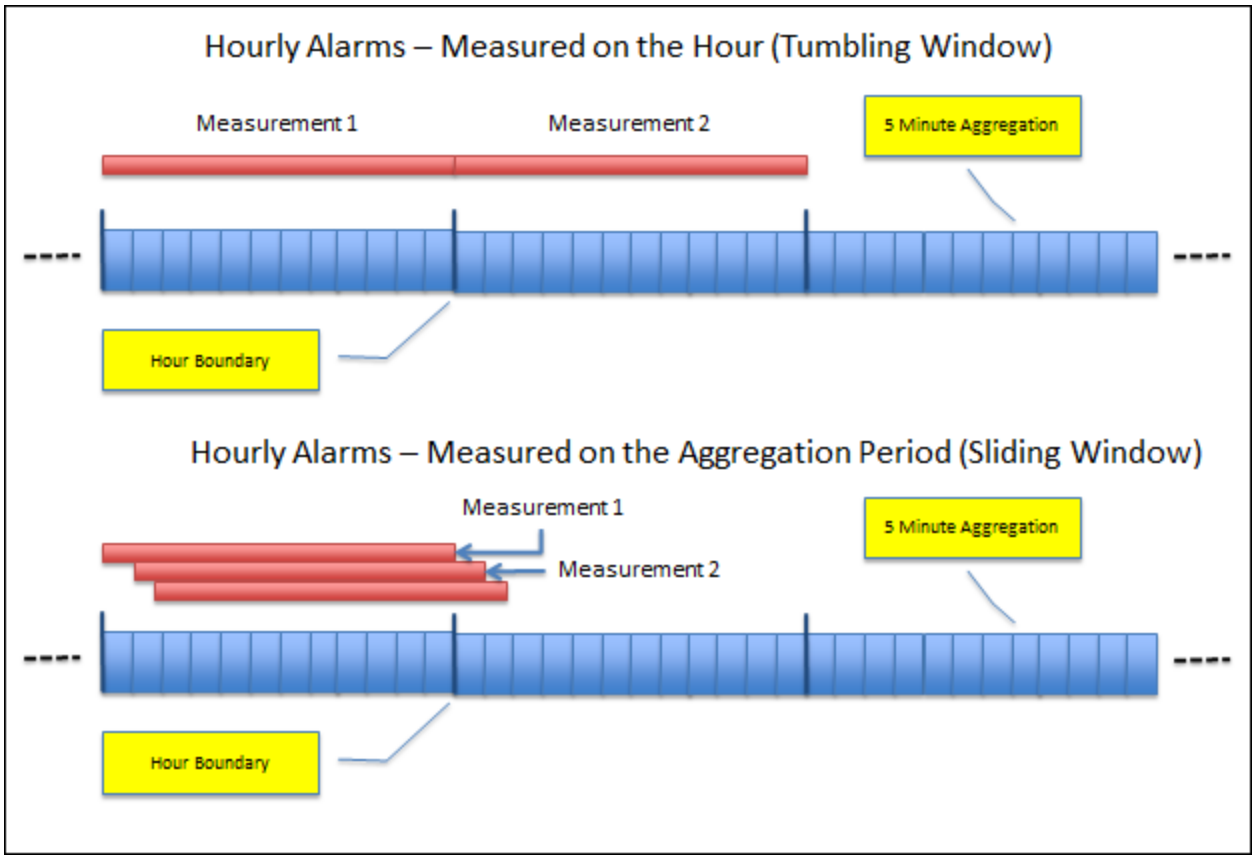
- When the Aggregation Window and the Sample Interval fields have the same value, the Aggregate alarm is said to be in a Tumbling window mode.
- If you decrease the value of the Sample Interval below the value of the Aggregation Window, the Aggregate alarm is said to be in a Sliding window mode.
- You can view IPI Aggregate alarms in FastPath.

Tumbling and Sliding Window Settings

Application	Aggregation Window	Sample Interval	
		Tumbling Window	Sliding Window
ITA	1 minute (default)	1 minute	none
	5 minutes	5 minutes	1 minute
	10 minutes	10 minutes	1, 2, 5 minutes
	15 minutes	15 minutes	1, 3, 5 minutes
IPI	5 minutes (default)	5 minutes	none
	10 minutes	10 minutes	5 minutes
	15 minutes	15 minutes	5 minutes
	1 hour	1 hour	5, 10, 15 minutes
	2 hours	2 hours	15, 30 minutes, 1 hour
	4 hours	4 hours	1, 2 hours
	6 hours	6 hours	1, 2 hours
	12 hours	12 hours	1, 2, 4, 6 hours
	24 hours	24 hours	2, 4, 6, 12 hours
ACE	1 minute (default)	N/A	N/A

Hourly Aggregate Alarms Example

The following graphic shows an example of an hourly alarm measured using a Tumbling window mode (top) and also using a Sliding window mode (bottom).



Iris Alarm Acknowledgement

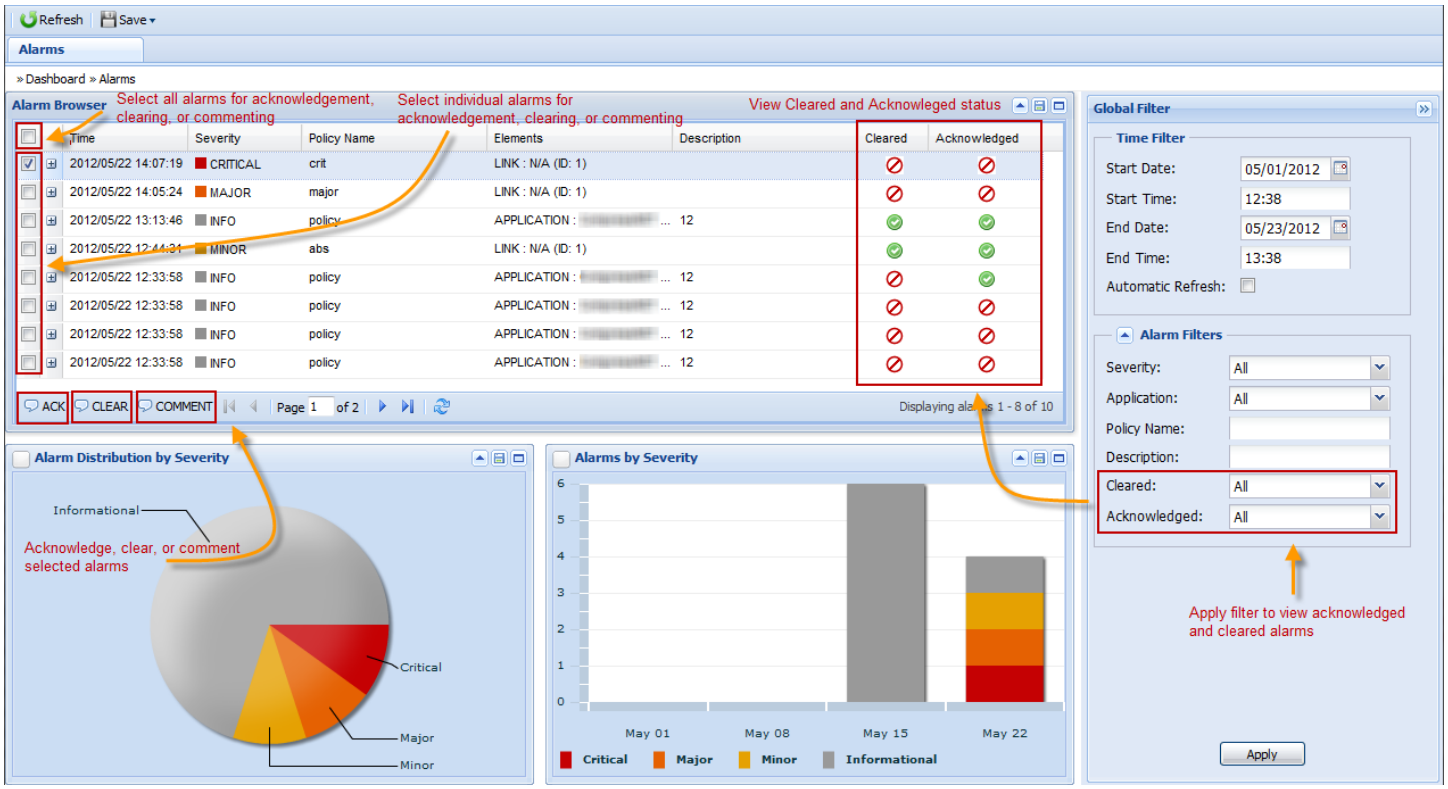
You can acknowledge alarms and monitor them in the Alarm dashboard and FastPath. Both system-level alarms and Iris applications alarms can be acknowledged by users who have an Alarm Acknowledge privilege; contact your Iris system administrator for privilege assignments. You only need an Alarms privilege to view acknowledged alarms.

The following table describes all the components used to acknowledge alarms and monitor acknowledged alarms.

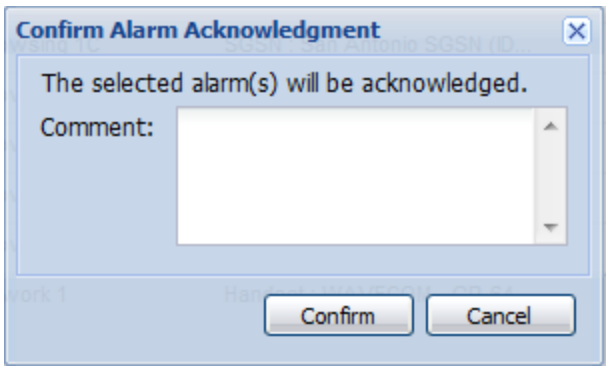
Location	Element	Description
Alarm Browser Table	Check Box Column	You must have an Alarm Acknowledge privilege to view the Check Box column and ACK button: • Click the top check box to select all alarms or click individual check boxes to select one or more alarms. • The ACK button at the bottom of the column becomes active when at least one acknowledge check box is selected. • Click the ACK button to acknowledge the selected alarms. You can enter a comment in the Confirm popup. • When you acknowledge an alarm, the icon in the Acknowledged column changes to a green check mark; the time stamp does not change. • You cannot remove an alarm acknowledgement nor acknowledge the same alarm more than once. • An email can be sent when a policy-based alarm is acknowledged (manually or automatically); contact Tektronix to enable this feature.
Alarm Browser Control Button	ACK Button	
Alarm Dashboard	Confirm Alarm Acknowledgement Dialog Box	This confirmation prompt appears when you click the ACK button. • Enter an optional comment to provide more details about the acknowledgement. • Click Confirm to confirm you want to acknowledge the alarm.
Alarm Browser Table	Acknowledged Column	Contains an icon indicating whether the alarm has been acknowledged. When you acknowledge an alarm using the ACK button, the icon in this column changes to a green check mark.
Alarm Browser Expanded Description	Alarm History Table	The Alarm History table provides a timestamp of when an alarm was acknowledged and by whom, as well as any comments that were made. • Alarms are automatically acknowledged when you clear them, and these are identified with an "Auto-Acknowledge" comment; contact Tektronix to disable this setting. • For acknowledged alarms, the history indicates if the acknowledgement was due to auto clearing or to manual clearing.
Alarm Dashboard Global Filter	Acknowledged Drop-Down Menu	Select All to view all acknowledged alarms, Yes to view only acknowledged alarms, or No to view only alarms that have not been acknowledged. When you click the Apply button only alarm data that fits this criteria appears in the Alarm Dashboard dashlets and browser.

Alarm Acknowledgement

In the following graphic, only users with Alarm Acknowledge or Alarm Clearing privilege can use the Check Box column. Only those with Alarm Acknowledge privilege can use the ACK button.

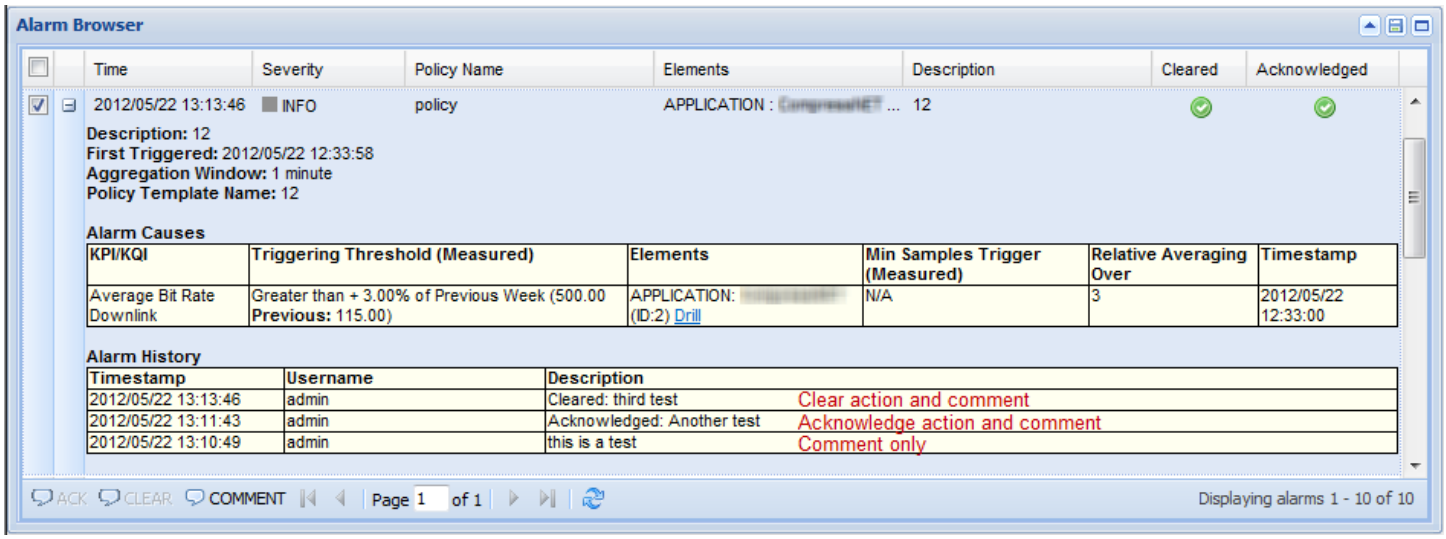


Confirm Alarm Acknowledgement



Alarm Acknowledge History

The following graphic shows a historical log of alarm events, including an alarm acknowledgement event and its associated comment.



Iris Alarm Clearing

You can clear alarms and monitor them in the Alarm dashboard and FastPath. Only users who have an Alarm Clearing privilege can manually clear alarms; contact your Iris system administrator for privilege assignments. You can configure automatic clearing of policy-based alarms if you have the Alarms Admin privilege. You only need an Alarms privilege to view the Cleared alarms status.The IrisView Network Maps data is updated automatically when alarms are cleared; only uncleared alarms are shown in maps.

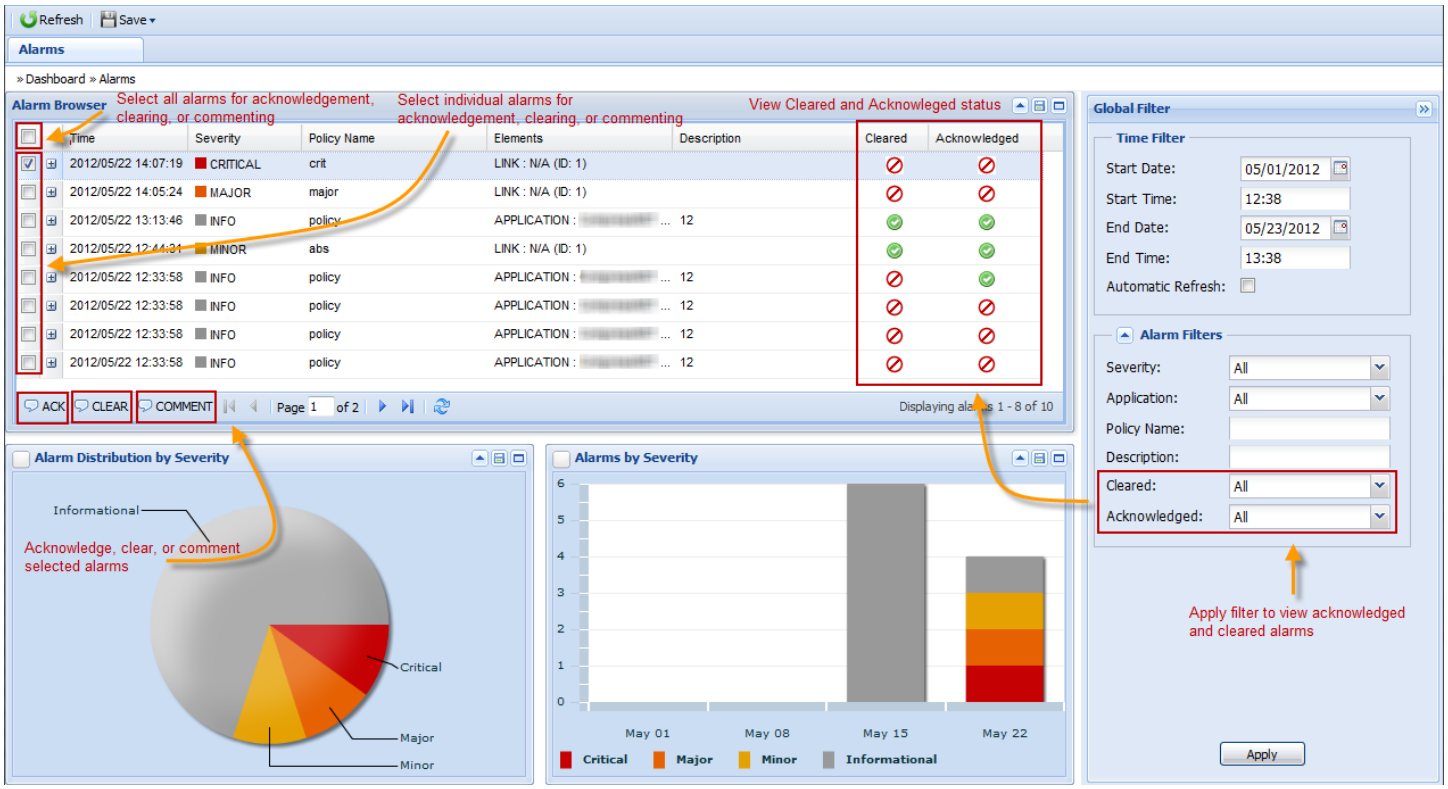
The following table describes all the components used to clear alarms and monitor cleared alarms.

Location	Element	Description
Policy Tab	Auto Clear Check Box	Select this option to enable automatic clearing of alarms that will be triggered when the policy is breached: • When an alarm is triggered, the time is incremented until the clearing threshold is reached. • You cannot overlap the clearing and triggering thresholds. • The Alarm Clearing privilege is not needed to set Auto Clear. • Alarms are automatically acknowledged when they are automatically cleared; contact Tektronix to disable this setting.
Condition Creation Dialog Box	Clear Threshold Field Minimum Samples Field	Use these fields to configure an automatic clear threshold and minimum number of samples to take before auto clearing the alarm.

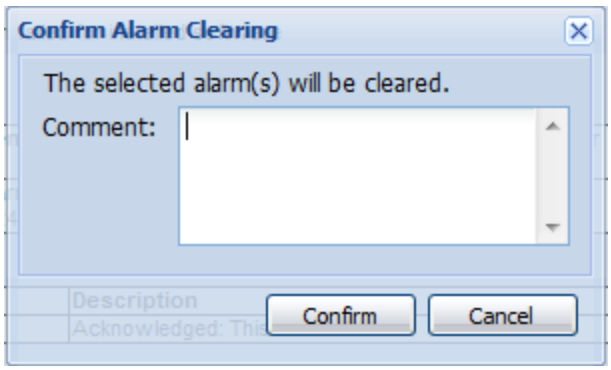
Location	Element	Description
Alarm Browser Table	Check Box Column	You must have an Alarm Clearing privilege to view the Check Box column and CLEAR button: • Click the top check box to select all alarms or click individual check boxes to select one or more alarms. • The CLEAR button at the bottom of the column becomes active when at least one check box is selected. • Click the CLEAR button to clear the selected alarms. You can enter a comment in the Confirm popup. • When you clear an alarm, the icon in the Cleared column changes to a green check mark and the time stamp changes. • Alarms are automatically acknowledged when they are manually cleared; contact Tektronix to disable this setting. • You cannot revert an alarm clearing nor clear the same alarm more than once.
Alarm Browser Control Button	CLEAR Button	
Alarm Dashboard	Confirm Alarm Clearing Dialog Box	This confirmation prompt appears when you click the CLEAR button. • Enter an optional comment to provide more details about clearing the alarm. • Click Confirm to clear the alarm and close the dialog box.
Alarm Browser Table	Cleared Column	Contains an icon indicating whether the alarm has been cleared. When you clear an alarm using the CLEAR button or the alarm clears automatically, the icon in this column changes to a green check mark.
Alarm Browser Expanded Description	Alarm History Table	The Alarm History table provides a timestamp of when an alarm was cleared and by whom, as well as any comments that were made. • Some system-level alarms are cleared automatically and these are identified with an "Auto-clear" comment. • If Auto Clear was configured in the policy that triggered the alarm, the history will show an "Auto-clear" comment, and the user will be "System." • When system-level alarms are cleared by the system, the history will also show an "Auto-clear" comment, and the user will be "System." • For acknowledged alarms, the history will indicate if it was due to auto clearing or due to manual clearing.
Alarm Dashboard Global Filter	Cleared Drop-Down Menu	Select All to view all cleared alarms, Yes to view only cleared alarms, or No to view only alarms that have not been cleared. When you click the Apply button only alarm data that fits this criteria appears in the Alarm Dashboard dashlets and browser.

Alarm Clearing

In the following graphic, only users with Alarm Acknowledge or Alarm Clearing privilege can use the Check Box column. Only those with Alarm Clearing privilege can use the CLEAR button.

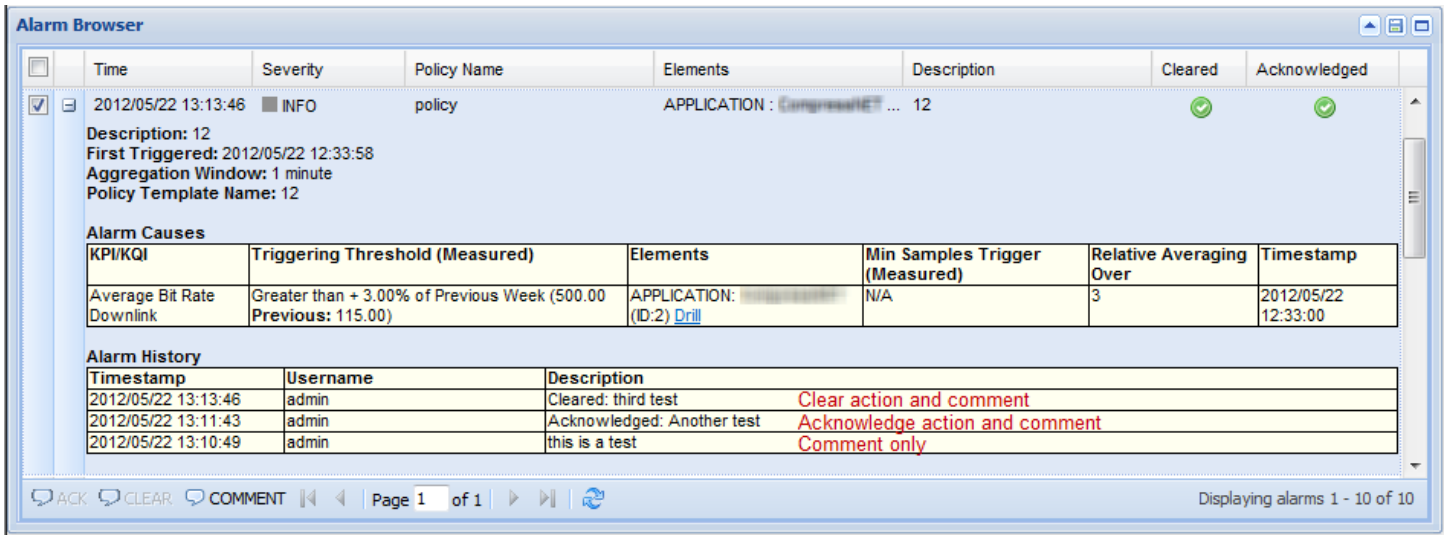


Confirm Alarm Clearing



Alarm Clearing History

The following graphic shows a historical log of alarm events, including an alarm clearing event and its associated comment.



Using Minimum Samples to Cancel Noise

When you create a Policy, you can configure the minimum number of samples (attempts) required before firing an alarm. This means that you can avoid triggering an alarm unless there is an adequate amount of data to validate a real issue that requires an alarm. Policy Management supports separate minimum samples for both alarm threshold triggers and alarm clearing triggers.

Use Cases

During the late night period, when the volume of transactions drops significantly, there is a chance that a KPI can go into a failure state, even if there is no real outage. For example, if there is only 1 transaction during a certain period and it just happens that this 1 transaction is a failure, then the ratio of transactions to failed transactions is 1:1 or 100% failure rate. In most cases, operators will want to see at least 10 transactions over a certain period before they deem it a network issue worthy of dispatching resources to investigate. This feature enables operators to define a minimum number of samples before an alarm can be triggered.

A policy is created with a threshold of 50% failure rate with a minimum of 10 attempts. It is marked as autoclear at 40% with the minimum number of attempts used during the raise automatically being used for the clear. Thus, if the alarm is raised with 65% failure rate and 15 attempts, it cannot be cleared with 35% failure rate and 8 attempts.This feature enables operators to set a minimum number of samples before an alarm can be cleared.

Application

You configure the Minimum samples in Policy Management. This feature has the following characteristics:

- You can only set a number of minimum samples for a threshold trigger for a volume KPI; the Minimum samples field is not active when other types of KPIs are used
- You can only set a number of minimum samples for a clear alarm trigger if you have selected the Auto Clear option in the Policy Details pane
- The default value for samples on new policies is 10 attempts, which is configurable; contact Tektronix Communications Customer Support for changes

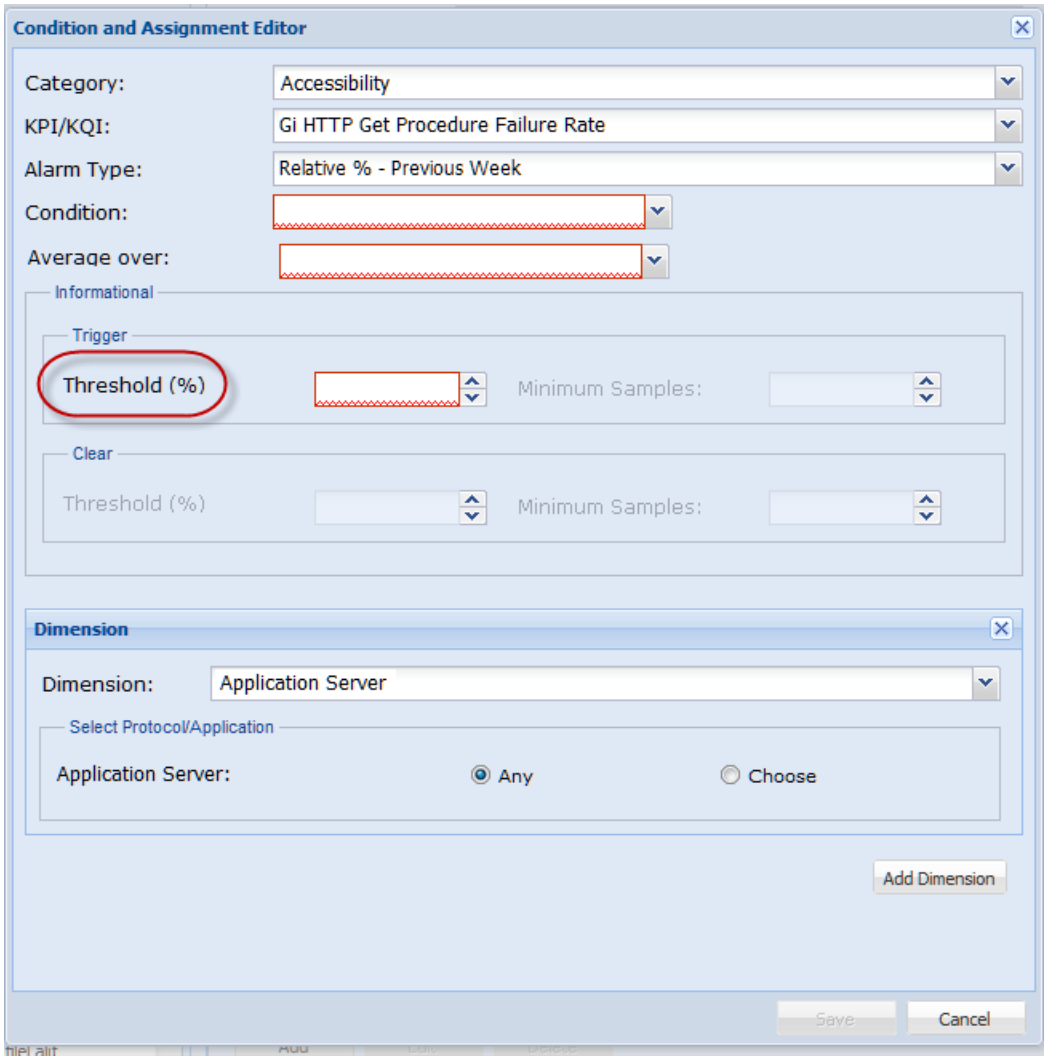
To Configure Minimum Samples in a New Policy

1. From IrisView, hover your cursor over the **Alarms** button and select **Policy Management** from the submenu.
2. Click the **Policies** tab.

3. In the Policies List pane, click the **Add** button and select the Iris application at the prompt. A blank form appears in the Policy Details pane.
4. In the Policy Details area, enter a Name and Description.
5. In the Owner field, select yourself to make the policy private, or Public to share the policy.
6. In the Profile field, select an alarm profile.
7. Select the **Interface** option and then select **Gi** as the interface.
8. Select the Severity and Aggregation parameters.
9. Select the **Auto Clear** check box to enable automatic clearing of the alarm once the minimum number of attempts have been made.
10. Near the bottom of the Conditions area, click the **Add** button to open the Conditions and Assignment Editor window.
11. In the Category field, select **Accessibility**.
12. From the KPI/KQI drop-down menu, select **Gi HTTP Get Procedure Failure Rate**. Choosing a volume KPI enables you to configure minimum samples on its trigger threshold.
13. Select an alarm type and the Condition.
14. If you select a relative alarm type, you must also choose the number of periods to average over.
15. In the **Trigger Threshold** field, enter a threshold value for triggering the alarm, and in the **Minimum Samples** field, change the default value of 10 if needed.
16. In the Clear fields, enter a threshold value for clearing the alarm, and in the Minimum Samples field, change the default value of 10 if needed.
17. Click the Add Dimension to bring up a list of possible dimensions.
18. Click **Save** to save the new condition and return to the Policy Details. The new condition appears in the Conditions area as a summary.
19. Click the expand **(+)** button next to the new condition to show the details in table form.
20. Add more conditions as needed. When done, click the **Save** button near the bottom of the Policy Details window.

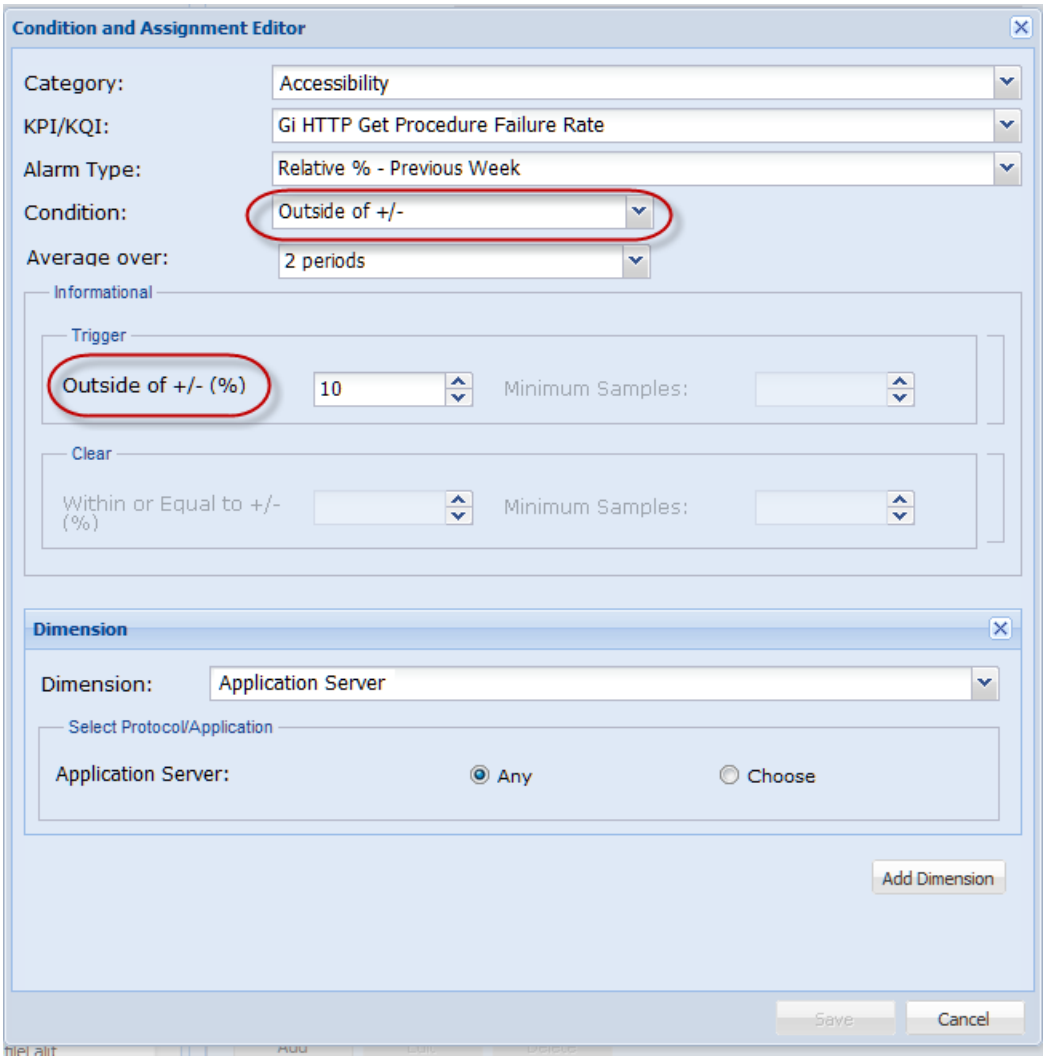
Condition and Assignments - Before Defining Condition and Triggers

The following graphic shows the original Threshold labels before the condition was selected. The blank fields with red shading indicate mandatory fields. The Informational area indicates that the alarm severity is Informational.



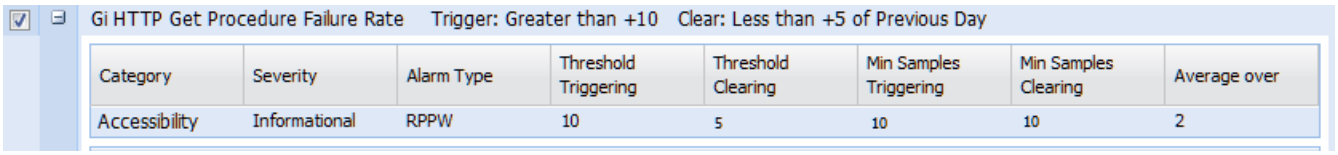
Condition Creation - After Defining Condition and Triggers

The following graphic shows the Threshold labels changed to reflect the condition selected.



Conditions Area in Policy Details Pane - After Saving Condition

The following graphic shows a table containing the Threshold and Minimum Samples values defined in the Condition and Assignments Editor window, as well as the number of periods to average over. The explicit condition is shown in the row above the table.



Configuring Protocol/Application Alarms for ITA KPIs

You can configure ITA alarm policies using specific transactions, responses, and messages KPIs and then assign them dimensions based on a hierarchical selection beginning with a choice of protocol or application. You can also configure ITA alarms using jitter and RTP packet KPIs and then assign them all to VLANs.

Supported KPI Types

KPI Types	Entities	Protocols	Description
Transaction KPIs	Links Servers (nodes)	Protocols used for ITA transactions	You can define policies based on thresholds for transactions within an application protocol. For example, you can set an alarm to trigger using the Number of Failed Transactions KPI for a server, if the number of failed transactions received during the aggregation period exceeds 10.
Number of Responses KPI			Only one protocol/application per condition is allowed because the dependent entities are only unique across the same protocol. To assign different protocols/applications to the same policy for Number of Responses, you need to add a separate policy condition for each protocol in the Policy Templates tab. For example, you can set an alarm to trigger using the Number of Responses KPI, for a server or link, if the number of SIP Response code 503 received during the aggregation period exceeds 100.
Number of Messages KPI	Links	TLS, MSRP	TLS and MSRP alarms are standard ITA KPIs for message counts. MSRP alarms are based on the KPI for the number of sent SEND, REPORT, and response code messages. For example, you can set an alarm to trigger when the number of MSRP REPORT messages received during the aggregation period exceeds 100. Or you can set an alarm to trigger when the number of TLS alerts received during the aggregation period exceeds 1000.
Jitter, MOS, and RTP Packet KPIs	Links	RTP	RTP alarms are standard ITA KPIs for RTP jitter, RTP MOS, RTP packet loss, duplicate RTP packets, and out-of-sequence RTP packets. Each of the RTP KPIs listed in the Dimensions table represents three KPIs: All kinds of traffic, only Audio traffic, and only Video traffic. In addition, "Packet Count with x Jitter Count" also represents multiple KPIs with different jitter ranges, each defined for either audio traffic, video traffic, or both.
Bandwidth KPIs	Links Servers	GTPv0-C, GTPv1-C, GTPv2-C	You can define policies based on thresholds for bandwidth within an application protocol to view the percentage of traffic split across the GTPv0, GTPv1, and GTPv2 control plane protocols. GTP-C alarms are generated when traffic bandwidth: • Surpasses an absolute, pre-configured value • Increases by a pre-configured percentage relative to the previous time interval Transaction-based alarms and statistics are not supported for GTPv0.

Dimension Hierarchy

The assignment of protocol/application-based dimensions to a policy is a hierarchical process. Each secondary dimension depends on the dimension you selected above it and is disabled until you choose the parent dimension. When you select "Choose" or "Choose One," the applicable Dimension choices appear in a list below. When you select one or more items from the list, you enable the secondary dimension below it in the hierarchy. Each succeeding option depends on the choices you made previously. For example, the list of Transaction Types will contain only the entities specific to the Protocol/Application dimension you selected.

Supported KPIs and Dimensions

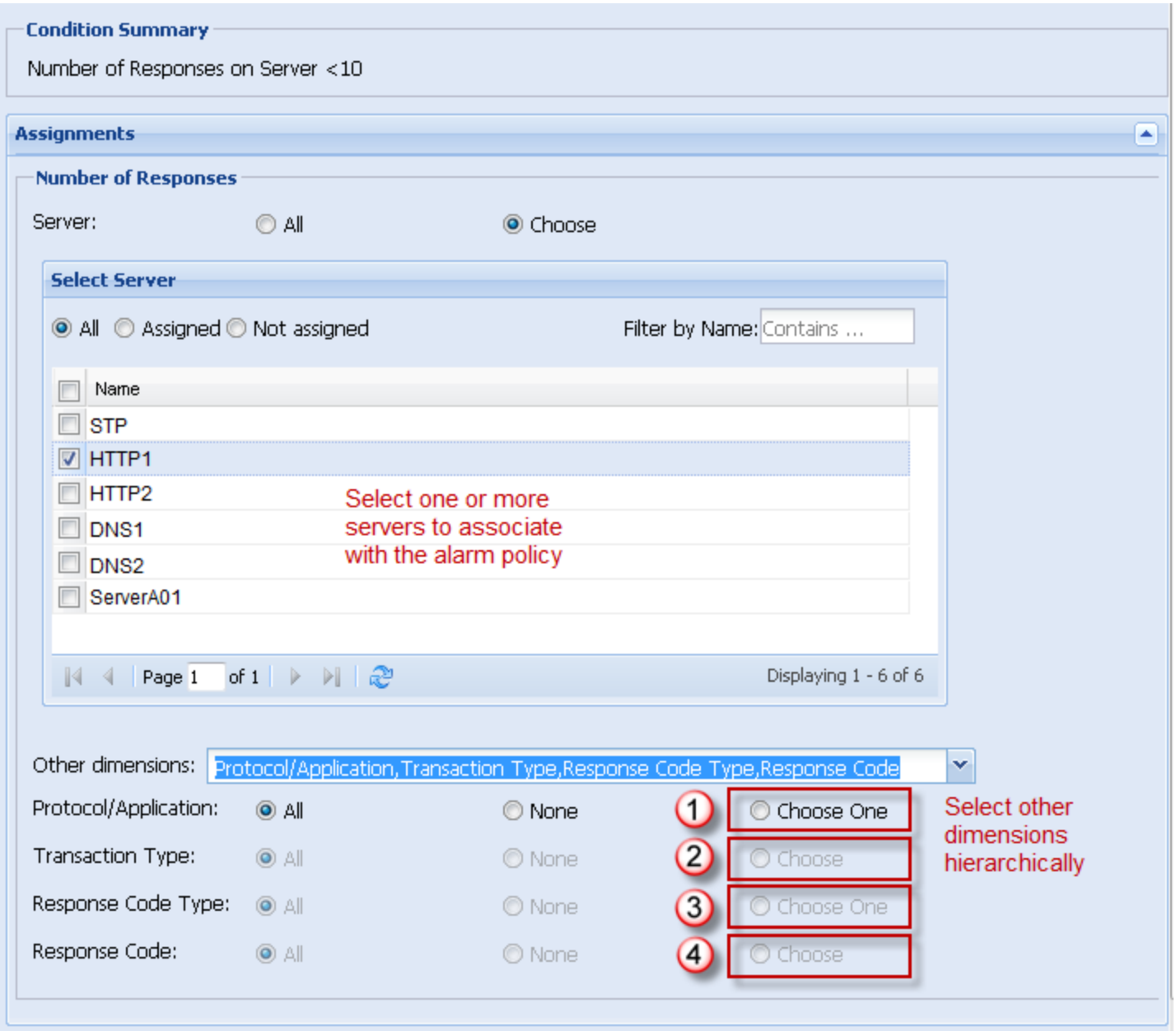
The following table lists the dimensions supported by specific KPIs; the list in the Dimensions Hierarchy column is hierarchical. The list of protocols/applications contains the union of protocols/applications configured for all selected servers

(nodes) or links. For the RTP jitter and packet KPIs, the RTP protocol is already selected and the only other dimension you can add is VLAN.

KPI Category	Supported KPIs	Dimensions Hierarchy
Server (Node)	• Number of Failed Transactions • Number of Timeout Transactions	1. Protocol/Application 2. Transaction Type
	• Number of Responses	1. Protocol/Application (select only one) 2. Transaction Type 3. Response Code Type (select only one) 4. Response Code
Link	• Number of Transactions • Number of Failed Transactions • Percent Failed Transactions • Number of Timeout Transactions • Percent Timeout Transactions	1. Protocol/Application 2. Transaction Type
	• Number of Messages	1. Protocol/Application (only MSRP and TLS) 2. Message type
	• Number of Responses	1. Protocol/Application (select only one) 2. Transaction Type 3. Response Code Type (select only one) 4. Response Code
	• Average Jitter Time for All Bins - x traffic • Packet Count with x Jitter Count - x traffic • Percent RTP Loss Packet - x traffic • Percent RTP Duplicate Packet - x traffic • Percent RTP Out Of Sequence Packet - x traffic • Avg MOS for all Bins - x traffic	1. Protocol/Application (RTP is implied; no selection needed) 2. All VLAN

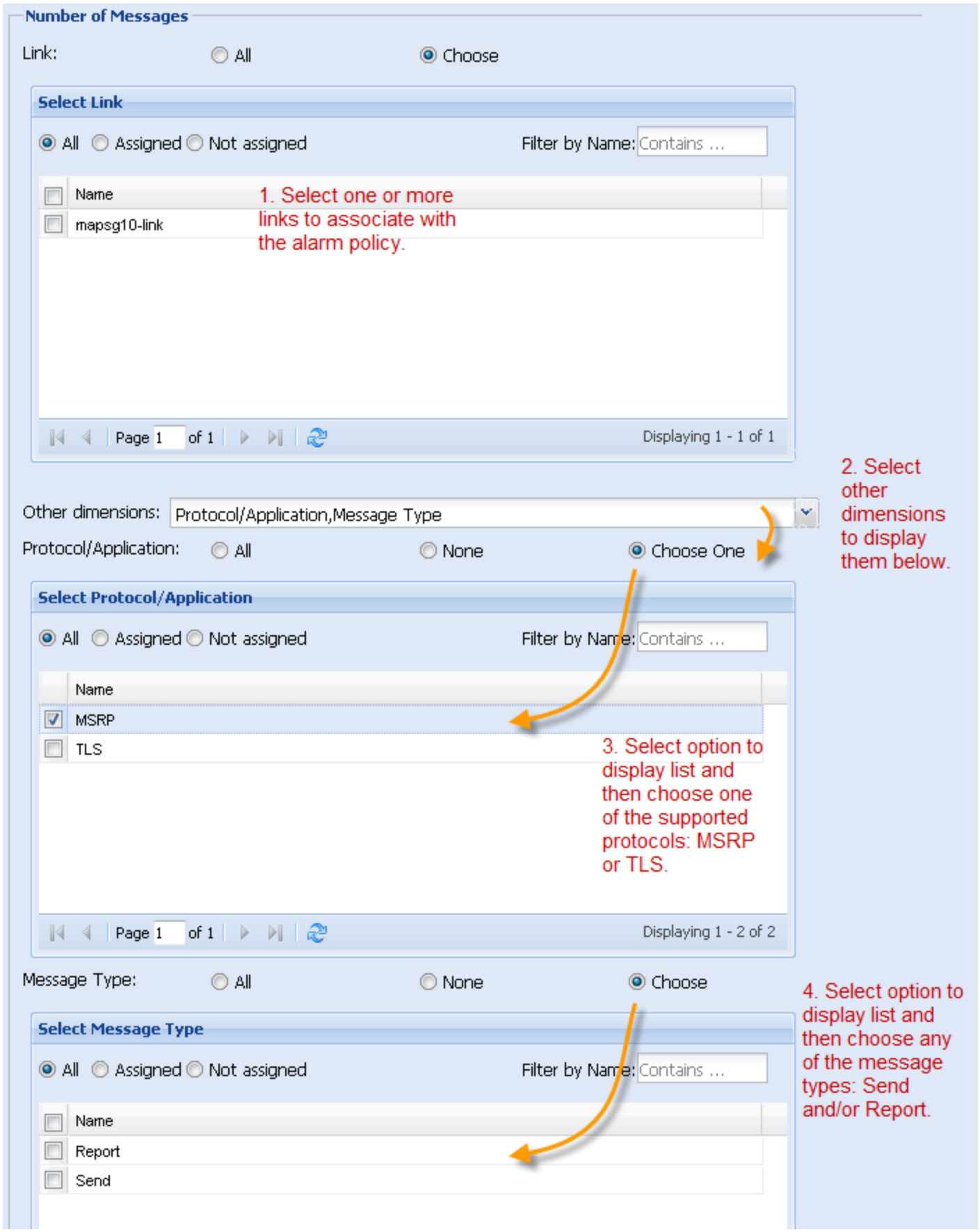
Number of Responses Example

The following example shows the dimensions that can be assigned to a policy based on the Number of Responses on a Server. As you select each Choose option in the order indicated, the list of supported elements appears.



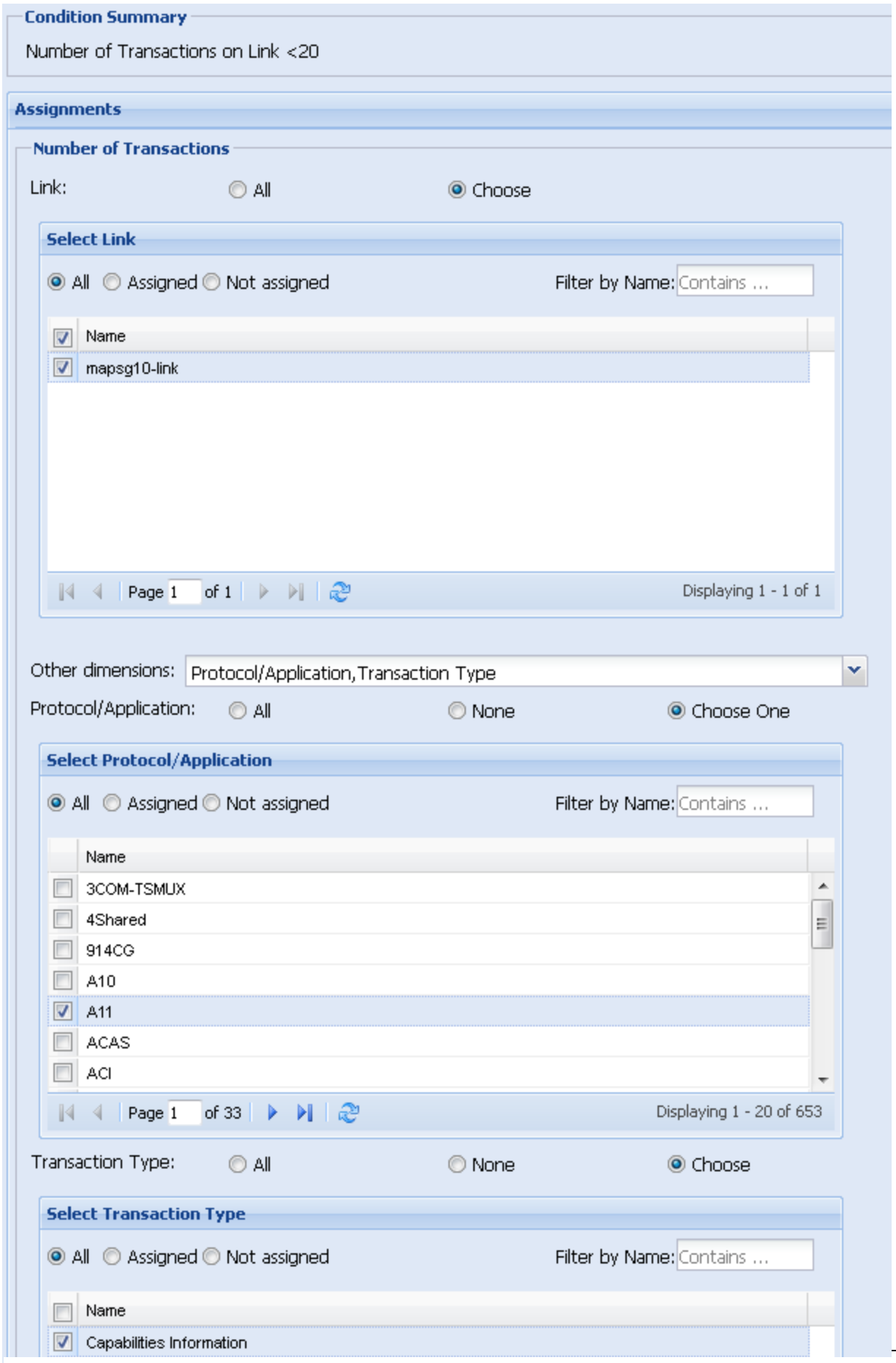
Number of Messages Example

The following example shows how to assign dimensions to a policy based on the Number of Messages on a Link.



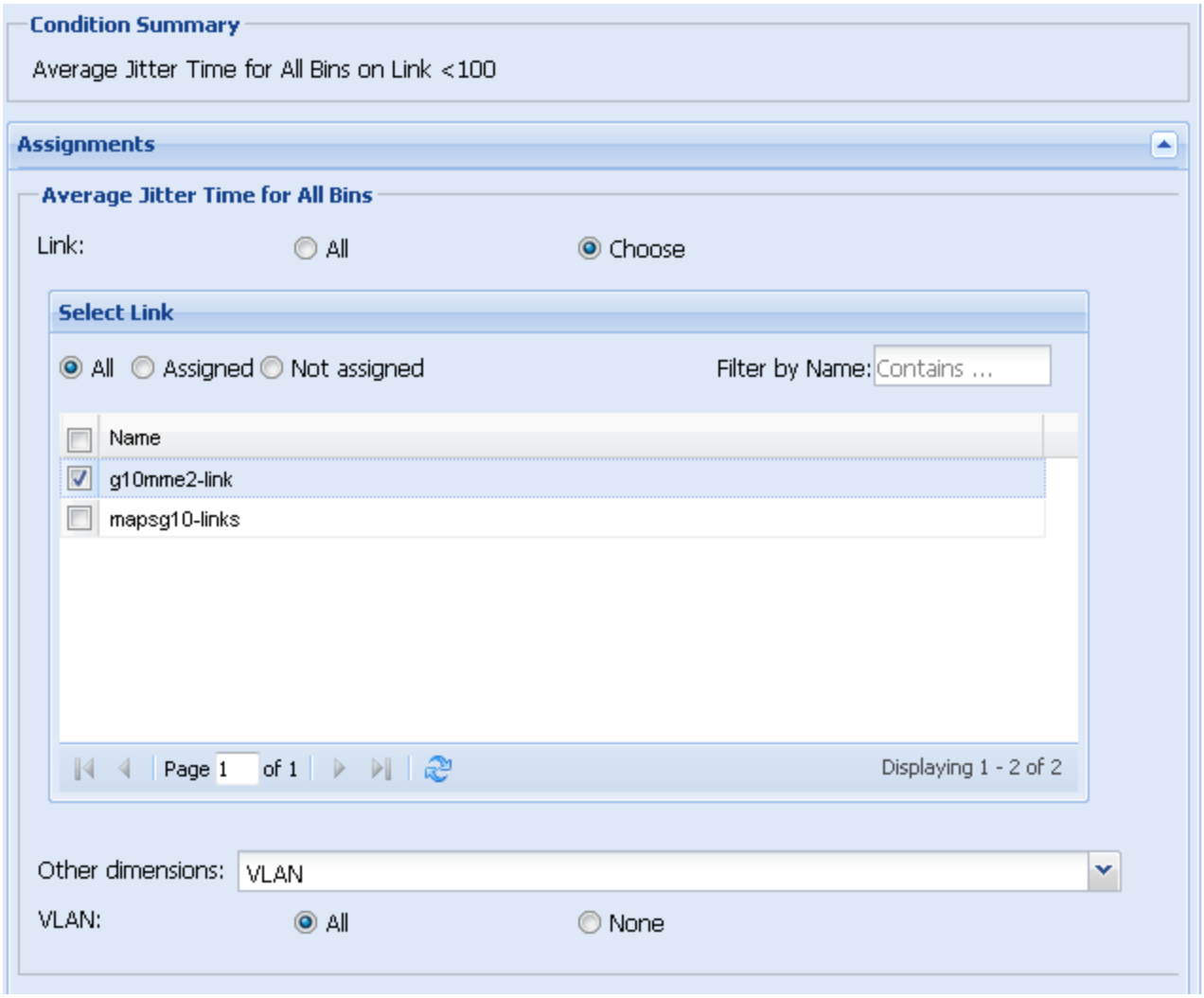
Number of Transactions Example

The following example shows the dimensions that can be assigned to a policy based on the Number of Transactions on a link.



Average Jitter Time for All Bins Example

The following example shows the dimensions that can be assigned to a policy based on the Average Jitter Time for All Bins KPI on a link.



Exporting Iris Alarms

Iris can be configured to periodically export alarm data to CSV files. To enable this feature or change default values, you must contact Customer Support. The Export Alarm capability has the following parameters.

Parameter	Default Value	Description
Aging of Exported Alarm Files	7 days	Indicates number of days to keep the Alarm Export CSV files before they are deleted. The minimum Aging value is 1 day and the maximum is 365 days.
Export Interval	Every 15 minutes	Indicates how often to export alarms. The interval can be changed to every 5 minutes or every hour. It is not recommended to use daily intervals.

Parameter	Default Value	Description
Export Delay	1 minute	Indicates how long to wait after the set interval before exporting. This setting allows you to include alarms that arrive slightly later than the start of the export interval. The delay can be set up to a maximum of 5 minutes.
Export Enabled/Disabled	Disabled	Indicates whether export will be performed automatically.
Export Directory	/data/alarms/	The system will only export alarm data to the Iris user's home directory. You can specify a different path under the home directory.

Export File Name Convention

Once the export is enabled, the system starts generating the files every 15 + 1 minutes and saves them to the Iris server at home/iris/data/alarms. When a file ages past 7 days, it is automatically deleted from the system. The file name of the exported files will contain the start time and end time of the export in the format:

ALARMS-YYYYMMDD-HHMMSS-YYYYMMDD-HHMMSS.csv

Where

- YYYYMMDD is the start or end date
- HHMMSS is the start or end time

For example, the following CSV file was generated on August 25, 2011 at 10:56 am and contains alarm data starting from August 25, 2011 at 10:40 am. The file was stored at /home/iris/data/alarms.

ALARMS-20110825-104011-20110825-105611.csv

File Syntax

The generated files are comma delimited and double quote enclosed. The last column (representing Alarm Causes) is a JSON string representing the list of Alarm Causes, each containing a list of elements. Within the Alarm Cause JSON, if an attribute does not apply or is not available, the attribute will not be present. You will need to parse the Alarm Causes using a JSON parsing utility. The values you see in the JSON are dependent on the type of alarm; there are different values for different types of alarms. The following example is for a relative alarm.

Header Field	Example
ID	"283984"
Time(GMT)	"2011/07/19 20:49:50"
First Triggered (GMT)	"2011/07/19 20:49:50"
Severity	"CRITICAL"
Policy Name	"Link Test 2"
Description	"Link Test 2 Increasing"
Acknowledged	"FALSE"
State	"ACTIVE"
Alarm Causes	[{"templateName":"Link Test Template 2 Increasing","kpi":"Average Total Bit Rate Downlink", "baselineType":"RPPP", "operator":"+","threshold":"1.00","measured":"679.33","baselineValue":"598.67", "timestamp":"2011/07/19 20:48:00"," elements":["LINK : N/A (ID: 100)"]}]

Exporting and Importing Alarm Policy Data

You can export Iris alarm policy data to an XML file and also import into Iris an XML file containing policy data created in the same or a different system. This feature enables you to import policy configurations into your own system to update them in bulk.

Export Process

You can export all policies, action templates, and schedule templates in the database to an XML file. The export file includes all policy management configuration settings and has the following default name:

`ALARM_POLICIES_YYYYMMDD_HHMMSS_<TIME ZONE>.xml`

XML Schema

An XML schema, `alarm_policies.xsd`, is provided. You can download this XSD file by clicking on the **More** button in the Policies tab and selecting the **Show XSD** option. This option opens the `alarm_policies.xsd` file within a new browser window.

 Alarm Policy IDs are for internal use only. Do not delete or modify these IDs.

Import Process

When importing policy configurations, you must choose between synchronizing the data or overwriting it. A warning is provided if you select the overwrite option.You cannot create policies while an import/export is in progress. The activity log indicates who started the import and when, plus includes other descriptions.

Import Synchronization

The synchronization of policy configuration data is based on the name of the policy, action template, or schedule template. If there are changes to the configuration of a given imported policy or template but the name of the policy or template is unchanged, the configuration changes will be ignored when you synchronize the imported data.

Examples of Synchronization and Overwrite

Changes to conditions are ignored if the name of the policy was not changed. To recognize the change, you must choose the Overwrite mode. If you change the severity of an alarm in a policy before you import it, the change will only be recognized if you do an overwrite; the synchronization option will ignore the change.

```
<policyTemplate id="8">
  <name>agg5samp1dataRateTemplate</name>
  <severity>CRITICAL</severity>
  <sampleInterval>60</sampleInterval>
  <aggregationWindow>300</aggregationWindow>
  <lastUpdated>2011-11-04T22:37:09Z</lastUpdated>
  <application>2</application>
  <category>3168</category>
  <interfaceType>121</interfaceType>
  <hidden>false</hidden>
  <markToDelete>false</markToDelete>
  <policyConditions>
    <policyCondition id="22">
      <elementType>111</elementType>
      <timeWindow>60</timeWindow>
      <lastUpdated>2011-11-04T22:37:09Z</lastUpdated>
      <kpi>3260</kpi>
      <baselineType>ABS</baselineType>
      <thresholdCompareOp>GT</thresholdCompareOp>
      <threshold>0</threshold>
      <andGroup>2</andGroup>
      <dimOrGrp>DIM</dimOrGrp>
    </policyCondition>
    <policyCondition id="8">
      <elementType>111</elementType>
      <timeWindow>60</timeWindow>
      <lastUpdated>2011-10-31T21:04:22Z</lastUpdated>
      <kpi>3263</kpi>
      <baselineType>ABS</baselineType>
      <thresholdCompareOp>GT</thresholdCompareOp>
      <threshold>0</threshold>
      <andGroup>1</andGroup>
      <dimOrGrp>DIM</dimOrGrp>
    </policyCondition>
  </policyConditions>
</policyTemplate>
```

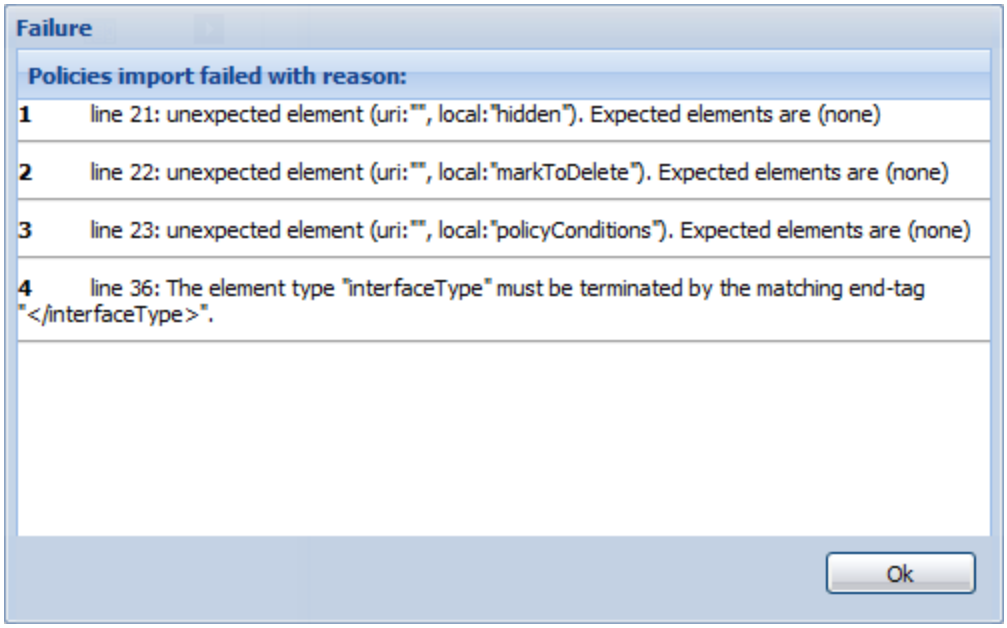
Import Limitation

The database will not be updated if the number of XML items to be saved is greater than 200. If you get this error, you will need to remove some items from the XML file. This limit keeps the browser window size manageable. To change the limit value, contact Customer Support. Also, concurrent imports are not allowed; only one import operation at a time can be performed.

Import Errors

Iris uses several validation layers for the import operation. Logical validation is performed during import. If even one alarm policy has an error, the import cannot be completed. Import errors are logged and enumerated in an error log, so you can fix them. If structural errors are detected on the file, the rest of the errors cannot be enumerated; otherwise, all errors are listed.

Import Error Log



Iris SNMP Alarm Forwarding

The SNMP Alarm Forwarding feature enables you to forward alarms to SNMP-based systems. Iris supports SNMPv2 protocol.

When this feature is enabled, Iris sends SNMP traps in real time over UDP to the defined destination address and port in your network management system. The destination port is used for issuing SNMP Get and Set commands, and it must match the port value used by your management system.

You can forward both policy-based alarms and system-level alarms. Iris uses SNMPv2c protocol to forward alarm data via UDP. The default community string is “public," but you can customize it per your requirements. The SNMP community string is like a user ID or password that allows access to the receiving device.

Policy Based Alarms

You can configure an Iris alarm policy to forward through SNMP all alarms generated when the policy is violated.

- Configure the SNMP destination IP address, port, and community string as an SNMP action in an Action Template in the Policy Management dashboard.
- Add multiple SNMP destinations as different actions.
- Assign them to policies on the Policies tab or to profiles on the Profiles tab.

When a policy associated with an SNMP action is violated, the Policy Manager forwards the alarm data to the appropriate network management system.

See the SNMP Trap Format for Policy-Based Alarms document for more details.

System-Level alarms

- Configure all system-level alarms or select alarms to be forwarded through SNMP on the System Alarms tab.
- When system-level alarms are generated, alarm data is forwarded for only those alarms configured for SNMP forwarding.
- Configure periodic test traps to be forwarded through SNMP to help detect outages.

Updating or Deleting Templates and Policies

You can update or delete policies and templates in the Policy Management dashboard.

- You can only update or delete Policy Management templates if they have not been assigned to policies. If they have been assigned to a policy, you must first delete the policies that use the template. When you delete a template, it is removed from the List pane.
- You can update a policy by modifying its name, description, template, and conditions, but you cannot change its severity or its interface.
- You can delete policies at any time. When you delete a policy it is removed from the Policy List pane.

KPI Studio Alarms

You can create alarm policies, action templates, and schedule templates for KPI Studio alarms, and display the alarms in the Alarm Browser. When creating a KPI Studio policy, you have to select a Studio Model, which is a defined Studio Service Model. Only one Studio Model can apply to a policy and once selected will determine the KPIs and dimensions available for selection on the Conditions and Assignments Editor window. Once a policy is created and saved, you cannot change the Studio Model. If you change the Studio Model **while you are creating** the policy, any existing KPIs and dimensions already configured in the policy will be removed, since they may not apply in the new Studio Model.

Available dimensions and KPIs are listed based on the KPI Studio Service Model definitions. Once you select a Studio Model, the Policy Manager extracts a list of available dimensions and KPIs based on the KPI Studio Service Model definition. The Service Model defines which dimensions are available for alarming and which attribute or attributes of the dimension will be used to aggregate for alarming.

Multiple attributes may be present in a dimension model. The attributes display as separate dimensions in the Policy definition GUI (for example: Path:Name; Path:Direction). When a policy is defined with multiple dimensions combined together (AND condition), the alarm instance will be triggered against the particular instance of each dimension in the policy.

- When viewing a matrix topology which is limited to a subset of the dimensions in an alarm policy, then the alarm can be properly placed in the dashboard.
- If an alarm dashboard topology contains a dimension not present in the policy, then the alarm will not be shown in the matrix or alarm dashlets.
- For an alarm to be shown in a matrix alarm chart or alarm trend chart, the alarm must contain at least the dimensions present in the defined matrix topology. This allows the higher levels of the tree to be a roll-up count of the lower levels.
- Any global filters applied to the dashboard can likewise remove policies from consideration in the matrix or alarm charts. The policy alarms must be defined with all dimensions in the topology AND the global filters to be shown in the matrix.
- A count will be shown in the GUI indicating the number of policies matching the current set of dimensions/filters in the dashlet. If the user changes a filter, it may reduce or increase the number of policies applicable to the dashlet.

For more information about KPI Studio, please refer to the ***KPI Studio System Administrator's Guide*** and the ***KPI Studio User Guide***.

Best Practice in Creating KPI Studio Alarms

It is best to create policies that include all dimensions which may appear together as a single topology combination in a KPI Studio dashboard. This will ensure that when an alarm occurs, it can be properly placed in the topology tree hierarchy. Otherwise the alarms will not be visible in the specified topology matrix.

When two KPI conditions of the same dimension are use the AND condition, the same dimension instance must cross both KPI thresholds for the alarm to trigger. In the following example, KPI 1 and KPI 3 must both cross the threshold for the same PGW node while KPI 2 crosses for a handset type.

KPI1 > 3% for PGW

AND

KPI2 > 10% for Handset

AND

KPI3 > 1200 for PGW

If some dimension types appear in several conditions with the AND condition, then an alarm is generated only against the elements selected for all conditions within that AND group even if the traffic data for the rest of the alarms is delivered.

When you delete a KPI or dimension definition, the policies referring to that KPI or dimension are also deleted (or are hidden, depending on the policy implementation decision) even if the policy contains KPIs and dimensions that are still valid. You will see a warning that alerts you to the impact of deleting the KPIs and dimensions before you proceed. All previous alarms in the alarm browser will remain unchanged and viewable.

System-Level Alarms

What's New in System-Level Alarms for 7.13.2

The following table summarizes updates to the Iris system-level alarms.

Alarm	Updates	Severity	Alarm Description
DATAFEED-101	New alarm	Critical	DataFeed probe TCP connection failure (per probe-bladeId-receiver)
DATAFEED-102	New alarm	Major	Number of dropped IP flow records (per probe-bladeId_instance-receiver-policy) exceeds threshold
DATAFEED-103	New alarm	Major	Number of dropped mobile flow records (per probe-bladeId_instance-receiver-policy) exceeds threshold
IPB-101	Moved from IPB Guide to online help	Informational	IPB configuration settings have been modified
IPB-102	Moved from IPB Guide to online help	Informational	A user has logged into the IPB console
IPB-103	Moved from IPB Guide to online help	Informational	A user has logged out of the IPB console
IPB-104	Moved from IPB Guide to online help	Minor	A user's login to the IPB console fails
IPB-105	Moved from IPB Guide to online help	Informational	The port identified in the alarm is active
IPB-106	Moved from IPB Guide to online help	Major	The port identified in the alarm is down
IPB-107	Moved from IPB Guide to online help	Major	Power supply 1 is not working properly
IPB-108	Moved from IPB Guide to online help	Informational	Power supply 1 recovers and is working properly
IPB-109	Moved from IPB Guide to online help	Major	Power supply 2 is not working properly

Alarm	Updates	Severity	Alarm Description
IPB-110	Moved from IPB Guide to online help	Informational	Power supply 2 recovers and is working properly
IPB-111	Moved from IPB Guide to online help	Major	IPB chassis air temperature is operating above normal acceptable range
IPB-112	Moved from IPB Guide to online help	Informational	IPB chassis air temperature resumes operating in acceptable range
IPB-113	Moved from IPB Guide to online help	Informational	IPB trigger event has occurred
IPB-114	Moved from IPB Guide to online help	Informational	Dedicated vMesh port identified in the alarm changes status
IPB-115	Moved from IPB Guide to online help	Informational	Chassis module has been removed from the IPB

The following system-level alarms are generated by Iris and appear in the Alarms Dashboard.

- BASE Alarms
- DATAFEED Alarms
- IFC Alarms
- IIC Alarms
- IPB Alarms
- ISA Alarms
- ITA Alarms
- LTE Mapper Alarms
- OAM Alarms
- Probe Alarms
- S2D Alarms
- SAMTCE Alarms
- SR2D Alarms
- TD140 Alarms
- XDR Alarms

BASE Alarms

The following system-level alarms are generated by Iris and appear in the Alarms Dashboard.

BASE-101 Application aborted

Probable Cause	A probe application has crashed or timed out.
Recommended Action	If alarm persists, contact Customer Support for additional diagnostics and debugging.
Severity	Critical
Element	Application
Value	Signal

BASE-110 Application high CPU occupancy

Probable Cause	Probe is over capacity.
Recommended Action	If alarm persists, contact Customer Support.
Severity	Major
Element	Application
Value	CPU occupancy percent
Alarm trigger default	90% CPU occupancy
Alarm clear default	85% CPU occupancy

BASE-150 Hardware failure

Probable Cause	Alarm triggers for following issues, indicated in alarm text: • BIOS RAM Error when IAP100/IAP200 boots up and does not see expected amount of memory. • 1G Fabric or 10G Fabric backplane error
Recommended Action	For BIOS RAM error: 1. Reseat memory. 2. If alarm persists, replace IAP100/IAP200. For 1G Fabric or 10G Fabric backplane error (single chassis): 1. Reseat the IAP100/IAP200. 2. If alarm persists (could be delayed several hours), replace IIC. For 1G Fabric or 10G Fabric backplane error (multi-chassis): 1. Check the inter-chassis fiber cabling. 2. If alarm persists, replace the board reported in alarm.
Severity	Critical
Element	Hardware
Value	N/A

BASE-160 System Alarm (Minor)

Probable Cause	Alarm reports what element is in alarm and applicable hardware details (such as cage, slot, and port).	
Recommended Action	Varies depending on element in alarm:	
	Element	***Action***
	SHMM Failover	None. If alarm persists, contact Customer Support.
Severity	Minor	
Element	Hardware	
Value	N/A	

BASE-161 System Alarm (Major)

Probable Cause	Alarm reports what element is in alarm and applicable hardware details (such as cage, slot, and port).	
Recommended Action	Varies depending on element in alarm; refer to following information.	
	Element	***Action***
	SHMM Failure (cage, primary/secondary)	Replace failed SHMM. If alarm persists, contact Customer Support.
	IIC lost system clock sync	• Media Probe (multi-chassis): Check the timing Ethernet cables (SYSCLK ports) between the primary chassis and the expansion chassis. If alarm persists, contact Customer Support. • Single chassis probe: Replace IIC.
	Optical RX/TX dBm	Light transmit/receive is too high or low (-inf indicates no light). Alarm reports: port, TX or RX, current dBm value, dBm threshold value. Check the cabling and SFP reported in alarm: • Current range is too low - Check cabling at port specified in alarm • Current range is too high - Check SFP to ensure it is fully seated. If so, replace SFP.
	Temperature	• Assess lab temperature; check lab cooling system. • Check probes in same rack for temperature alarms; if probes in same rack have temperature alarms, verify power source to rack. • Check for fan alarms
	Fan	Check fan module; if fan speed too slow or not operating, replace fan tray.
	Voltage Levels	Power supply voltage too high or too low; contact Customer Support to analyze cause.
	Power Feed	Power has been interrupted to the probe. • Check that the GREEN LED is illuminated • Check power cabling at rear of G10 chassis • Check rack power source If alarm persists, contact Customer Support.
Severity	Major	
Element	Hardware	
Value	N/A	

BASE-162 System Alarm (Critical)

Probable Cause	Alarm reports what element is in alarm and applicable hardware details (such as cage, slot, and port).

Recommended Action	Varies depending on element in alarm; refer to following information.	
	Element	***Action***
	Intercage connection	Multi-chassis probe: Check inter-chassis cabling connections for ports reported in alarm. Refer to the G10 installation guides for cabling diagrams.
	Redundant Primary LAN	• Check cabling connections for Port A and Port B on PRM100 RTM or PRM200 RTM. • If alarm persists, replace the RTM.
	Optical RX/TX dBm	Light transmit/receive is too high or low (-inf indicates no light). Alarm reports: port, TX or RX, current dBm value, dBm threshold value. Check the cabling and SFP reported in alarm: • Current range is too low - Check cabling at port specified in alarm • Current range is too high - Check SFP to ensure it is fully seated. If so, replace SFP.
	Temperature	• Assess lab temperature; check lab cooling system. • Check probes in same rack for temperature alarms; if probes in same rack have temperature alarms, verify power source to rack. • Check for fan alarms
	Fan	Check fan module; if fan speed too slow or not operating, replace fan tray.
	Voltage Levels	Power supply voltage too high or too low; contact Customer Support to analyze cause.
	Ethernet Connections to Disk Array	Check Ethernet cabling connections to disk arrays. If alarm persists, contact Customer Support.
	Board/Fan Status Alarms	If bad state, perform corrective action reported in alarm. If alarm persists, contact Customer Support.
	Inventory	All IICs must be the same model (IIC100 or IIC200). You cannot mix IIC100s and IIC200s in the same Media probe. Replace the hardware accordingly.
Severity	Critical	
Element	Hardware	
Value	N/A	

BASE-163 F/W Out Of Date

Probable Cause	The firmware found during an audit is out of date.
Recommended Action	Update firmware.
Severity	Minor
Element	N/A
Value	N/A

BASE-164 F/W Update Failed

Probable Cause	Firmware update failed.
Recommended Action	Ensure that the failure is valid, if so contact Customer Support.
Severity	Critical
Element	N/A
Value	N/A

BASE-165 F/W Incompatibility Detected

Probable Cause	Two installed firmware versions are incompatible.
Recommended Action	Contact Customer Support.
Severity	Major
Element	N/A
Value	N/A

BASE-201 Slave blade communication lost

Probable Cause	Communication is lost from the master blade to a slave blade. This alarm exists because in some scenarios a slave blade (such as the IIC) is not able to report a failure itself. The IIC automatically restarts.
Recommended Action	If alarm persists, contact Customer Support.
Severity	Critical
Element	Blade
Value	N/A

BASE-210 Slave blade NTP failure

Probable Cause	A slave blade cannot set its date/time to a valid value due to an invalid NTP server assignment. The IIC automatically restarts.
Recommended Action	From IrisView Admin Probe Management, select a valid NTP Server for the probe. If alarm persists, contact Customer Support.
Severity	Critical
Element	Blade
Value	N/A

BASE-301 Invalid installation directory

Probable Cause	The G10 application software is not correctly installed.

Recommended Action	Contact Customer Support.
Severity	Critical
Element	N/A
Value	N/A

BASE-302 Corrupted software installation

Probable Cause	The G10 software has missing or changed files. It is not safe to upgrade G10 software using the Admin Software Management Tab.
Recommended Action	Contact Customer Support.
Severity	Critical
Element	N/A
Value	N/A

BASE-303 Loss of NTP server

Probable Cause	The master blade has lost sync with the original NTP server.
Recommended Action	From IrisView Admin Probe Management, select a valid NTP Server for the probe. If alarm persists, contact Customer Support.
Severity	Major
Element	N/A
Value	N/A

BASE-401 CPU usage above normal

Probable Cause	The average idle CPU value for any blade has fallen below the minimum for normal limits. This is caused when one or more processes may be consuming CPU resources at a high CPU usage rate (such as during busy hours).
Recommended Action	If alarm escalates to BASE-402 or BASE-403, contact Customer Support.
Severity	Minor
Element	Blade
Value	CPU idle percent
Alarm trigger default	35% idle
Alarm clear default	40% idle

BASE-402 CPU usage above overload

Probable Cause	The average idle CPU value for any blade has fallen below the minimum overload limits. This is caused when one or more processes may be consuming CPU resources at a high CPU usage rate (such as during busy hours).
Recommended Action	Contact Customer Support.
Severity	Major
Element	Blade
Value	CPU idle percent
Alarm trigger default	25% idle
Alarm clear default	30% idle

BASE-403 CPU usage above safety limits

Probable Cause	The average idle CPU value for any blade has fallen below the minimum safe limits. This is caused when one or more processes may be consuming CPU resources at a high CPU usage rate (such as during busy hours).
Recommended Action	Contact Customer Support.
Severity	Critical
Element	Blade
Value	CPU idle percent
Alarm trigger default	10% idle
Alarm clear default	15% idle

BASE-411 Memory usage above normal

Probable Cause	The average free memory has fallen below the minimum normal limits. This is caused when one or more processes may be consuming memory at a high rate (such as during busy hours).
Recommended Action	If alarm escalates to BASE-412 or BASE-413, contact Customer Support.
Severity	Minor
Element	Blade
Value	Free memory percent
Alarm trigger default	35% free memory
Alarm clear default	40% free memory

BASE-412 Memory usage above overload

Probable Cause	The average free memory has fallen below the minimum overload limits. This is caused when one or more processes may be consuming memory at a high rate (such as during busy hours).
Recommended Action	If alarm persists, contact Customer Support.

Severity	Major
Element	Blade
Value	Free memory percent
Alarm trigger default	25% free memory
Alarm clear default	30% free memory

BASE-413 Memory usage above safety limits

Probable Cause	The average free memory has fallen below the minimum safe limits.
Recommended Action	If alarm persists, contact Customer Support.
Severity	Critical
Element	Blade
Value	Free memory percent
Alarm trigger default	10% free memory
Alarm clear default	15% free memory

BASE-415 Page swaps in (suggests memory exhaustion)

Probable Cause	Virtual memory pages are swapped in, suggesting memory exhaustion.
Recommended Action	If alarm persists, contact Customer Support.
Severity	Major
Element	Blade
Value	Page swap in events

BASE-421 Disk usage above normal limits

Probable Cause	The average free disk space has fallen below the minimum normal limits possibly due to log files or archive software packages filling up disks.
Recommended Action	Remove unused files from disk. Contact Customer Support.
Severity	Minor
Element	Mount Point
Value	Free disk space percent
Alarm trigger default	35% free disk space
Alarm clear default	40% free disk space

BASE-422 Disk usage above high limits

Probable Cause	The average free disk space on the probe has fallen below the minimum high usage limits possibly due to log files or archive software packages filling up disks.
Recommended Action	Remove unused files from probe disk. Contact Customer Support.
Severity	Major
Element	Mount Point
Value	Free disk space percent
Alarm trigger default	25% free disk space
Alarm clear default	30% free disk space

BASE-423 Disk usage above safe limits

Probable Cause	The average free disk space has fallen below the minimum safe limits possibly due to log files or archive software packages filling up disks.
Recommended Action	Remove unused files from probe disk. Contact Customer Support.
Severity	Critical
Element	Mount Point
Value	Free disk space percent
Alarm trigger default	10% free disk space
Alarm clear default	15% free disk space

BASE-431 High network traffic (Input Traffic)

Probable Cause	The average traffic load has surpassed normal limits. This alarm normally appears with BASE-110 indicating the probe is over capacity.	
Recommended Action	If alarm persists, contact Customer Support to diagnose cause.	
Severity	Minor	
Value	Megabits per second (input)	
Element	Interface (alarms on specific element)	
	public0/public1, base0/base1	
	Alarm trigger default	240 Mbps
	Alarm clear default	200 Mbps
	fabric0	
	Alarm trigger default	480 Mbps
	Alarm clear default	400 Mbps

BASE-432 Very high network traffic (Input Traffic)

Probable Cause	The average traffic load has surpassed high usage limits. This alarm normally appears with BASE-110 indicating the probe is over capacity.	
Recommended Action	If alarm persists, contact Customer Support to diagnose cause.	
Severity	Major	
Value	Megabits per second (output)	
Element	Interface (alarms on specific element)	
	public0/public1, base0/base1	
	Alarm trigger default	360 Mbps
	Alarm clear default	300 Mbps
	fabric0	
	Alarm trigger default	720 Mbps
	Alarm clear default	600 Mbps
	fabric1	
	Alarm trigger default	2500 Mbps
	Alarm clear default	2000 Mbps

BASE-433 Extremely high network traffic (Input Traffic)

Probable Cause	The average traffic load has surpassed safe limits. This alarm normally appears with BASE-110 indicating the probe is over capacity.	
Recommended Action	If alarm persists, contact Customer Support to diagnose cause.	
Severity	Critical	
Value	Megabits per second (input)	
Element	Interface (alarms on specific element)	
	public0/public1, base0/base1	
	Alarm trigger default	480 Mbps
	Alarm clear default	400 Mbps
	fabric0	
	Alarm trigger default	840 Mbps
	Alarm clear default	720 Mbps

BASE-441 High network traffic (Output Traffic)

Probable Cause	The average traffic load has surpassed normal limits. This alarm normally appears with BASE-110 indicating the probe is over capacity.
Recommended Action	If alarm persists, contact Customer Support to diagnose cause.
Severity	Minor

Value	Megabits per second (output)	
Element	Interface (alarms on specific element)	
	public0/public1, base0/base1	
	Alarm trigger default	240 Mbps
	Alarm clear default	200 Mbps
	fabric0/fabric1	
	Alarm trigger default	480 Mbps
	Alarm clear default	400 Mbps

BASE-442 Very high network traffic (Output Traffic)

Probable Cause	The average traffic load has surpassed high usage limits. This alarm normally appears with BASE-110 indicating the probe is over capacity.	
Recommended Action	If alarm persists, contact Customer Support to diagnose cause.	
Severity	Major	
Value	Megabits per second (output)	
Element	Interface (alarms on specific element)	
	public0/public1, base0/base1	
	Alarm trigger default	360 Mbps
	Alarm clear default	300 Mbps
	fabric0/fabric1	
	Alarm trigger default	720 Mbps
	Alarm clear default	600 Mbps

BASE-443 Extremely high network traffic (Output Traffic)

Probable Cause	The average traffic load has surpassed safe limits. This alarm normally appears with BASE-110 indicating the probe is over capacity.	
Recommended Action	If alarm persists, contact Customer Support to diagnose cause.	
Severity	Critical	
Value	Megabits per second (output)	
Element	Interface (alarms on specific element)	
	public0/public1, base0/base1	
	Alarm trigger default	480 Mbps
	Alarm clear default	400 Mbps
	fabric0/fabric1	
	Alarm trigger default	840 Mbps
	Alarm clear default	720 Mbps

BASE-451 Probe network packet errors

Probable Cause	A hardware issue is causing packet errors to occur on probe network interfaces reported in alarm.
Recommended Action	Check probe cabling. Refer to the ***G10 Installation Guide*** for cabling diagrams. If cabling is correct, replace the blade reported in alarm. If alarm persists, call Customer Support.
Severity	Minor
Element	Interface
Value	Packet errors

BASE-461 Network packet drops

Probable Cause	A hardware issue is causing packets to be dropped on probe network interfaces reported in alarm.
Recommended Action	Check probe cabling. Check probe cabling. Refer to the ***G10 Installation Guide*** for cabling diagrams. If cabling is correct, replace the blade reported in alarm. If alarm persists, call Customer Support.
Severity	Minor
Element	Interface
Value	Packet drops

BASE-471 Network correction magnitude out of spec

Probable Cause	The probe's time is more than 5 seconds different from the NTP server. Differences in time could be due to an invalid NTP server assigned to probe or a recently changed NTP server.
Recommended Action	Wait 24 hours to see if issue clears. If the alarm persists, or continually triggers and clears, call Customer Support.
Severity	Minor
Element	ntp_server
Value	Time offset (seconds)
Alarm trigger default	5 seconds
Alarm clear default	4 seconds

DATAFEED Alarms

The following system-level alarms are generated by Iris and appear in the Alarms Dashboard.

DATAFEED-101 DataFeed probe TCP connection failure (per probe-bladeId-receiver)

Probable Cause	The alarm is generated if DataFeed probe has TCP connection failure to the receiver.

Recommended Action	Check if receiver is up and running. Check whether the TCP connection between probe and receiver is up.
Severity	Critical
Element	Application
Value	N/A

DATAFEED-102 Number of dropped IP flow records (per probe-bladeId_instance-receiver-policy) exceeds threshold

Probable Cause	The alarm is generated when the number of dropped IP flow records exceeds threshold from DataFeed probe to receiver.
Recommended Action	Check if receiver is up and running. Check whether the TCP connection between probe and receiver has congestion.
Severity	Major
Element	Application
Value	Flow Records

DATAFEED-103 Number of dropped mobile flow records (per probe-bladeId_instance-receiver-policy) exceeds threshold

Probable Cause	The alarm is generated when the number of dropped mobile flow records exceeds threshold from DataFeed probe to receiver.
Recommended Action	Check if receiver is up and running. Check whether the TCP connection between probe and receiver has congestion.
Severity	Major
Element	Application
Value	Flow Records

IFC Alarms

The following IFC system-level alarms are generated by Iris and appear in the Alarms Dashboard.

Note: *IFC alarms are not accessible from the System Alarms tab and cannot be modified or forwarded using SNMP.*

IFC-101 Error Parsing Profile

Probable Cause	Invalid parameters defined in profile; IFC profile will not be processed.
Recommended Action	Check profile parameters and correct any errors.
Severity	Major
Element	IFC

IFC-102 Error Parsing Mount Point

Probable Cause	Invalid mount point defined; IFC profile will not be processed.
Recommended Action	Check mount point settings in profile. The defined path is the absolute path for storage; for example, "/export0/artifacts."
Severity	Major
Element	IFC

IFC-201 Unable to access mount point

Probable Cause	Network issues; disk access issues. IFC profile will not be processed.
Recommended Action	Check network status and access privileges to mount point defined in profile.
Severity	Major
Element	IFC

IFC-301 Unable to find node(s)/probe(s)

Probable Cause	Selected nodes or probes do not exist in Iris system.
Recommended Action	Compare the names of the nodes and probes configured in the profile with the names configured in Admin Topology Management.
Severity	Major
Element	IFC

IFC-302 Profile execution terminated (max execution time reached)

Probable Cause	Maximum execution time has been reached; profile has been terminated.
Recommended Action	None. The maximum time a profile can be executed is 8 hours.
Severity	Major
Element	IFC

IFC-303 Some searches for profile XYZ failed while retrieving records.

Probable Cause	Search failed because some IMSIs do not have session records during the selected time period (no session activity).
Recommended Action	Update profile with valid IMSIs.
Severity	Major
Element	IFC

IFC-304 Profile execution terminated (max IMSI per day reached)

Probable Cause	Maximum IMSI per day threshold has been reached; profile has been terminated.
Recommended Action	Maximum IMSI per day threshold is set by Tektronix; contact Customer Support.
Severity	Major
Element	IFC

IFC-401 Profile experienced export errors and some searches failed when saving to disk.

Probable Cause	Possible causes include: • Network connection error during file export • No session records exist to export for an IMSI • Internal error during exporting, such as memory issue or database error
Recommended Action	If only a few export files are missing, you can ignore the alarm. The issue is most likely no session records exist for the IMSI for the selected time period. For possible save to disk errors, contact Customer Support for assistance in troubleshooting log files such as profile.log and capture.log.
Severity	Major
Element	IFC

IFC-402 Profile experienced export errors and some searches failed when saving to the remote repository.

Probable Cause	Possible causes include: • Network connection error during file export • No session records exist to export for an IMSI • Internal error during exporting, such as memory issue or database error
Recommended Action	If only a few export files are missing, you can ignore the alarm. The issue is most likely no session records exist for the IMSI for the selected time period.
Severity	Major
Element	IFC

IIC Alarms

The following system-level alarms are generated by Iris and appear in the Alarms Dashboard.

IIC-101 IIC interface status

Probable Cause	An IIC port is inactive and not receiving traffic possibly due to one of the following conditions: • Physical link disconnected • IIC internal EzChip issue
Recommended Action	• Check cable connections to the IIC. • Verify that the SFP is completely seated. • Verify port provisioning in Iris Admin. Refer to the Iris Admin help for details about provisioning physical links. If alarm persists, contact Customer Support.
Severity	Critical
Element	Interface
Value	N/A

IIC-102 Valid physical links are not present yet and IIC will be in inactive mode

Probable Cause	No physical links are configured for an IIC or the IIC has not received topology updates.
Recommended Action	Configure physical links for the probe in Iris Admin Topology. Refer to the Iris Admin help for details. If alarm persists, contact Customer Support.
Severity	Info
Element	Link
Value	N/A

IIC-103 An SCTP path cannot be matched with any detected associations

Probable Cause	All topology auto-detection algorithms have failed for an SCTP path carrying data. This alarm usually clears when the probe reboots, when the path times out, or when the path is able to be associated during analysis of additional traffic.
Recommended Action	If the alarm does not clear since the path cannot be associated after analysis of additional traffic, you can manually configure a logical link using the IP addresses and ports defined in the alarm. See Admin online help for details.
Severity	Info
Element	SCTP Path (address, port -- address, port)
Value	N/A

IIC-104 IIC interface enable failed

Probable Cause	The IIC interface enable failed.
Recommended Action	If alarm persists, contact Customer Support.

Severity	Major
Element	Interface
Value	N/A

IIC-201 IIC packet drops

Probable Cause	Packets are being dropped by the IIC, possibly due to one of the following reasons: • excessive packet fragmentation • overload of incoming packets • overload of traffic processor
Recommended Action	If alarm persists, additional diagnostics/debug is required by Customer Support.
Severity	Critical
Element	Component
Value	Packet drops

IIC-202 IIC errors

Probable Cause	Errors are occurring on the IIC; the alarm text will provide specific error.
Recommended Action	If alarm persists, contact Customer Support.
Severity	Critical
Element	Component
Value	Errors

IIC-203 Max media stream capture limit reached

Probable Cause	The maximum number of simultaneous media stream captures is reached or exceeded.
Recommended Action	The maximum number of simultaneous captures is set by Tektronix; contact Customer Support for more information.
Severity	Major
Element	Component
Value	Number of captured streams
Alarm trigger default	Maximum number of simultaneous captures is reached or exceeded.
Alarm clear default	Number of simultaneous captures falls below 80% of the configured maximum value.

IIC-204 Max MSRP capture bandwidth reached

Probable Cause	The maximum capture bandwidth of MSRP packets is reached or exceeded. MSRP packets will be randomly dropped.

Recommended Action	The maximum capture bandwidth is set by Tektronix; contact Customer Support for more information.
Severity	Major
Element	Component
Value	packet drops
Alarm trigger default	Maximum capture bandwidth is reached or exceeded.
Alarm clear default	Capture bandwidth falls below 80% of the configured maximum value.

IIC-205 DPI Module failed to send packet or process received message

Probable Cause	Deep Packet Classification (DPC) traffic is exceeding capacity. Packets will be randomly dropped.
Recommended Action	If alarm persists, contact Customer Support.
Severity	Major
Element	Component
Value	Packet drops

IIC-206 LPC100 AMC (Avenger) timing fault discovered

Probable Cause	The LPC100 AMC (Avenger) is losing timing sync on the IRIS lines.
Recommended Action	If alarm persists, contact Customer Support.
Severity	Major
Element	Component
Value	Timing signal fault detected

IIC-207 EZCfg table overflow discovered

Probable Cause	The EZCfg table's provisioning leads to overflow.
Recommended Action	If alarm persists, contact Customer Support.
Severity	Major
Element	Component
Value	N/A

IIC-208 IPsec active sessions exceeded 1M

Probable Cause	Max limit reached for IPsec active sessions.
Recommended Action	Visibility to customer.
Severity	Major
Element	Component
Value	Packet Drops

IIC-301 IIC core inactive

Probable Cause	An Octeon Packet PipeLine (OPPL) core has stopped receiving data for processing for an extended period. This alarm is usually a precursor to IIC-302 alarm where the IIC crashes.
Recommended Action	If alarm persists, contact Customer Support.
Severity	Major
Element	Application
Value	N/A

IIC-302 IIC core crash/lockup

Probable Cause	An Octeon Packet PipeLine (OPPL) core locked up or crashed. IIC will automatically restart.
Recommended Action	If alarm persists, contact Customer Support.
Severity	Critical
Element	Application
Value	N/A

IIC-303 IIC PKO lockup

Probable Cause	The Octeon PCI output (PKO) hardware on the IIC locked up or crashed. IIC will automatically restart.
Recommended Action	If alarm persists, contact Customer Support.
Severity	Critical
Element	Application
Value	N/A

IIC-304 IIC PKO throttling

Probable Cause	The Octeon PCI output (PKO) hardware on the IIC is throttling because bandwidth exceeded expected capacity.
Recommended Action	If alarm persists, contact Customer Support.
Severity	Major
Element	Application
Value	N/A
Alarm trigger default	Maximum bandwidth is reached or exceeded.
Alarm clear default	When throttling stops.

IIC-402 IIC PPP Errors

Probable Cause	Errors occurred in the Point-to-Point (PPP) traffic processing module.
Recommended Action	If alarm persists, contact Customer Support.
Severity	Major
Element	Application
Value	N/A

IIC-403 IIC FSPP Errors

Probable Cause	Errors occurred in the Flow State Packet Processing (FSPP) module.
Recommended Action	If alarm persists, contact Customer Support.
Severity	Major
Element	Application
Value	N/A

IIC-404 IIC EZDBGSTATS Errors

Probable Cause	Errors occurred in the Line processor software.
Recommended Action	If alarm persists, contact Customer Support.
Severity	Major
Element	Application
Value	N/A

IIC-405 IIC OPPLSTATS Errors

Probable Cause	Errors occurred in the Octeon Packet PipeLine (OPPL) module.
Recommended Action	If alarm persists, contact Customer Support.
Severity	Major
Element	Application
Value	N/A

IIC-407 IIC DFGSTATS Errors

Probable Cause	Errors occurred in the IP defragmentation module.
Recommended Action	If alarm persists, contact Customer Support.
Severity	Major
Element	Application
Value	N/A

IIC-408 IIC SCTPSTATS Errors

Probable Cause	Errors occurred in the SCTP processing module.
Recommended Action	If alarm persists, contact Customer Support.
Severity	Major
Element	Application
Value	N/A

IIC-409 IIC STMGTPSTATS Errors

Probable Cause	Errors occurred in the GTP Correlation module.
Recommended Action	If alarm persists, contact Customer Support.
Severity	Major
Element	Application
Value	N/A

IIC-410 IIC KPI_STATS Errors

Probable Cause	Errors occurred in the KPI module.
Recommended Action	If alarm persists, contact Customer Support.
Severity	Major
Element	Application
Value	N/A

IIC-411 IIC PROTOSTATS Errors

Probable Cause	Errors occurred in the L7 protocols processing module.
Recommended Action	If alarm persists, contact Customer Support.
Severity	Major
Element	Application
Value	N/A

IIC-412 IIC VOIPSTATS Errors

Probable Cause	Errors occurred in the L7 VOIP protocols processing module.
Recommended Action	If alarm persists, contact Customer Support.
Severity	Major
Element	Application
Value	N/A

IIC-413 IIC SIGTRANSTATS Errors

Probable Cause	Errors occurred in the Sigtran protocols processing module.
Recommended Action	If alarm persists, contact Customer Support.
Severity	Major
Element	Application
Value	N/A

IIC-414 IIC IMON_DDM_DEBUG_REG Errors

Probable Cause	Errors occurred in the Data Distribution module.
Recommended Action	If alarm persists, contact Customer Support.
Severity	Major
Element	Application
Value	N/A

IPB Alarms

The following system-level alarms are generated by Iris and appear in the Alarms Dashboard.

IPB-101 systemConfigChange

Probable Cause	Generated when IPB configuration settings have been modified. The alarm reports the following information: • Type of configuration change (such as Port settings, system settings, access settings, filter settings). • ID Information (such as port ID) • User Name • IP Address of IPB where change was made
Recommended Action	None
Severity	Informational

IPB-102 consoleLogin

Probable Cause	Generated when a user logs into the IPB console. The alarm reports the following information: • User Name • IP Address of IPB where login occurred • Login Access Type (such as via serial, telnet, ssh)
Recommended Action	None
Severity	Informational

IPB-103 consoleLogout

Probable Cause	Generated when a user logs out of the IPB console. The alarm reports the following information: • User Name • IP Address of IPB where logout occurred • Login Access Type (such as via serial, telnet, ssh)
Recommended Action	None
Severity	Informational

IPB-104 consoleAuthFailed

Probable Cause	Generated when a user's login to the IPB console fails. The alarm reports the following information: • User Name • IP Address of IPB where login authorization failed • Login Access Type (such as via serial, telnet, ssh)
Recommended Action	None
Severity	Minor

IPB-105 portLinkUp

Probable Cause	Generated when the port identified in the alarm is active. Port designation is indicated as [chassis module]/[port number]. This alarm clears IPB-106.
Recommended Action	None
Severity	Informational

IPB-106 portLinkDown

Probable Cause	Generated when the port identified in the alarm is down. Port designation is indicated as [chassis module]/[port number].
Recommended Action	Check the cabling and SFP reported in alarm. Check configured port settings, such as negotiation settings.
Severity	Major

IPB-107 powerSupplyOneError

Probable Cause	Generated when Power Supply 1 is not working properly, possibly due to: • Power supply voltage too high or too low • Power has been interrupted to the IPB
Recommended Action	• Check power cabling at rear of IPB chassis • Check rack power source If alarm persists, contact Customer Support.
Severity	Major

IPB-108 powerSupplyOneOK

Probable Cause	Generated when Power Supply 1 recovers and is working properly. This alarm clears IPB-107.
Recommended Action	None
Severity	Informational

IPB-109 powerSupplyTwoError

Probable Cause	Generated when Power Supply 2 is not working properly, possibly due to: • Power supply voltage too high or too low • Power has been interrupted to the IPB
Recommended Action	• Check power cabling at rear of IPB chassis • Check rack power source If alarm persists, contact Customer Support.
Severity	Major

IPB-110 powerSupplyTwoOK

Probable Cause	Generated when Power Supply 2 recovers and is working properly. This alarm clears IPB-109.
Recommended Action	None
Severity	Informational

IPB-111 temperatureError

Probable Cause	Generated when IPB chassis air temperature operating above normal acceptable range.

Recommended Action	• Assess lab temperature; check lab cooling system. • Check equipment in same rack for temperature alarms; if equipment in same rack have temperature alarms, verify power source to rack. If alarm persists, contact Customer Support.
Severity	Major

IPB-112 temperatureOK

Probable Cause	Generated when IPB chassis air temperature resumes operating in acceptable range. This alarm clears IPB-111.
Recommended Action	None
Severity	Informational

IPB-113 triggerNotify

Probable Cause	Generated when an IPB trigger event has occurred. The alarm reports the name of the trigger and trigger details.
Recommended Action	Varies depending on the trigger notification.
Severity	Informational

IPB-114 vStackLinkState

Probable Cause	Generated when a dedicated vMesh port identified in the alarm changes status. The alarm reports the following information: • Local Port ID • Remote IP • Remote Port ID • Link Status Change
Recommended Action	None
Severity	Informational

IPB-115 moduleRemovalInfo

Probable Cause	Generated when a chassis module has been removed from the IPB. The alarm reports the following information: • Module ID (1-4) • Module Removal Status
Recommended Action	Ensure chassis module is properly seated. If alarm persists, contact Customer Support.
Severity	Informational

ISA Alarms

The following system-level alarms are generated by Iris and appear in the Alarms Dashboard.

ISA-101 Media Capture Memory Usage

Probable Cause	Memory used for storing the Direct Access Storage Addresses (DASAs) of the captured media PDUs exceeds a predefined threshold. Media capture packets will be discarded.
Recommended Action	Contact Customer Support.
Severity	Major
Element	Application
Value	Threshold

ISA-102 High MPC query request

Probable Cause	The probe has received a large number of queries in a short amount of time. This scenario could indicate a multi-protocol (MPC) rule is not configured correctly.
Recommended Action	Contact Customer Support.
Severity	Major
Element	Application
Value	Number of MPC queries

ISA-103 ISA cannot write to SR2D

Probable Cause	ISA stripe queues on SR2D archive have reached or exceeded maximum capacity.
Recommended Action	The maximum capacity is set by Tektronix; contact Customer Support for more information.
Severity	Critical
Element	Stripe
Value	N/A
Alarm trigger default	Maximum stripe queue is reached or exceeded maximum capacity.
Alarm clear default	After 1 minute of successful storage into ISA stripe queue. This time is configurable by Tektronix.

ISA-104 DC archive not configured

Probable Cause	The Decrypted archive option for data storage has been enabled by Tektronix (in a plist), but the DC storage array archive is not configured correctly. Deciphered PDUs are not stored.
Recommended Action	Contact Customer Support.
Severity	Critical
Element	S2D archive
Value	N/A

ISA-105 ISA Down

Probable Cause	The probe raises this alarm when it is not allowing ISA queries. Currently, this is raised when storage is not responding (when SR2D-106 is raised).
Recommended Action	Contact Customer Support.
Severity	Major
Element	ISA
Value	N/A

ISA-110 Flow summaries discarded due to exceed number of flow protocols in segment

Probable Cause	Too many Flow Summaries were generated for a particular protocol in a session record segment, and additional flow summaries are being discarded. Affected cage, slot, and traffic processor are specified in alarm description.
Recommended Action	The maximum threshold is set by Tektronix; contact Customer Support for more information.
Severity	Major
Element	Application
Value	N/A

ISA-201 Tracking New Sessions Disabled

Probable Cause	Memory usage exceeded a configured limit to disable creating new sessions in ISA.
Recommended Action	Contact Customer Support. Confirm this behavior is desired at the specified memory threshold. If not, reconfigure. Otherwise, more probe resources may be required to fully monitor the traffic.
Severity	Major
Element	ISA
Value	N/A

ITA Alarms

The following system-level alarms are generated by Iris and appear in the Alarms Dashboard.

ITA-101 ITA Probe to ITA Collector connection failure

Probable Cause	The G10 probe has a failed TCP connection to the ITA collector due to network issues or an incorrectly configured ITA Collector Engine.
Recommended Action	Contact Customer Support to verify the ITA Collector host name and port is configured correctly (ITA Admin in Admin Application Management tab).
Severity	Critical
Element	Application
Value	N/A

ITA-102 ITA Probe send data to ITA Collector unsuccessfully

Probable Cause	Data loss occurred between the G10 probe and the ITA Collector due to probe buffer reaching capacity.
Recommended Action	The Buffer size is set by Tektronix; contact Customer Support for more information.
Severity	Critical
Element	Application
Value	N/A
Alarm trigger default	Buffer capacity is reached or exceeded.
Alarm clear default	After 5 minutes of no data loss. This time is configurable by Tektronix.

ITA-103 ITA probe TCP connection failure between master and slave processor

Probable Cause	LTE Control Plane probe: An IAP200 in the expansion chassis failed to send data to the IAP200 in the primary chassis due to TCP connection failure/timeout.
Recommended Action	Check inter-cage cabling and current blade state of the IAP200s; refer to the ***LTE Control Plane Probe Installation Guide*** for cabling diagrams. If alarm persists, contact Customer Support.
Severity	Critical
Element	Application
Value	N/A

ITA-104 ITA probe slave processor send data to master processor unsuccessfully

Probable Cause	LTE Control Plane probe: An IAP200 in the expansion chassis failed to send data to the IAP200 in the primary chassis due to its buffer reaching capacity.
Recommended Action	Contact Customer Support.
Severity	Critical
Element	Application
Value	N/A

MAPPER Alarms

The following system-level alarms are generated by Iris and appear in the Alarms Dashboard.

MAPPER-101 LTE Mapper data save failure

Probable Cause	LTE Mapper failed to save data to disk due to: • Write permissions • Disk full

Recommended Action	Contact Customer Support. The time interval to check the data save status can be set by Tektronix.
Severity	Major
Element	LTE Mapper

MAPPER-102 LTE Mapper Client connection failure

Probable Cause	Packets will be dropped due to a connection failure between the LTE Mapper client and the LTE Mapper server due to one of the following: • Network issues • Incorrectly configured LTE Mapper server in plist • LTE Server is down
Recommended Action	Contact Customer Support. The time interval to clear the alarm after connection recovery can be set by Tektronix.
Severity	Minor
Element	LTE Mapper
Value	N/A

MAPPER-103 LTE Mapper IPM message send failure

Probable Cause	LTE Control Plane Probe alarm: the traffic processor on a G10 IAP200 failed to send IPM messages to another IAP200.
Recommended Action	Verify the traffic processors are in the UP state. Contact Customer Support.
Severity	Critical
Element	Application
Value	N/A

MAPPER-104 LTE Mapper subscriber capacity exceed the limitation

Probable Cause	LTE Mapper subscriber capacity exceeds predefined threshold.
Recommended Action	Contact Customer Support.
Severity	Major
Element	LTE Mapper
Value	N/A
Alarm trigger default	Maximum subscriber threshold is reached or exceeded.
Alarm clear default	Maximum subscriber capacity falls below 90% of the set maximum value per probe type.

OAM Alarms

The following system-level alarms are generated by Iris and appear in the Alarms Dashboard.

OAM-101 Connection Refused

Probable Cause	Generated when the Iris server refuses a connection attempt due to invalid probe ID (such as incompatible software versions between probe and server).
Recommended Action	Contact Customer Support.
Severity	Critical
Element	Server
Value	N/A

OAM-201 Invalid plist file update

Probable Cause	Generated when a locally-modified plist file is detected. Plists are modified by Tektronix personnel; contact Customer Support for more information.
Recommended Action	Contact Customer Support.
Severity	Critical
Element	File
Value	N/A

Probe Alarms

The following system-level alarms are generated by Iris and appear in the Alarms Dashboard.

Note: *The Probe alarm is not accessible from the System Alarms tab and cannot be modified or forwarded using SNMP.*

Probe-Server connection loss

Probable Cause	The probe has lost connectivity to the Iris server. Connectivity is determined by Keep Alive messages sent from the probe to the Iris server.
Severity	Critical
Element	Probe
Alarm Triggered	Iris Server has not received Keep Alive messages from the specified probe.
Alarm Cleared	Connectivity between probe and Iris server is restored.

Server does not have plist versions reported by Probe

Probable Cause	The server does not have plist versions reported by the Probe.
Severity	Critical
Element	Probe
Alarm Triggered	Iris Server does not have plist version reported by the Probe.
Alarm Cleared	Iris Server has plist versions reported by the Probe.

SHMM OAM LAN connection Failure Alarm

Probable Cause	The server lost connection to SHMM.
Severity	Critical
Element	Probe
Alarm Triggered	SHMM IP is not reachable.
Alarm Cleared	SHMM IP is reachable.

Storage (S2D) Alarms

The following system-level alarms are generated by Iris and appear in the Alarms Dashboard.

S2D-101 S2D application shutdown

Probable Cause	A Store-to-disk application is in shutdown mode due to one of the following errors: • Hardware configuration error • S2D configuration error in plists • SAS cabling errors • LSI hardware status error
Recommended Action	Contact Customer Support.
Severity	Critical
Element	Subsystem
Value	N/A

S2D-102 S2D misconfigured

Probable Cause	A Store-to-disk archive is not configured correctly due to errors in a plist file. Alarm message indicates plist error details.
Recommended Action	Contact Customer Support.
Severity	Critical
Element	S2D Archive
Value	N/A

S2D-103 DC archive not configured

Probable Cause	The Decrypted archive option for data storage has been enabled by Tektronix (in a plist), but the DC storage array archive is not configured correctly. Deciphered PDUs are not stored.
Recommended Action	Contact Customer Support.
Severity	Critical
Element	S2D Archive
Value	N/A

S2D-201 S2D archive failure

Probable Cause	An S2D archive is down due to one of the following errors: • No SAS connectivity • Detection of large IO time to some volume • Detection of consecutive IO errors to some volume • Archive manually brought down by admin action • Temporary error • No connection to S2D server • Configuration error • Timemap is too old • Received data behind latest archive time
Recommended Action	Contact Customer Support.
Severity	Critical
Element	S2D Archive
Value	N/A

S2D-202 SAS link down

Probable Cause	SAS connectivity to a Storage Array controller is lost due to a cable disconnect or because the corresponding disk array is down.
Recommended Action	Check SAS cabling (refer to G10 Installation Guides for cabling diagrams). If alarm persists, contact Customer Support.
Severity	Critical
Element	SAS Link
Value	N/A

S2D-203 S2D volume failure

Probable Cause	A critical error on a Storage Array volume has occurred due to one of the following errors: • A volume on the archive could not be opened • Detection of large IO time to some volume • Detection of consecutive IO errors to some volume; some disk in volume may be bad

Recommended Action	• Determine if the probe is over capacity by following the steps on the Capacity Bandwidth Calculations tab. • Log on to Disk array and check event logs for controller module/disk errors. Address any existing error conditions. • Arch_up ALL archives if no errors are found. • If issue persists, an RMA of controller modules or disks may resolve issue. Additional diagnostics/debug is required by Tekcomms Customer Support.
Severity	Critical
Element	S2D Volume
Value	N/A

S2D-301 Archive duration below threshold

Probable Cause	Duration of the **short term** packets archive falls below threshold.
Recommended Action	Add additional volumes to the archives so the capacity, and thus the duration, is increased. If alarm persists, contact Customer Support.
Severity	Major
Element	S2D Archive
Value	Duration
Alarm trigger default	30 minutes
Alarm clear default	35 minutes

S2D-302 Archive duration below threshold

Probable Cause	Duration of the **long term** packets archive falls below threshold.
Recommended Action	Add additional volumes to the archives so the capacity, and thus the duration, is increased. If alarm persists, contact Customer Support.
Severity	Major
Element	S2D Archive
Value	Duration
Alarm trigger default	60 minutes
Alarm clear default	65 minutes

S2D-303 Archive duration below threshold

Probable Cause	Duration of the **DC** packets archive falls below threshold.
Recommended Action	Add additional volumes to the archives so the capacity, and thus the duration, is increased. If alarm persists, contact Customer Support.
Severity	Major

Element	S2D Archive
Value	Duration
Alarm trigger default	60 minutes
Alarm clear default	65 minutes

S2D-304 Archive duration below threshold

Probable Cause	Duration of the **Extra** packets archive falls below threshold.
Recommended Action	Add additional volumes to the archives so the capacity, and thus the duration, is increased. If alarm persists, contact Customer Support.
Severity	Major
Element	S2D Archive
Value	Duration
Alarm trigger default	60 minutes
Alarm clear default	65 minutes

S2D-401 Archive out of buffers

Probable Cause	Packets are discarded due to an archive being out of buffers.
Recommended Action	Contact Customer Support.
Severity	Major
Element	S2D archive
Value	N/A

S2D-402 Packets with bad timestamps received

Probable Cause	Some packets were timestamped with an incorrect value. Consequently, these packets may be missed (not returned) on a retrieve-by-time query.
Recommended Action	Check the system time on both IIC and IAP to see if there are discrepancies. If so, you may attempt to clear the error by rebooting the probe. The alarm is cleared automatically when there are no invalid packet timestamps for 15 seconds. If the problem persists and the alarm repeatedly stays on for more than one minute within the same day, contact Customer Support.
Severity	Major
Element	S2D Packet archive
Value	N/A

SAMTCE Alarms

The following system-level alarms are generated by Iris and appear in the Alarms Dashboard.

SAMTCE-101 Storage array configuration fails

Probable Causes	Storage array configuration error has occurred due to one of the following errors: • Configuration script timed out • Failed to read configuration • Failed to remove file systems • Failed to remove volumes from array • Failed to add volume <name> • Failed to partition volume <name> • Failed to add file system <name> • Failed to scan the SCSI bus for new devices
Recommended Action	Contact Customer Support.
Severity	Critical
Element	Storage Array
Value	N/A

SAMTCE-102 Storage array configuration

Probable Cause	This alarm is generated when the storage array configuration does not have enough resources to run the current profile. This could be due to missing disks or controllers for example.
Recommended Action	Add or replace the missing resources.
Severity	Critical
Element	Storage Array
Value	N/A

SAMTCE-300 Temperature or voltage in the warning range

Probable Cause	The sensors detected temperature or voltage in the warning range.
Recommended Action	Check for any obstructions to the storage array airflow. If alarm persists, contact Customer Support.
Severity	Major
Element	Storage Array
Value	N/A

SAMTCE-301 Temperature or voltage in the failure range

Probable Cause	The sensors detected temperature or voltage in the failure range.
Recommended Action	Verify that the fans are running. If alarm persists, contact Customer Support.

Severity	Critical
Element	Storage Array
Value	N/A

SAMTCE-302 Over-temperature condition

Probable Cause	A temperature sensor on a controller module FRU detected an over-temperature condition.
Recommended Action	Replace the controller module FRU if the temperature is within range (41°F to 104°F). Refer to the ***G10 Hardware Maintenance Guide for details***. If alarm persists, contact Customer Support.
Severity	Critical
Element	Storage Array
Value	N/A

SAMTCE-303 A FRU has failed or is not operating correctly

Probable Cause	The FRU specified in the alarm message has failed or encountered an error.
Recommended Action	Examine the FRU specified in the message. Contact Customer Support.
Severity	Critical
Element	Storage Array
Value	N/A

SAMTCE-304 Power supply unit failure

Probable Cause	One of the storage array's power supplies fails.
Recommended Action	Examine the power supply specified in the message. Contact Customer Support.
Severity	Critical
Element	Storage Array
Value	N/A

SAMTCE-305 Power supply fan failure

Probable Cause	One of the storage array's power supply fans fails.
Recommended Action	Examine the power supply fan specified in the message. Contact Customer Support.
Severity	Major
Element	Storage Array
Value	N/A

SAMTCE-400 Enclosure reported a general failure

Probable Cause	An expansion or controller enclosure in the storage array reports a general failure.
Recommended Action	Check the controller/expansion module for problems, for example, the module is not fully inserted or the cables are bad. Contact Customer Support.
Severity	Critical
Element	Storage Array
Value	N/A

SAMTCE-401 Duplicated controller serial number

Probable Cause	Both controllers in an active-active configuration have the same serial number.
Recommended Action	Contact Customer Support. Verify both controller serial numbers and change at least one of them.
Severity	Critical
Element	Storage Array
Value	N/A

SAMTCE-402 Disk controller critical error

Probable Cause	The controller experienced the critical error specified in the alarm description.
Recommended Action	Determine the problem from the alarm message. Contact Customer Support.
Severity	Critical
Element	Storage Array
Value	N/A

SAMTCE-403 Flash chip write failure

Probable Cause	A failure occurred when trying to write to the flash chip.
Recommended Action	Replace the controller module. Contact Customer Support.
Severity	Critical
Element	Storage Array
Value	N/A

SAMTCE-404 Master copy-on-write I/O failure

Probable Cause	The background master copy-on-write operation has failed.
Recommended Action	Isolate and replace failed hardware components described in alarm description. Contact Customer Support.

Severity	Critical
Element	Storage Array
Value	N/A

SAMTCE-405 FRU-ID SEEPROM read/write problem

Probable Cause	A problem exists writing/reading the persistent IP data to/from the FRU-ID SEEPROM.
Recommended Action	Contact Customer Support. Check the IP settings, and update them if they are incorrect.
Severity	Major
Element	Storage Array
Value	N/A

SAMTCE-406 An I/O module is down

Probable Cause	An I/O module is down and will not be automatically restarted.
Recommended Action	Contact Customer Support. The Standby Controller (SC) needs service or replacement.
Severity	Critical
Element	Storage Array
Value	N/A

SAMTCE-407 A super-capacitor failure

Probable Cause	A super-capacitor failure.
Recommended Action	Contact Customer Support. Replace the controller module.
Severity	Critical
Element	Storage Array
Value	N/A

SAMTCE-408 The super-capacitor pack is near end of life

Probable Cause	A super-capacitor has failed.
Recommended Action	Contact Customer Support. Replace the controller module.
Severity	Major
Element	Storage Array
Value	N/A

SAMTCE-500 Volume unrecoverable failure

Probable Cause	A storage array volume has an unrecoverable failure.
Recommended Action	Contact Customer Support. Replace the failed vdisk (virtual disk) specified in the alarm message.
Severity	Critical
Element	Storage Array
Value	N/A

SAMTCE-501 Disk Failure, Raid5 redundancy lost

Probable Cause	At least one disk on the RAID5 volume has failed.
Recommended Action	Contact Customer Support. Replace the failed disk and add it as a vdisk (virtual disk) spare to the critical vdisk.
Severity	Major
Element	Storage Array
Value	N/A

SAMTCE-600 A SMART event occurred

Probable Cause	A Self-Monitoring, Analysis, and Reporting Technology (SMART) event occurred, which could result in impending disk failure.
Recommended Action	Check and replace the affected disk. Contact Customer Support.
Severity	Critical
Element	Storage Array
Value	N/A

SAMTCE-601 Degraded disk transfer rate

Probable Cause	The expected transfer rate is degrading, possibly due to a hardware failure.
Recommended Action	If alarm persists contact Customer Support for assistance in troubleshooting the issue.
Severity	Critical
Element	Storage Array
Value	N/A

SAMTCE-602 Disk failed alarm

Probable Cause	A disk associated with a storage volume has failed.
Recommended Action	Replace the disk, and initiate the volume repair procedure.

Severity	Critical
Element	Storage Array
Value	N/A

Session Record (SR2D) Alarms

The following system-level alarms are generated by Iris and appear in the Alarms Dashboard.

SR2D-101 Failure to write session record

Probable Cause	A session record has failed to write to disk, possibly due to a hardware failure. Affected stripe, volume, and mount point are specified in alarm description.
Recommended Action	Monitor SAMTCE alarms to isolate hardware issue. Contact Customer Support.
Severity	Major
Element	SR2D
Value	N/A
Alarm trigger default	Session record write failure
Alarm clear default	After a configurable amount of time has passed without write errors or when volume is deleted. This time is configurable by Tektronix.

SR2D-102 Failure to write SR2D index

Probable Cause	An SR2D index has failed to write to disk, possibly due to a hardware failure. Affected stripe, volume, and mount point are specified in alarm description.
Recommended Action	Monitor SAMTCE alarms to isolate hardware issue. Contact Customer Support.
Severity	Major
Element	SR2D
Value	N/A
Alarm trigger default	SR2D index write failure
Alarm clear default	After a configurable amount of time has passed without write errors or when volume is deleted. This time is configurable by Tektronix.

SR2D-103 Failure to write SR2D session details

Probable Cause	SR2D session details (part of Session Summary) have failed to write to disk, possibly due to a hardware failure. PDUs and flow details from session summaries are lost and cannot be recalled for historical analysis. Affected stripe, volume, and mount point are specified in alarm description.
Recommended Action	Monitor SAMTCE alarms to isolate hardware issue. Contact Customer Support.

Severity	Major
Element	SR2D
Value	N/A
Alarm trigger default	SR2D session details write failure
Alarm clear default	After a configurable amount of time has passed without write errors or when volume is deleted. This time is configurable by Tektronix.

SR2D-104 Session records written with invalid timestamps

Probable Cause	One or more session records have end times that are invalid. Issue could be caused by: • Probe is over capacity. • Disk failure causing excess backlog of writing session records (this could cause inability to retrieve session records within expected time window) Affected stripe, volume, and mount point are specified in alarm description.
Recommended Action	Contact Customer Support.
Severity	Major
Element	SR2D
Value	N/A
Alarm trigger default	SR2D session records detected with invalid end times.
Alarm clear default	After a configurable amount of time has passed without invalid end times or when volume is deleted. This time is configurable by Tektronix.

SR2D-105 Session Records discarded due to excess size

Probable Cause	A Session Summary record is too large to be written to disk. This could be due to an extremely busy call or data corruption. Data loss will occur for the affected call. Affected stripe, volume, and mount point are specified in alarm description.
Recommended Action	Contact Customer Support.
Severity	Major
Element	SR2D
Value	N/A
Alarm trigger default	Session record size exceeds threshold.
Alarm clear default	After a configurable amount of time has passed without session records exceeding threshold or when volume is deleted. This time is configurable by Tektronix.

SR2D-106 Storage not responding

Probable Cause	The operating system on the x86 blade blocks I/O threads (writing and reading) for at least one minute. The probe detects this condition and enters a state where it will not allow any ISA queries.

Recommended Action	Contact Customer Support.
Severity	Critical
Element	SR2D
Value	N/A

SR2D-107 Diskless Mode

Probable Cause	Indicates that the G10 either has no storage configuration, or it has a storage configuration which does not support session record storage.
Recommended Action	If Session Record storage is desired for this probe, provide a storage configuration that allows Session Record storage. Contact Customer Support for assistance.
Severity	Major
Element	SR2D
Value	N/A

TD140 Alarms

The following system-level alarms are generated by Iris and appear in the Alarms Dashboard. For more information about the TD140 load balancer, refer to the ***TD140 Hardware Maintenance Guide*** or ***TD140 Hardware Installation Guide***.

TD140-101 Configured ports are down

Probable Cause	Generated when a previously In-Service port goes down.
Recommended Action	• Check cabling on the affected port (the port could be one of the ports on the front panel of PPM40 or one of the ports on the RTM). • On the PPM40, run the command: swcf configure interface <eg:1/1> no shutdown
Severity	Major
Element	TD140

TD140-102 Session was aborted

Probable Cause	Generated when sessions are aborted due to overload and the TD140 receives a GTP-C message for which it has to create a new session. When Load balancing is configured in Limited mode, overload occurs due to either of the following conditions: • Packet rate for the G10 is equal to the Session Drop Onset Packet Rate configured for the G10. • Number of active sessions for the G10 is equal to the Max Sessions configured for the G10. Sessions can also be aborted when the number of sessions active in the TD140 is equal to the maximum number of sessions supported by the TD140. Sessions can also be aborted due to certain traffic, in the case of an IMSI Abort.
Recommended Action	No action is required by user. When the TD140 enters overload condition it will delete Least Recently Used sessions to accommodate new sessions. If alarm persists, contact Customer Support to increase maximum thresholds.
Severity	Major
Element	TD140

TD140-103 Temperature of the processor and on-board temp sensor exceeded a pre-defined value

Probable Cause	The sensor specified in alarm detected temperature in the warning range.	
Recommended Action	• Assess lab temperature; check lab cooling system. • Check probes and other equipment in same rack for temperature alarms; if other equipment in same rack have temperature alarms, verify power source to rack. • Check for fan alarms • Restart the chassis and see if the fans start working.	
Severity	Major	
Element	DPB1 Octeon Temp (85H) / DPB2 Octeon Temp (93H)	
Thresholds	Upper non-recoverable thresholds (UNR)	88
	Upper critical thresholds (UC)	72
	Upper non-critical thresholds (UNC)	65
	Lower non-critical thresholds (LNC)	0
	Lower critical thresholds (LC)	5
	Lower non-recoverable thresholds (LNR)	10

TD140-104 Management port is down [Logged to TD140 Alarm File]

Probable Cause	Connection to the OAM port (Port B/ETH3) has been lost. An alarm cannot be generated when Management ports are down; this condition will be logged to the /tmp/lb_evt.log alarm file in the TD140 Shelf Management Controller (ShMC). Note: This alarm only indicates when Port B/ETH3 is down. It will not trigger when Port A/ETH2 is down. The ETH2 port will not be configured by the user, and the default IP (ETH2) will only be used in an emergency situation by a site technician. The (ETH2:1) IP will not be configured for usage.
Recommended Action	Check the OAM port cable on the ShMC.
Severity	Major
Element	TD140

TD140-105 The board is removed

Probable Cause	Generated when the PPM40 is removed (slot number specified in alarm) or starts to reboot.
Recommended Action	The alarm clears when PPM40 successfully comes up. If the alarm does clear after 5 minutes, then reseat boards.
Severity	Major
Element	PPM40

TD140-106 The processor crashed/restarted

Probable Cause	An OCTEONS processor in the PPM40 has crashed.
Recommended Action	No user action required. The PPM40 board will automatically restart. ***Tektronix Communications Engineers: Collect the crash log from the RSM in directory /tmp/app-backtrace/.***
Severity	Major
Element	PPM40 OCTEONS processor

TD140-107 Packets were dropped

Probable Cause	CPU usage is above 99%. Packets are dropped on ingress or egress ports, possibly due to one of the following conditions: • Errors in MAC (Layer 2) processing • Unavailable G10 • Uncorrelated GTP-U packets in Limited mode • Certain traffic cases such as unsupported packets due to packet size, too many MPLS labels, or too many VLAN tags
Recommended Action	Display packet-drop statistics from the CLI: show stats packet-drop. Contact Customer Support.
Severity	Major
Element	TD140

TD140-108 Attempted software activation failed

Probable Cause	The TD140 software upgrade activation has failed, possibly due to one of following causes: 1. The RSM may not have enough disk space to complete the upgrade procedure. 2. MD5sum of the ISO mismatching. 3. Flash Failures due to flash corruption The TD140 software package contains the Shelf Management Controller (ShMC) and PPM40 images (system OS, Application).
Recommended Action	**Cause 1** • Check if RSM has enough free space on the RSM (df –h). • Ensure use% for rootfs and tmpfs is not more than 30%. If use% is greater than 30% reboot ShMC • Retry the upgrade procedure again **Cause 2** • Verify the MD5sum of the ISO image and push a proper MD5 file to TD140. **Cause 3** • Contact next level support
Severity	Critical
Element	TD140

TD140-109 Attempted configuration activation failed

Probable Cause	The configuration activation refers to the configuration of the load balancer application in TD140 through the XML file sent by the Iris server. Possible causes for failure: • Md5sum of the XML file does not match the md5sum present in the lb_cfg.md5 file. • Both NTP and PTP server configuration present in the XML file • Parsing error in the XML file. • Parameter values out of range
Recommended Action	• Check The XML file for errors. Errors in XML file should be corrected and sent to the TD-140 and the configuration activation should be retried. • Verify the MD5sum of the configuration file and push a proper MD5 file from Irisview.
Severity	Critical
Element	TD140

TD140-110 Loss of sync with NTP server

Probable Cause	The TD140 has lost sync with the original NTP server.
Recommended Action	From IrisView Admin Probe Management, select a valid NTP server for the TD140. If alarm persists, contact Customer Support.
Severity	Major
Element	TD140

TD140-111 Excessive NTP offset

Probable Cause	The TD140's time is more than 1000 milliseconds different from the NTP server. Differences in time could be due to an invalid NTP server assigned to probe or a recently changed NTP server.
Recommended Action	From IrisView Admin Probe Management, verify that a valid NTP server is assigned for the TD140. Wait 24 hours to see if issue clears. If the alarm persists, or continually triggers and clears, call Customer Support.
Severity	Minor
Element	TD140
Alarm trigger default	NTP offset greater than 1000 ms
Alarm clear default	NTP offset at 500 ms

TD140-112 Packets dropped on management interface

Probable Cause	This management port refers to the public management interface of the ShMC (eth3/port B) used to communicate with the Iris server and SNMP alarm collector. Possible causes include: • fcs errors • jobbers • auto negotiation failures
Recommended Action	Check the physical connectivity and cabling.
Severity	Minor
Element	TD140

TD140-113 CPU core usage exceeds minor threshold

Probable Cause	One or more processes may be consuming CPU core resources at a high usage rate possibly due to an increase in the volume of the ingress packet traffic.
Recommended Action	For information purposes, and normally no action is needed. However if for the volume of ingress traffic the CPU usage is deemed to be high, contact Customer Support.
Severity	Minor
Element	TD140
Alarm trigger default	65% CPU core usage
Alarm clear default	60% CPU core usage

TD140-114 CPU core usage exceeds major threshold

Probable Cause	One or more processes may be consuming CPU core resources at a high usage rate possibly due to and increase in the volume of the ingress packet traffic.

Recommended Action	For information purposes and normally no action is needed. However if for the volume of ingress traffic the CPU usage is deemed to be high, contact Customer Support.
Severity	Major
Element	TD140
Alarm trigger default	75% CPU core usage
Alarm clear default	70% CPU core usage

TD140-115 CPU core usage exceeds critical threshold

Probable Cause	One or more processes may be consuming CPU core resources at a high usage rate possibly due to and increase in the volume of the ingress packet traffic.
Recommended Action	For information purposes and normally no action is needed. However if for the volume of ingress traffic the CPU usage is deemed to be high, contact Customer Support.
Severity	Critical
Element	TD140
Alarm trigger default	90% CPU core usage
Alarm clear default	85% CPU core usage

TD140-116 Memory usage exceeds minor threshold

Probable Cause	One or more processes may be consuming CPU resources at a high usage rate possibly due to a high incoming packet rate.
Recommended Action	This is just for information purposes and normally no action is needed. If alarm escalates to TD140-117 or TD140-118, contact Customer Support.
Severity	Minor
Element	TD140
Alarm trigger default	65% memory usage
Alarm clear default	60% memory usage

TD140-117 Memory usage exceeds major threshold

Probable Cause	One or more processes may be consuming CPU resources at a high usage rate possibly due to a high incoming packet rate.
Recommended Action	This is just for information purposes and normally no action is needed. If for the volume of ingress traffic the CPU usage is deemed to be high, contact Customer Support.
Severity	Major
Element	TD140
Alarm trigger default	75% memory usage
Alarm clear default	70% memory usage

TD140-118 Memory usage exceeds critical threshold

Probable Cause	One or more processes may be consuming CPU resources at a high usage rate possibly due to: • High incoming packet rate • Defect the application software leading to memory leak
Recommended Action	Contact Customer Support.
Severity	Critical
Element	TD140
Alarm trigger default	90% memory usage
Alarm clear default	85% memory usage

TD140-119 File system usage exceeds minor threshold

Probable Cause	One or more processes may be consuming SHMM resources at a high usage rate possibly due to: • An unwanted large file is manually placed onto the SHMM file system. • A defect in ShMC software
Recommended Action	• If any files were manually placed into the TD140 ShMC, remove them. • If possible, try restarting the ShMC. • If the problem persists, or alarm escalates to TD140-120 or TD140-121, contact Customer Support.
Severity	Minor
Element	TD140
Alarm trigger default	65% file system usage
Alarm clear default	60% file system usage

TD140-120 File system usage exceeds major threshold

Probable Cause	One or more processes may be consuming SHMM resources at a high usage rate possibly due to: • An unwanted large file is manually placed onto the SHMM file system. • A defect in ShMC software
Recommended Action	• If any files were manually placed into the TD140 ShMC, remove them. • If possible, try restarting the ShMC. • If the problem persists, or alarm escalates to TD140-121, contact Customer Support.
Severity	Major
Element	TD140
Alarm trigger default	75% file system usage
Alarm clear default	70% file system usage

TD140-121 File system usage exceeds critical threshold

Probable Cause	One or more processes may be consuming SHMM resources at a high usage rate possibly due to: • An unwanted large file is manually placed onto the SHMM file system. • A defect in ShMC software
Recommended Action	• If any files were manually placed into the TD140 ShMC, remove them. • If possible, try restarting the ShMC. • If the problem persists, contact Customer Support.
Severity	Critical
Element	TD140
Alarm trigger default	90% file system usage
Alarm clear default	85% file system usage

TD140-122 Power supply failure

Probable Cause	Power has been interrupted to the TD140.
Recommended Action	Perform the following: • Check that the GREEN OK LED is illuminated. • Check power cabling at rear of TD140 chassis. • Check rack power source. If alarm persists, contact Customer Support.
Severity	Critical
Element	TD140

TD140-123 Power feed failure

Probable Cause	Power supply voltage too high or too low, possibly due to an unregulated power supply.
Recommended Action	Check all the power cabling steps in the ***TD140 Installation Guide*** were followed. Contact Customer Support to analyze cause if problem persists.
Severity	Major
Element	TD140

TD140-124 Fan failure

Probable Cause	Fan is not operating normally.
Recommended Action	Check fan tray; if fan speed too slow or not operating, replace fan tray.
Severity	Critical
Element	TD140

TD140-125 Chassis air temperature

Probable Cause	Chassis air temperature operating above normal acceptable range.
Recommended Action	• Assess lab temperature; check lab cooling system. • Check equipment in same rack for temperature alarms; if equipment in same rack have temperature alarms, verify power source to rack. • Check for fan alarms
Severity	Critical
Element	TD140

TD140-126 Optical dB out-of-range (only for active ports)

Probable Cause	Light transmit/receive is too high or low. Alarm reports: port, TX or RX, current dBm value. Probable causes could be: • SFP is not plugged in properly • Optical cable is not inserted properly • Faulty SFP • Unsupported SFP
Recommended Action	Check the cabling and SFP for the port reported in alarm.
Severity	Critical
Element	TD140

TD140-127 RTM failure

Probable Cause	Communications with an RTM have been interrupted.
Recommended Action	Check that the RTM is fully seated. Use the following CLI command to verify RTM: mcli->platform-mgmt->show frus. The output should display "ATCA-7240-IO RT" in RTM column. If not, try reseating RTM. Contact Customer Support to analyze cause if problem persists.
Severity	Critical
Element	TD140

TD140-128 Voltage levels (all blades)

Probable Cause	Voltage levels to all blades is too high or too low, possibly due to a PPM40 blade not properly installed in chassis.
Recommended Action	Reseat the PPM40 blades. Contact Customer Support to analyze cause if problem persists.
Severity	Critical
Element	TD140

TD140-129 Base switch drops on packet processing blade

Probable Cause	The Base switch routes traffic (mainly the OAM, time sync, or persistency packets) on 1G links internally to various components in the TD140. Possible reasons for packets drops: • Congestion of ports due to excessive traffic • Erroneous packets Alarm displays port number and number of packets dropped.
Recommended Action	If alarm persists, call Customer Support.
Severity	Major
Element	TD140

TD140-130 Fabric switch drops on packet processing blade

Probable Cause	Packets entering the TD140 on the I/O ports reach the load balancer running in the Octeon processors through the fabric switch. Packet drops occur in the fabric switch possibly due to: • Congestion of ports due to excessive traffic • Erroneous packets
Recommended Action	If alarm persists, call Customer Support.
Severity	Major
Element	TD140

TD140-131 CPU packet drops on packet processing blade

Probable Cause	Packets dropped in the load balancer application.
Recommended Action	Use the CLI command *show stats packet-drops* or the stats file *lb_pktdrops.csv* to examine the reason (classification) for packet drops. If the packet drops persist and it is deemed unexpected, call Customer Support.
Severity	Major
Element	TD140

TD140-132 Persistent recovery failure

Probable Cause	Indicates that one or more G10s did not complete the session persistency information download procedure after a TD140 restart.
Recommended Action	Contact Customer Support.
Severity	Major
Element	TD140

TD140-133 Loss of sync with PTP server

Probable Cause	The TD140 has lost sync with the original PTP server.
Recommended Action	From IrisView Admin Probe Management, select a valid PTP server for the TD140. If alarm persists, contact Customer Support.
Severity	Major
Element	TD140

TD140-134 Management port auto negotiation failure

Probable Cause	The OAM port B on the TD140 SHMM has auto-negotiated to incorrect settings. Correct settings should be: • Speed: 1000Mb/s • Duplex: Full
Recommended Action	Check the configuration at the peer end.
Severity	Major
Element	TD140

TD140-135 Incorrect firmware version

Probable Cause	TD140 firmware is incorrect version to support installed applications. This alarm is raised when software upgrade fails and then the subsequent rollback to previous software version also fails to update any of the firmware components in the TD140.
Recommended Action	Contact Customer Support.
Severity	Minor
Element	TD140

XDR Alarms

The following system-level alarms are generated by Iris and appear in the Alarms Dashboard.

XDR-101 Failure to send XDR

Probable Cause	G10 probe failed to send XDR to DataCast server due to one of the following conditions: • Invalid receiver configured • Network issues • DataCast server is unresponsive Profile name, and IP address, and port of DataCast server are reported in alarm.

Recommended Action	Verify the IP Address and Port configured for the DataCast Server are valid for the XDR profile in alarm. See the XDR Profile Management tab in Admin Application Management for details. If alarm persists, contact Customer Support.
Severity	Major
Element	XDR
Alarm trigger default	XDR transmission failure
Alarm clear default	After a configurable amount of time has passed without XDR transmission failure or when all profiles using that connection have been disabled or deleted. This time is configurable by Tektronix.

XDR-102 Connection is not established

Probable Cause	G10 probe connection to DataCast server is lost.
Recommended Action	• Verify the IP Address and Port configured for the DataCast Server are valid for the XDR profile identified in alarm. See the XDR Profile Management tab in Admin Application Management for details. • If alarm persists, contact Customer Support.
Severity	Major
Element	XDR

Alarms Video Demos

The following Alarms video demo is provided in the online help.[1]

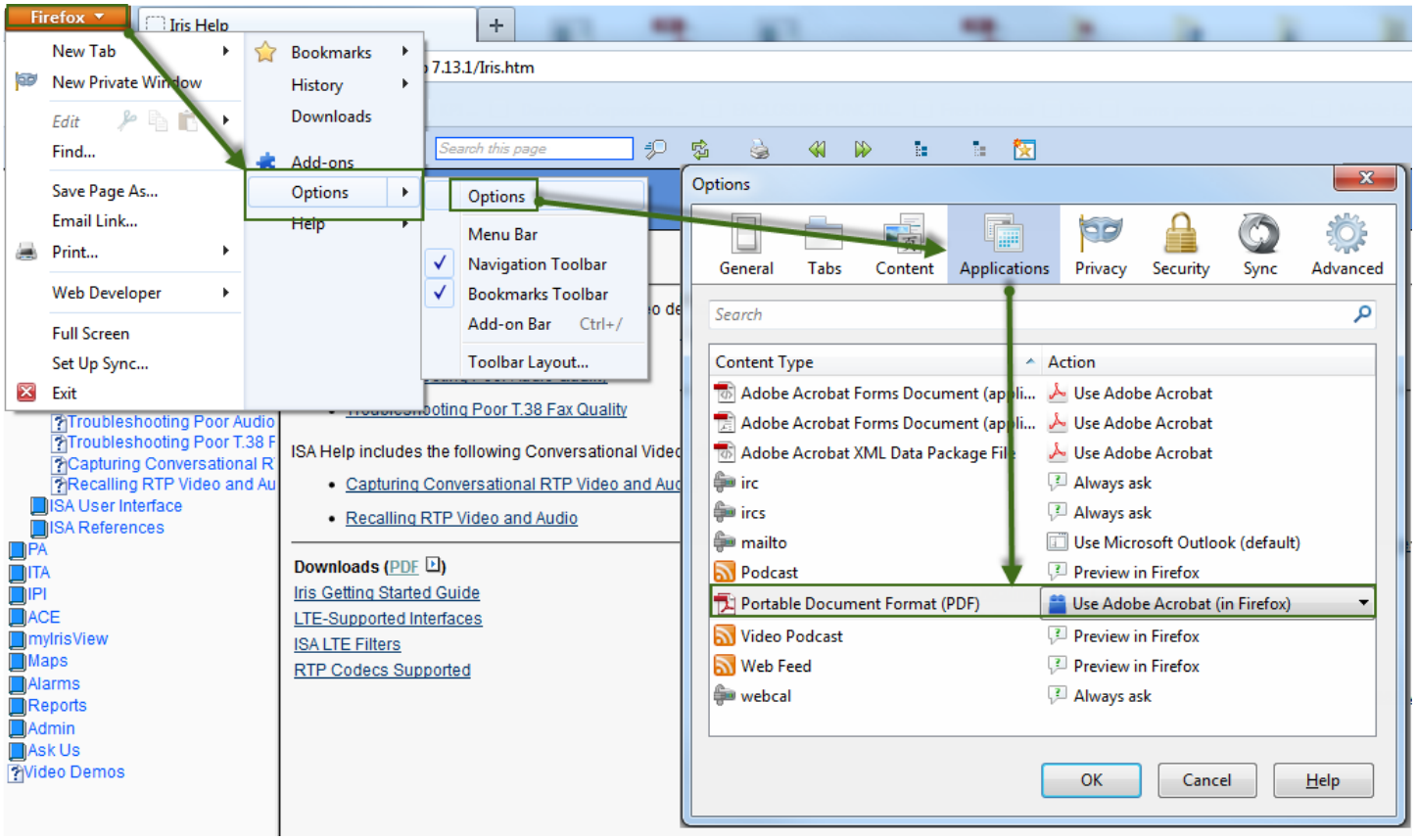
- Using IPI to Detect One-Way Audio

Video Demos in Firefox

If you are using Firefox and are having trouble viewing the PDF video demos, you may need to adjust your browser settings to enable Adobe Acrobat Reader to play them.

Enable Adobe Acrobat Reader in Firefox

1. Select the Firefox menu and then select **Options** from the Options menu.
2. In the Options dialog box, click the **Applications** button and then select **Use Adobe Acrobat (in Firefox)** from the Portable Document Format (PDF) menu.
3. Click **OK** to apply your settings.



1 The content of most video demos refers to a previous release; the user interface may appear slightly different in the current release.