Network Management
User Documentation

Iris Automated Controller Engine User Guide

Version 7.13.2

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

uadocfeedback@tektronix.com (Technical Publications email)

Plano, Texas USA - serves North America, South America, Latin America
+1 469-330-4581 (Customer Support voice)
uaservice@tek.com (Customer Support USA email)

London, England UK - serves Northern Europe, Middle East, and Africa
+44-1344-767-100 (Customer Support voice)
uaservice-uk@tek.com (Customer Support UK email)

Frankfurt, Germany DE - serves Central Europe and Middle East
+49-6196-9519-250 (Customer Support voice)
uaservice-de@tek.com (Customer Support DE email)

Padova, Italy IT - serves Southern Europe and Middle East
+39-049-762-3832 (Customer Support voice)
uaservice-it@tek.com (Customer Support IT email)

Melbourne, Australia - serves Australia
+61 396 330 400 (Customer Support voice)
uaservice-ap@tek.com (Customer Support Australia and APAC email)

Singapore - serves Asia and the Pacific Rim
+65 6356 3900 (Customer Support voice)
uaservice-ap@tek.com (Customer Support APAC and Australia email)

Tektronix Communications, Inc. Proprietary Information
992-0434-08-001-140228

Table of Contents

CHAPTER 1: INTRODUCTION TO ACE

This chapter provides an overview of the Iris Automated Controller Engine (ACE) application which is a component of the Iris Network Intelligence solution. ACE is part of the Iris Assurance toolset, a set of network and service monitoring applications that enable the assessment and proactive management of both the customer experience and end-to-end service quality.

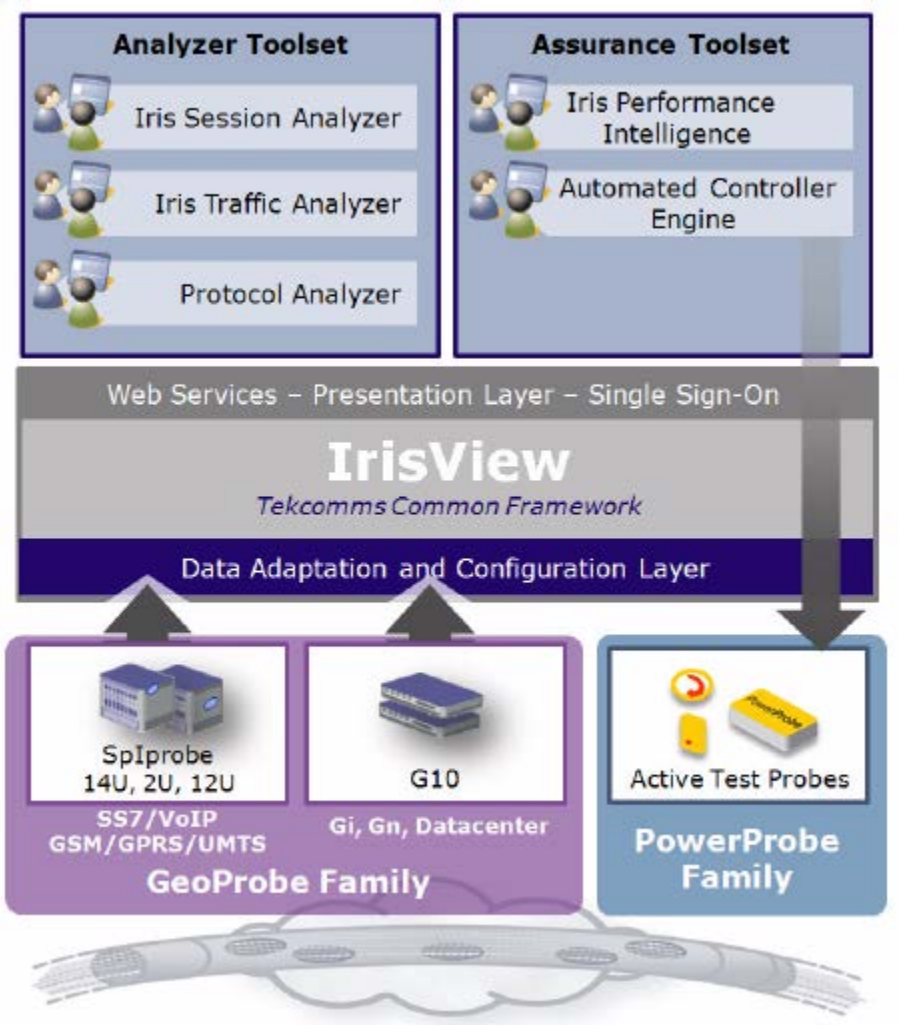

Figure 1 – Iris Network Intelligence Solution

ACE Overview

Going far beyond simple GUI integration, the Iris Automated Controller Engine (ACE) application enables automated, intelligent interworking between Tektronix Communication's best-in-class network monitoring and active test solutions. ACE provides the ability to automatically launch actions, such as active tests, driven by the network intelligence data monitored and correlated by the GeoProbe family of passive probes.

Automating troubleshooting workflows with ACE allows Service Providers to resolve issues faster by focusing resources on analyzing root causes, rather than on time-consuming data collection tasks and manual trial-and-error testing. The rules-based IrisView Policy Engine allows users to define the specific network conditions or events which trigger ACE to take action. ACE provides users with a dashboard which brings together a summary of the incoming events correlated with the results of the corresponding active tests.

ACE includes the following features:

- ☐ Define policies that identify specific network issues or events, such as call failures, low MOS or one-way audio problems.
- ☐ Automatically run active tests and other actions to verify, isolate, and quantify the impact of these network events.
- ☐ Drill-down to additional event details, including the list of affected subscribers and the associated session traces for the failed calls.
- ☐ View a summary of which events occurred and where they are occurring, together with the results of the automated actions.

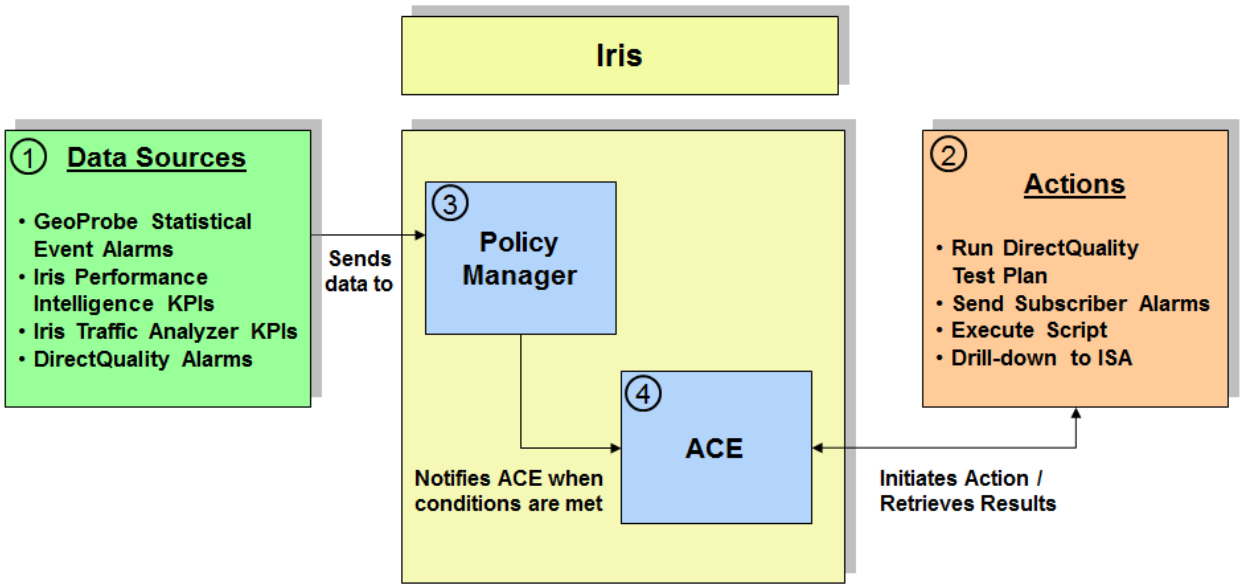

Figure 2 – ACE General Workflow

Table 1 describes the process flow for configuring ACE to automate actions when the data inputs meet specific conditions.

Table 1 – ACE Process Flow Description

Step	Process
1	Configure the systems that provide the data inputs for ACE. Refer to Chapter 2 for more information on ACE Data Sources.
2	Configure the systems that ACE initiates actions to or retrieves data from. Refer to Chapter 3 for more information on ACE Target Systems.
3	Configure policies that define the conditions that will trigger ACE to take action. Refer to Chapter 4 for more information on configuring ACE Policies.
4	Use the ACE Configuration Tools to map policies to actions and use the ACE Dashboard to view the status of the policies and actions. Refer to Chapter 5 for more information on ACE configuration, and to Chapter 6 for more information on the ACE Dashboard.

CHAPTER 2: UNDERSTANDING INPUTS AND DATA SOURCES

This chapter describes the systems that can input data to ACE. These systems provide the data about your network that is used by the policies to determine when ACE is notified.

GeoProbe Statistical Event Alarms

Overview

The GeoProbe Statistical Event Alarms enable you to generate alarms based on the conditions you set on the statistical counters measured by the SpIprobes. The GeoProbe system supports statistical packages for many protocols, services, and interfaces which enable you to generate alarms to meet specific needs. Availability of these packages depends on the applications installed on your GeoProbe system. For more information about configuring Statistical Event Alarms, refer to the GeoProbe Alarms Guide.

Key Performance Indicators and Dimensions

The GeoProbe Statistical Event Alarms data source provides the following KPIs for use in ACE policies:

- Number of Statistical Event Alarms – a count of the number of statistical event alarms forwarded by the SpIserver.

The GeoProbe Statistical Event Alarms data source provides the following Dimensions for use in ACE policies:

- Alarm Number – trigger on a particular user-defined alarm number
- Source Probe – trigger on a particular SpIprobe that generates the statistical event alarm

Iris Performance Intelligence KPIs

Overview

The Iris Performance Intelligence application provides extensive metrics for complete visibility into network and service performance. Through flexible application modeling, the IPI KPIs enable ACE to trigger actions when there are issues with service accessibility, retainability, or performance. KPI availability depends on the packages installed on your Iris system.

Key Performance Indicators and Dimensions

The Iris Performance Intelligence application provides a variety of network and service KPIs for use in ACE policies. The following KPI packages are available for use with ACE. For a complete list of KPIs supported, refer to Appendix A in the Iris Performance Intelligence User Guide.

- Voice Signaling KPIs
- Voice Media KPIs
- Voice Session KPIs
- Voice Call QoS KPIs

The IPI KPI data source provides the following Dimensions for use with ACE:

- Source Node – trigger on KPIs for a particular node that is the source of the traffic
- Destination Node – trigger on KPIs for a particular node that is the destination of the traffic

Iris Traffic Analyzer KPIs

Overview

The Iris Traffic Analyzer application provides visibility into a carrier's network traffic to monitor performance and usage of the following network resources—Links, Applications, Nodes, and Node Groups. Through continuous monitoring and analysis of the traffic characteristics, the ITA KPIs enable ACE to trigger actions when there are issues with network performance or deviations from defined baselines. KPI availability depends on the packages installed on your Iris system.

Key Performance Indicators and Dimensions

The Iris Traffic Analyzer application provides a variety of network performance KPIs for use with ACE. For a complete list of KPIs supported, refer to Appendix A in the Iris Traffic Analyzer System Features Document.

- Traffic Volumes
- Application Response Times
- Retransmissions
- Ethernet Errors

The ITA KPI data source provides the following Dimensions for use with ACE:

- Protocol/Application – trigger on KPIs for a particular network protocol or application as defined by URL or port numbers
- Link – trigger on KPIs for a particular network interface link
- Server – trigger on KPIs for a particular Server network element

DirectQuality Alarms

Overview

The DirectQuality active test platform provides alarm notifications when test measurements fail to meet user-defined thresholds. Using these DirectQuality threshold alarms as a data source enables ACE to automate actions based on the results of active tests. For more information about configuring DirectQuality alarms, refer to the DirectQuality Admin Guide.

Key Performance Indicators and Dimensions

The DirectQuality Alarms data source provides the following KPIs for use in ACE policies:

- Number of Threshold Alarms – a count of the number of threshold alarms forwarded by DirectQuality.

The DirectQuality Alarms data source provides the following Dimensions for use in ACE policies:

- Called Number – trigger on alarms for a particular test destination phone number
- Originating Probe – trigger on alarms for a particular originating PowerProbe
- Test Type – trigger on alarms for a particular active test type

CHAPTER 3: UNDERSTANDING ACTIONS AND TARGET SYSTEMS

This chapter describes the actions that ACE can initiate upon notification of a network issue or event. These actions enable ACE to automate activities and workflows that support your service assurance processes.

DirectQuality

Overview

The DirectQuality active test system provides visibility into your customer's Quality of Experience by proactively quantifying service levels through testing, alarming and service level reporting. The active tests are conducted by the PowerProbe family of test probes, which support a variety of test types designed for particular applications such as measuring voice quality, validating call routing, or determining fax and data service performance. Availability of these test types depends on the licenses installed on your DirectQuality system. For more information about the active test types, refer to the DirectQuality User Guide.

Actions

The DirectQuality target system enables ACE to initiate the following actions:

- DirectQuality Test – generates the active tests defined in a test plan. Test plans are created using XML files and generated using GatewayDQ, an API provided by DirectQuality. Refer to the GatewayDQ User Guide for information on the XML file format.

SNMP Alarms

Overview

The IrisView Policy Manager provides the ability to generate SNMP alarms based on performance thresholds. These alarms are typically forwarded to third-party systems, such as fault management systems, to notify Network Operations teams about network issues. ACE has the ability to enrich these threshold alarms with additional levels of detail or data needed to support your business processes.

Actions

ACE can generate the following types of alarms:

- Per-Subscriber Alarms – generates an SNMP trap for Iris Performance Intelligence (IPI) KPI failures. The alarms contain address information for the affected subscribers as well as details on the failing KPI values. An alarm is transmitted for each failed call to one or more SNMP destinations defined by the user.

Scripts

Overview

The Script Execution action type enables you to create custom actions for your ACE policies. ACE can automatically launch user-defined Linux scripts, enabling a wide variety of actions on proprietary or third party systems. You can trigger your scripts using any of the ACE data sources, including IPI KPIs, ITA KPIs, GeoProbe and DirectQuality alarms, providing customized workflows to support your business processes.

Actions

ACE can execute the following type of script actions:

- Script Execution – launches a user-defined Linux Bash shell script

CHAPTER 4:
MANAGING ACE POLICIES

This chapter describes the process for creating and managing policies for ACE. You use the Iris Policy Management application to create policies that define the conditions that trigger ACE to initiate an action.

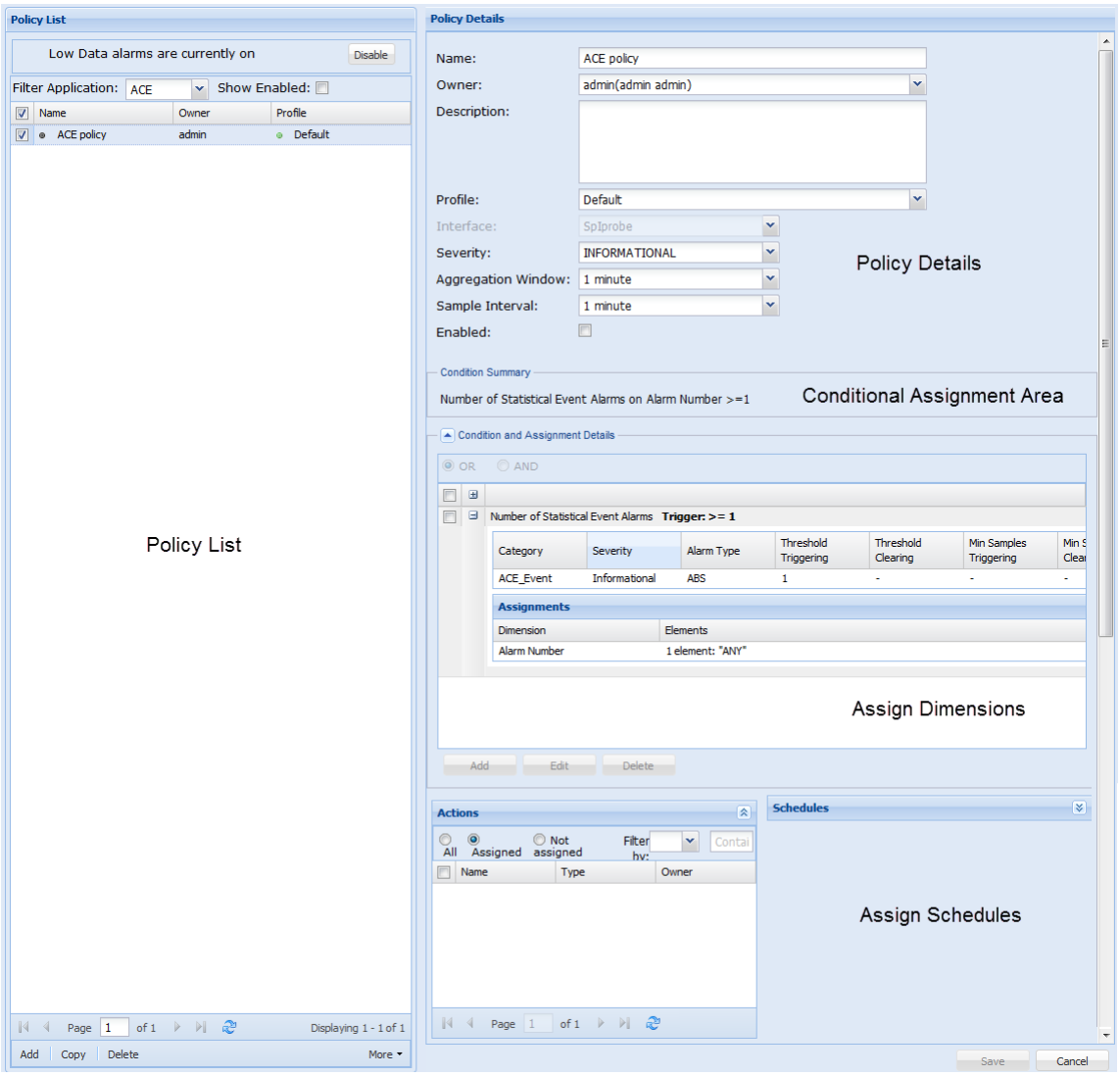

Figure 3 – Iris Alarm Policy Management Page – ACE Policies

Creating ACE Policies

You create policies for ACE using the following high level process:

1. Create a policy template for each data source and KPI type.
2. Create a policy and select the template you created.
3. Assign the Notify ACE action to your policy.
4. Assign a schedule to your policy (optional, see online help for scheduling details).
5. Assign dimensions to your policy to limit the scope of the KPIs.
6. Enable the policy.

ACE Action Template

The Notify ACE action template is pre-configured on your system when ACE is licensed. No additional configuration is required. The Email and SNMP action templates are also supported by ACE policies. Refer to the Online Help for more information on these action types.

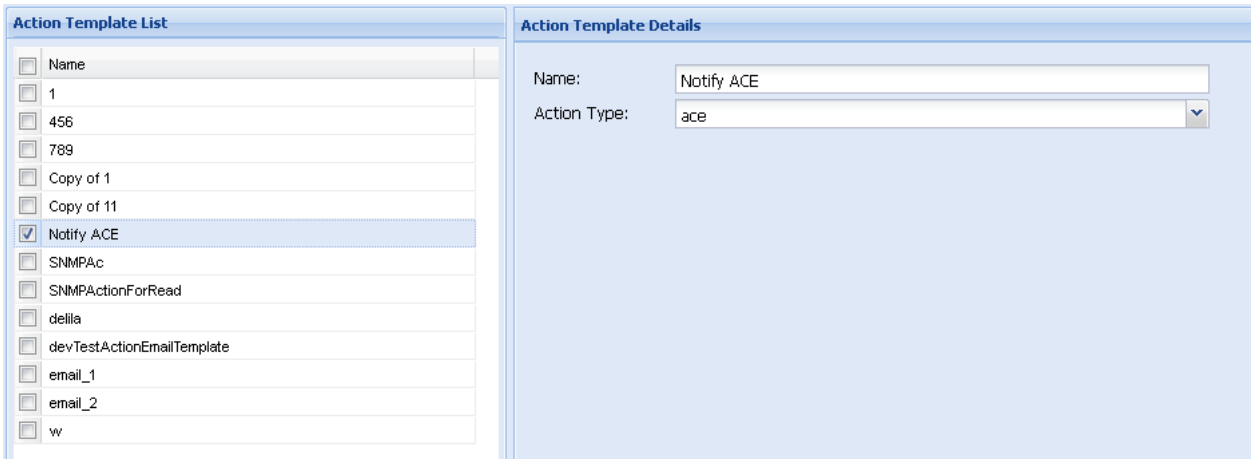

Figure 4 – Notify ACE Action Template

The Notify ACE action can be added to ACE, IPI and ITA policies. The following procedures describe how to create an ACE policy for Statistical Event Alarms. Refer to the ACE Online Help for procedures on how to create an ITA or IPI policy that triggers ACE actions.

ACE Policies

ACE policies apply specific conditions on the KPI defined in the policy template. The following process describes how to create a policy for GeoProbe Statistical Event alarms.

1. Click the Policies tab in the Alarms Application Policy Management page. Click the Add button to create a new policy.
2. Select ACE from the Select Application window.
3. Enter a name and optional description for the policy.
4. Select the severity, aggregation window, and sample interval for the alarm.
5. Enable the policy by clicking the Enabled check box.
6. In the Actions dashlet, select the Notify ACE action.

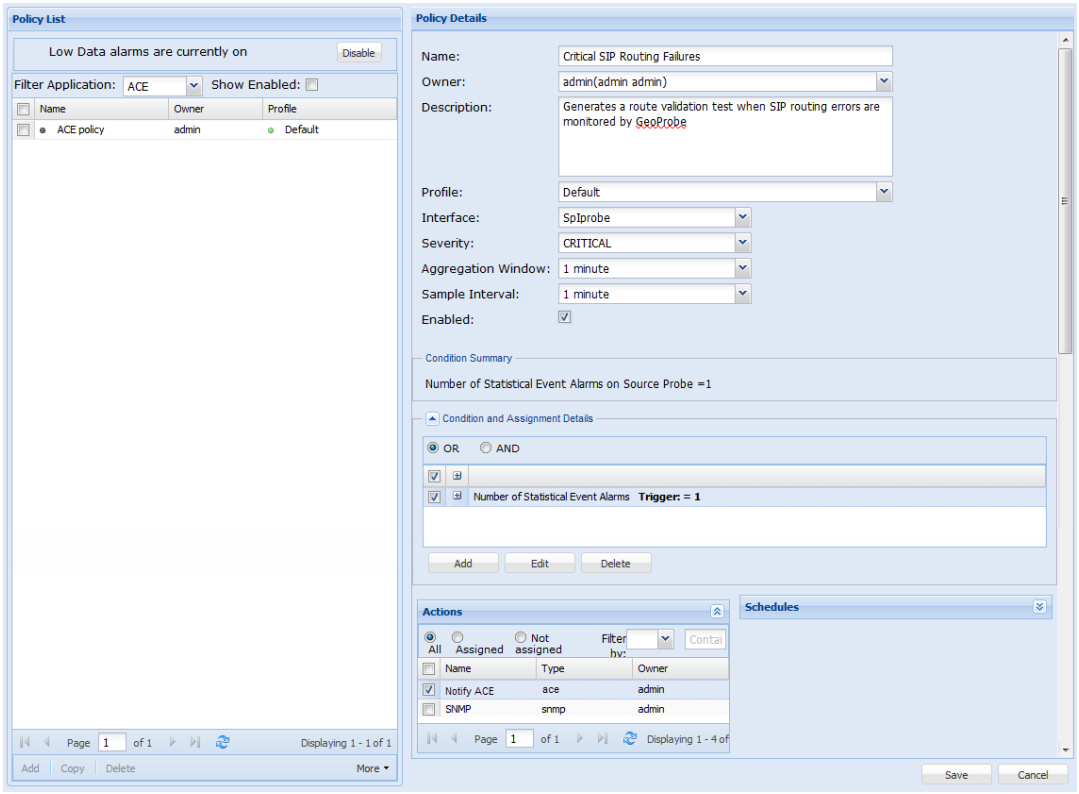

Figure 5 – Defining a New ACE Policy

7. At the bottom of the Condition area, click Add to open the Condition and Assignment Editor window.
8. In Category, select ACE_Event.
9. In KPI/KQI, select Number of Statistical Event Alarms.
10. Select the alarm conditions and trigger for the alarm.

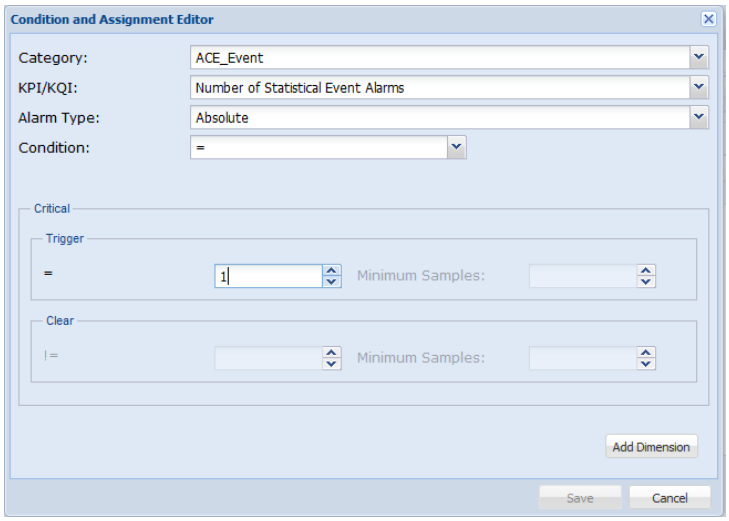

Figure 6 – Assigning Conditions for Statistical Event Alarms

11. Click Add Dimension to add a dimension for the alarm.
12. In Dimension, select Alarm Number and select the Choose option to select the alarm number you assigned to the Statistical Event Alarm you created on the SpIserver.

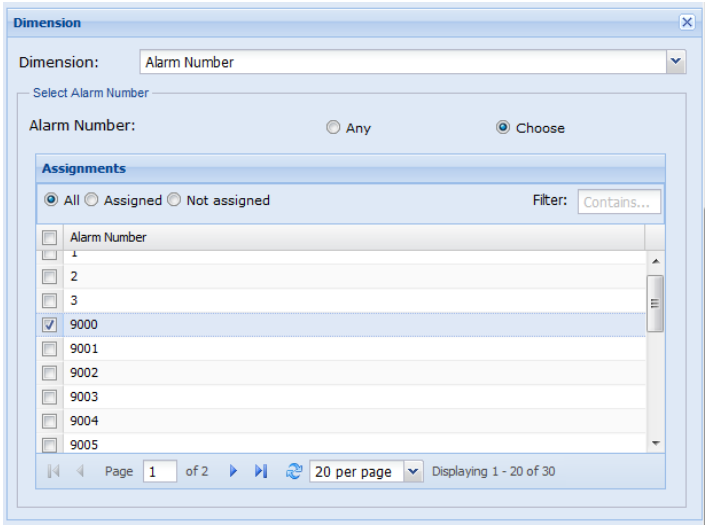

Figure 7 – Assigning Dimensions for Statistical Event Alarms

13. Click Save to save the dimension assignment to the policy. The Condition and Assignment Editor window closes.
14. Click Save on the Policy Details pane to save the policy.

This policy will notify ACE whenever an alarm containing the specified alarm number is received from the SpIserver. ACE will initiate an action based on the mapping defined using the ACE Deployment tools.

Using the Alarm Dashboard

The Alarm Dashboard provides a unified view of alarms across all Iris applications, enabling you to view alarms/events from different applications as well as system-level alarms simultaneously. You access this dashboard by clicking the Alarm Dashboard button in the Alarms toolbar. The Alarm Dashboard provides the following features for viewing alarms resulting from ACE policies.

- ☐ Alarm Browser – view detail information about any alarm and drill down further to validate alarm details such as time of occurrence, element type, alarm description and threshold values.
- ☐ Alarm Distribution by Severity (Pie Chart) – view alarm severity based on an aggregated percentile distribution of alarms: Critical, Major, Minor, and Informational.
- ☐ Alarms by Severity (Bar Chart) – view a breakdown of alarms by time series and volume.

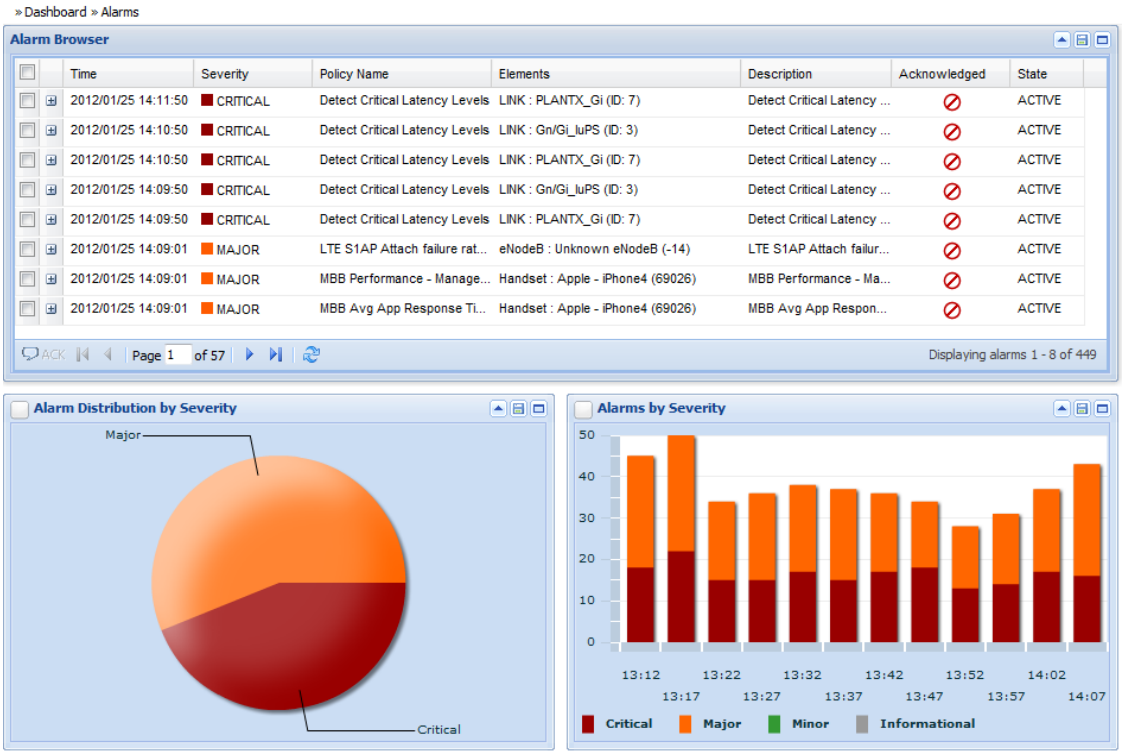

Figure 8 – Iris Alarm Dashboard

CHAPTER 5:
WORKING WITH THE ACE DEPLOYMENT TOOLS

This chapter describes the tools used for mapping ACE policies to actions. Tektronix Service & Delivery provides assistance with this step of the ACE configuration.

ACE Deployment Tools User Interface

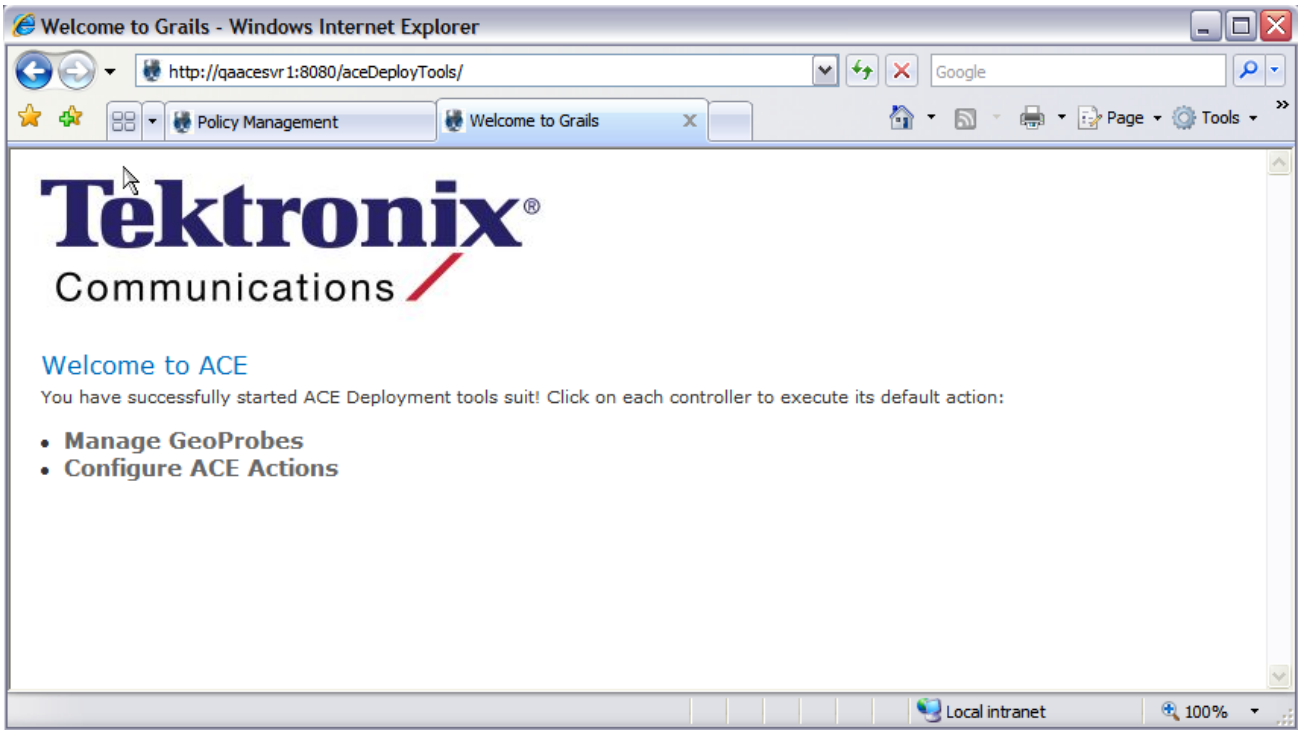

Figure 9 – ACE Deployment Tools Main Page

Source Probe Configuration

The Source Probe configuration tool enables you to define the names of the SpIprobes that will transmit Statistical Event Alarms to ACE. The name defined here must match the name defined on the SpIserver. The ACE Action configuration tool uses the SpIprobe name to determine which test plan to run.

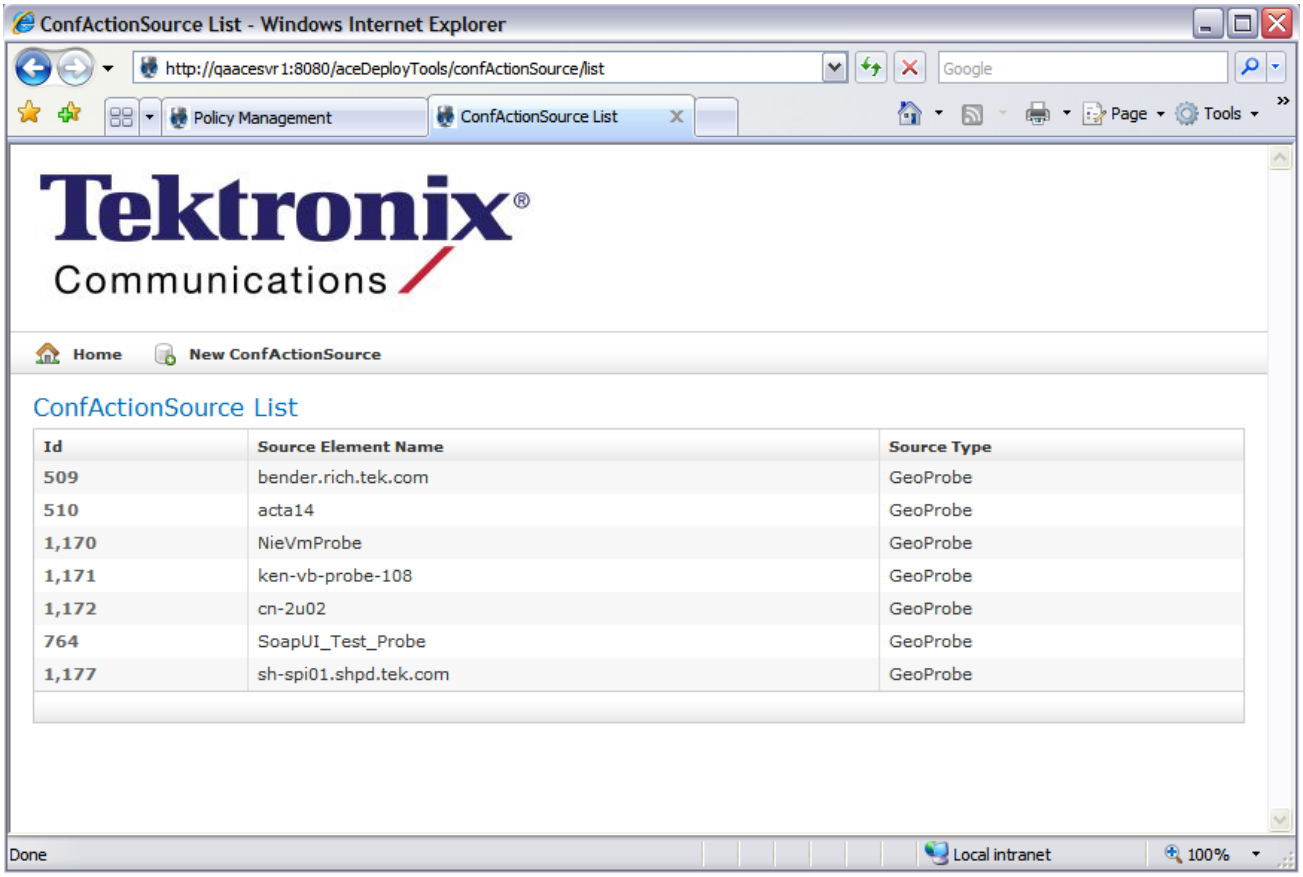

Figure 10 – Source Probe Configuration

ACE Action Configuration

The ACE Action configuration tool enables you to associate your policies with specific actions, for example, the name of the script or DirectQuality test plan to execute. Before creating the ACE Action Configuration, the file that defines the DirectQuality test plan or script must be copied to your ACE server.

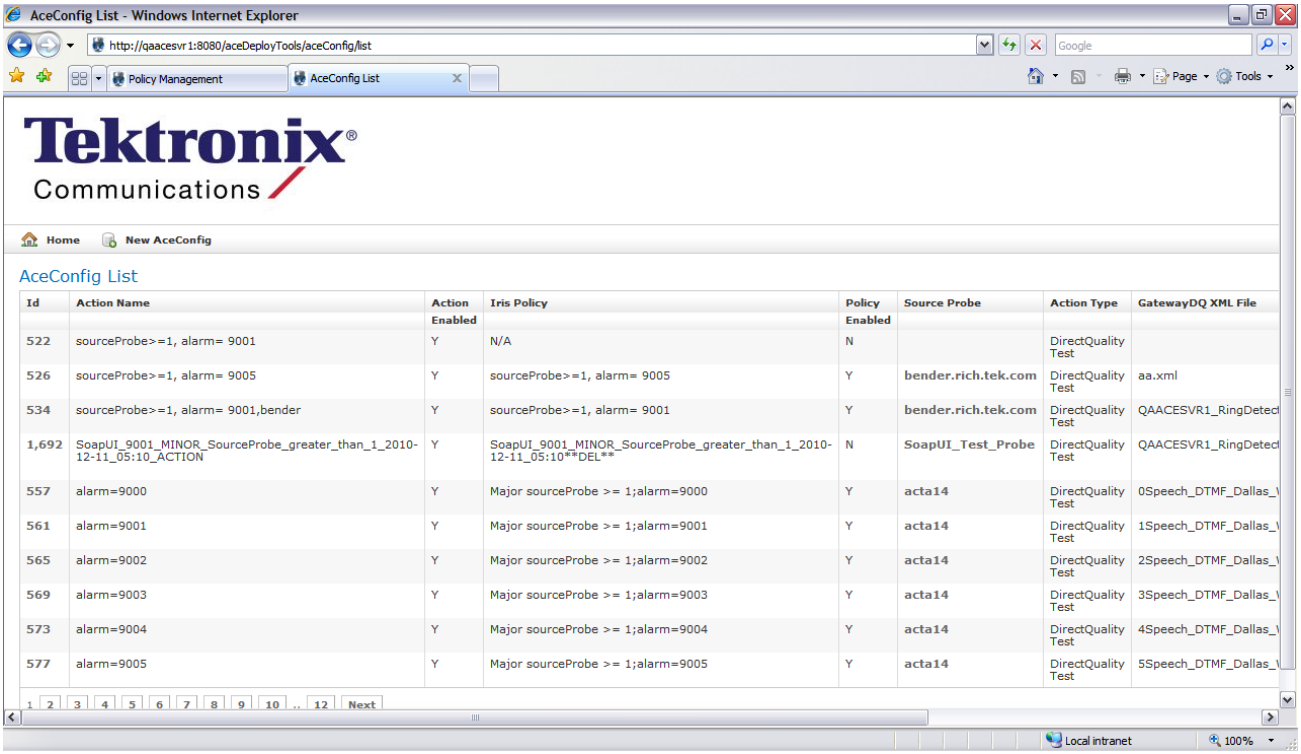

Figure 11 – ACE Policy to Action Mapping

The following process describes how to associate a policy with an action.

1. Select Configure ACE Actions from the ACE Deployment Tools main page.
2. Click the New ACEConfig button to create a new action mapping.
3. Select one of the action options from the Action type list.
4. Enter a name for this action.
5. Select your ACE, ITA or IPI policy name.
6. For IPI policies, enable the “Use Subscriber Info” option to instruct ACE to retrieve the subscriber phone numbers associated with the KPI policy violation, and insert them into the GatewayDQ XML file or SNMP trap.
7. For ACE policies, select a SpIprobe name from the Source Probe list. ACE will launch the specified test plan when receiving Statistical Event Alarms from this SpIprobe.
8. For DirectQuality Test actions, select the GatewayDQ XML file for the test plan you want to associate with the selected policy. You can optionally select an SNMP action template to send a conditional alarm if the test plan fails.
9. For SNMP Trap actions, select name of the SNMP action template that corresponds to the destination for the alarm.

10. For Script Execution actions, select the name of the file that contains the script definition.
11. Click the Create button to save the action mapping.

Repeat this process for each action you want ACE to execute for your policy (e.g. a test plan and a script).

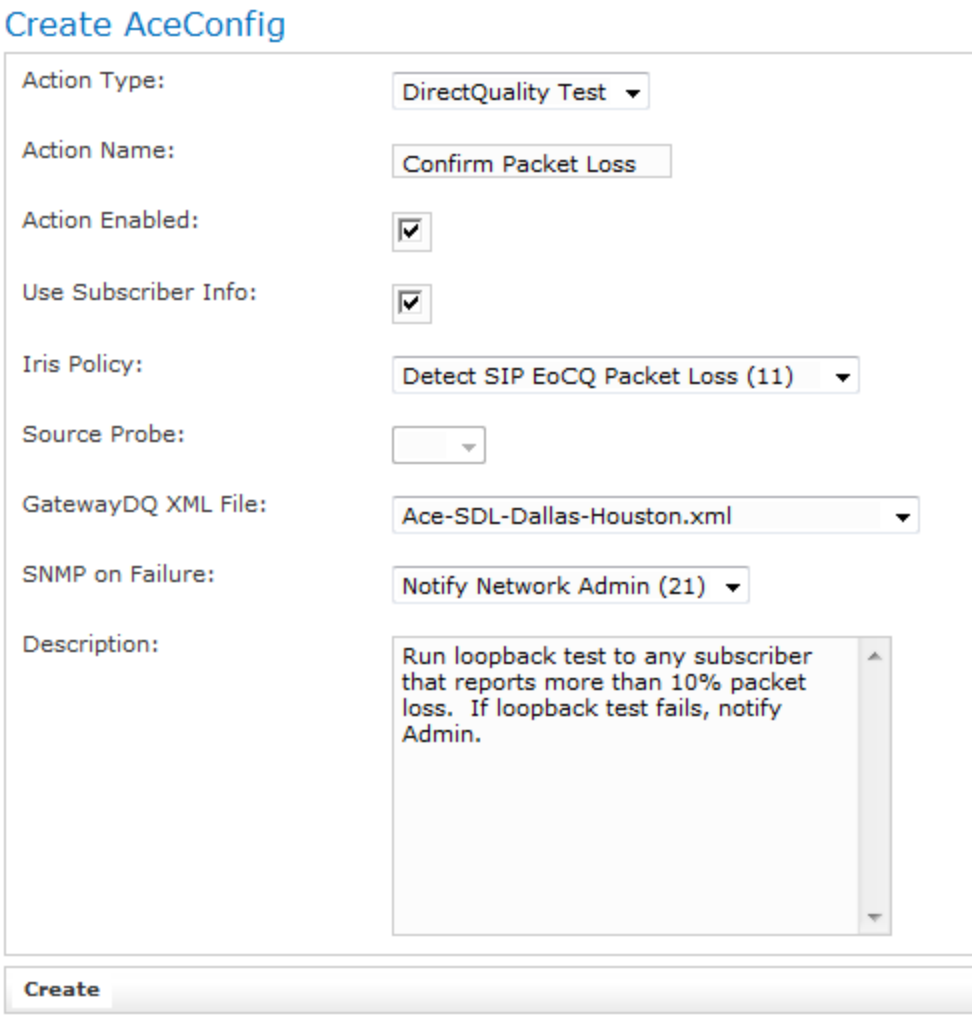

Figure 12 – Action Mapping for an IPI Policy

CHAPTER 6:
WORKING WITH THE ACE DASHBOARD

This chapter describes the graphical user interface components of the ACE Dashboard.

Dashboard User Interface

You access the ACE Dashboard by clicking on the ACE button on the Iris toolbar.

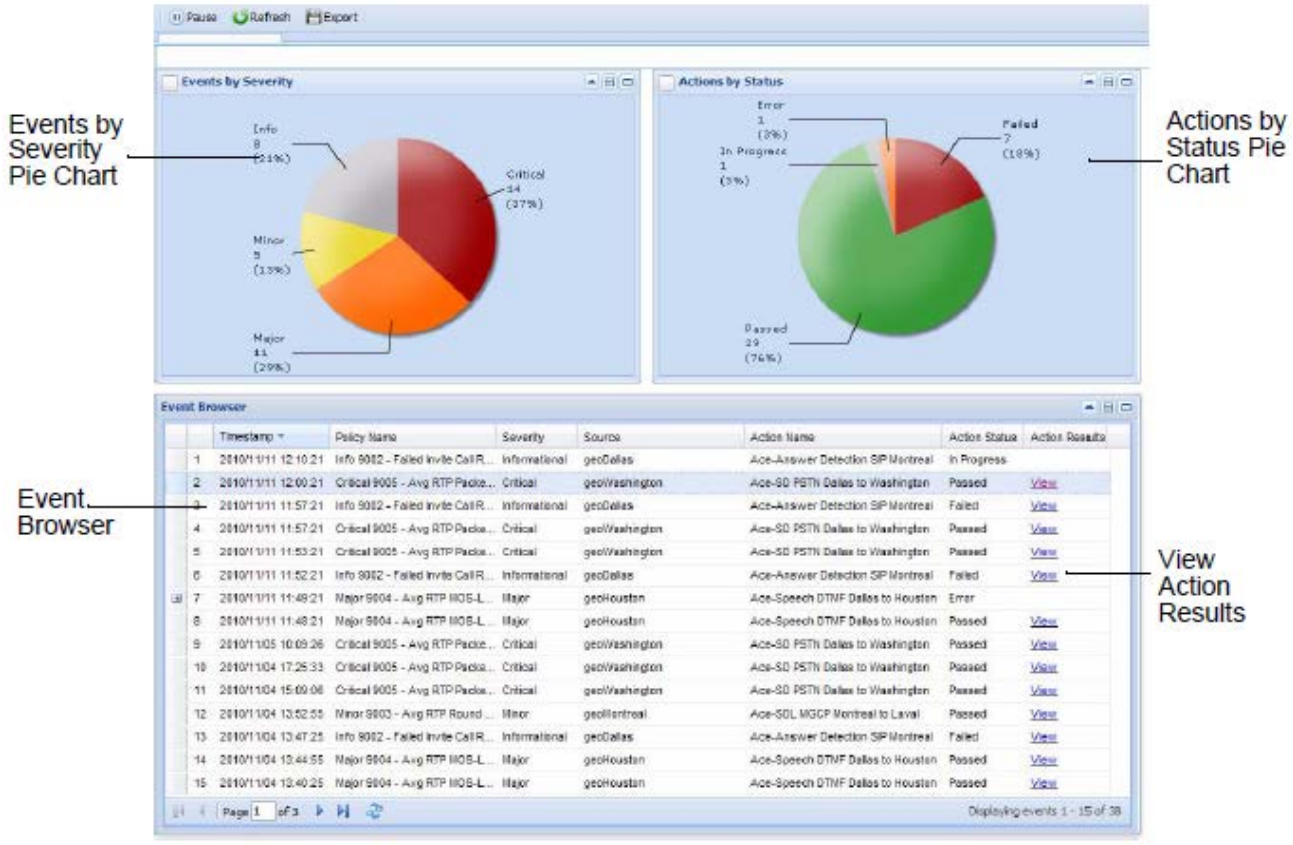

Figure 13 – ACE Dashboard

The ACE Dashboard contains the following components.

Events by Severity Pie Chart

The Events pie chart displays event severity based on an aggregated percentile distribution of events: Major, Critical, Minor, or Informational. You define the severity of an event when you create a policy for that event in the Policy Manager. Select a slice on the pie chart to filter the dashboard using the selected severity.

Actions by Status Pie Chart

The Actions pie chart displays action status based on an aggregated percentile distribution of actions: Passed, Failed, In Progress, or Error. The status is determined from the test results returned by the Target System. Select a slice on the pie chart to filter the dashboard using the selected status.

Event Browser

The Event Browser displays detailed information about all of the events together with the results of the initiated actions. You can click the View link for each event to open a CSV file containing the full set of results from the active tests.

When the event is based on an IPI KPI related to individual calls, you can click the + symbol in the first column to view the phone numbers associated to the failing calls. You can click on the phone numbers to open the Iris Session Analyzer application to view the ladder diagram for the failed call. You must have the ISA user role to access the ISA drill-through feature.

If the test results contain an error, you can click the + symbol in the first column to view the error details.

Global Filters

You can filter the ACE Event Browser by time or by any of the column values. You can also disable the Automatic Refresh option to freeze the data displayed in the dashboard. The ACE Dashboard supports the following event filter options:

- ☐ Start Date / Time – Enter the time
- ☐ End Date / Time – Enter the time
- ☐ Policy Name – Enter the text to search for; wildcards are supported.
- ☐ Severity – Select One: Critical, Major, Minor, or Informational
- ☐ Source – Enter the text to search for; wildcards are supported.
- ☐ Action Name – Enter the text to search for; wildcards are supported.
- ☐ Action Type – Select One: DirectQuality Test, SNMP Trap, or Script Execution
- ☐ Action Status – Select One: Passed, Failed, Error, In Progress, Preparing, Sent, Executed

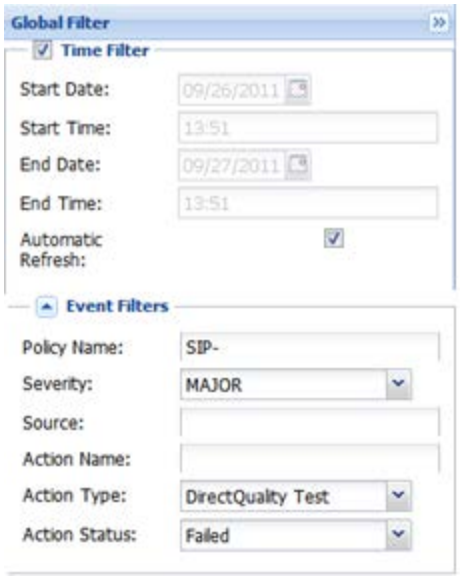

Figure 14 – ACE Event Filters

You can specify multiple filter criteria, which will be combined using the AND operator. The Severity and Action Status filters can also be enabled by selecting slices on the pie charts.

Dashboard Configuration

The ACE Dashboard supports the following customization options:

- ☐ You can move, resize or close the pie charts or Event Browser panels.

- ☐ You can sort the Event Browser by any column by clicking on the column headers.
- ☐ You can add or remove the Event Browser columns by right-clicking on the column headers.
- ☐ You can change the order of the Event Brower columns by clicking and dragging the column headers.

CHAPTER 7:
ACE BEST PRACTICES

The procedure described in this chapter provides a high-level process for using ACE to validate potential impacts to service quality in your network.

ACE Planning Process

1. Define the impairments to service quality that you want validate with automated active tests. Some examples are: one-way audio issues, high levels of packet loss, or SIP registration failures.
2. Find an instance of the issue in the Iris monitoring system and determine how Iris classifies or recognizes this problem. For example, the RTP Packet Count statistic is equal to 0 when there is a one-way audio problem.
3. Define the test plan strategy:
    a. Which active test type can validate the problem or provides measurements that can help troubleshoot the problem?
    b. For each source probe or node, where should the test call originate? Where should the test call terminate?
    c. How many tests are required to validate or quantify the problem?
    d. Are multiple test points required to segment or isolate the issue?
    e. If the tests fail, who should be notified?

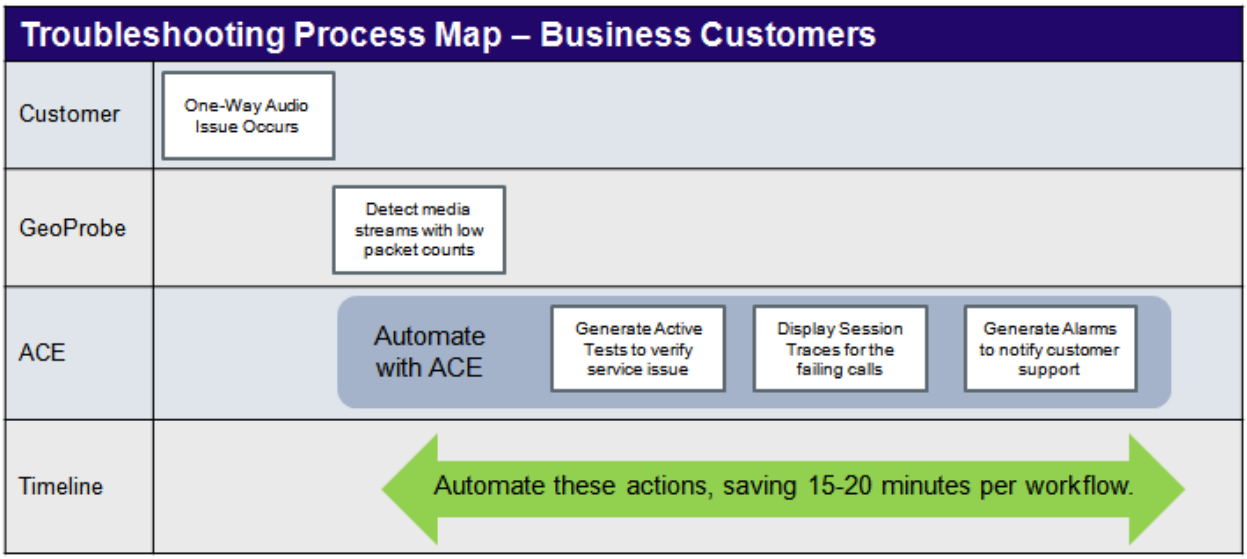

Figure 15 – ACE Workflow Planning Example