HP Business Availability Center

for the Windows and Solaris operating systems

Software Version: 8.02

Using Problem Isolation

Document Release Date: June 2009
Software Release Date: June 2009

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

© Copyright 2005 - 2009 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated.

Intel®, Pentium®, and Intel® Xeon™ are trademarks of Intel Corporation in the U.S. and other countries.

Java™ is a US trademark of Sun Microsystems, Inc.

Microsoft®, Windows®, Windows NT®, and Windows® XP are U.S registered trademarks of Microsoft Corporation.

Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California.

Unix® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign-in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support web site at:

http://www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

Table of Contents

Welcome to This Guide **7**
How This Guide Is Organized 7
Who Should Read This Guide 8
Getting More Information 8

PART I: REACTIVE ANALYSIS

Chapter 1: Problem Isolation Reactive Analysis **11**
Reactive Analysis Overview 12
On-demand Monitors 13
Calculating Suspect CI Weights 15
Calculating On-demand Monitor Success Ratios 16
Permissions 16
Problem Isolation and HP Service Manager Integration 16
Deploy Problem Isolation – Workflow 17
Isolate a Problem – Workflow 19
Deploy the Sitescope Problem Isolation Content.zip File 22
Modify Default Suspect Algorithms and On-demand Monitor TQLs 25
Modify Default Suspect CI Weights 26
On-Demand Monitor SQL Scripts 26
Reactive Analysis User Interface 27
Troubleshooting and Limitations 110

PART II: PROACTIVE ANALYSIS

Chapter 2: Problem Isolation Proactive Analysis **117**
Proactive Analysis Overview 118
Expected Transaction Behavior 120
Permissions 122
Configure Proactive Analysis – Workflow 122
Configure Expected Transaction Behavior 123
Proactive Analysis User Interface 123

PART III: REPORTS

Chapter 3: Problem Isolation Reports 151
Problem Isolation Reports Overview.....151
Problem Isolation Reports User Interface.....152

Index.....161

Welcome to This Guide

This guide describes how to configure and work with the Problem Isolation application in HP Business Availability Center.

This chapter includes:

- How This Guide Is Organized on page 7
- Who Should Read This Guide on page 8
- Getting More Information on page 8

How This Guide Is Organized

The guide contains the following parts:

Part I Reactive Analysis

Describes the concepts, tasks and reference information used for reactive analysis in Problem Isolation.

Part II Proactive Analysis

Describes the concepts, tasks and reference information used for proactive analysis in Problem Isolation.

Part III Reports

Describes the concepts, tasks and reference information used for reports in Problem Isolation.

Who Should Read This Guide

This guide is intended for the following users of HP Business Availability Center:

- HP Business Availability Center administrators
- HP Business Availability Center application administrators
- HP Business Availability Center end users

Readers of this guide should be knowledgeable about navigating and using enterprise applications, and be familiar with HP Business Availability Center and enterprise monitoring and management concepts.

Getting More Information

For a complete list of all online documentation included with HP Business Availability Center, additional online resources, information on acquiring documentation updates, and typographical conventions used in this guide, see the *HP Business Availability Center Deployment Guide* PDF.

Part I

Reactive Analysis

1

Problem Isolation Reactive Analysis

This chapter includes the main concepts, tasks, and reference information for reactive analysis in Problem Isolation.

This chapter includes:

Concepts

- Reactive Analysis Overview on page 12
- On-demand Monitors on page 13
- Calculating Suspect CI Weights on page 15
- Calculating On-demand Monitor Success Ratios on page 16
- Permissions on page 16
- Problem Isolation and HP Service Manager Integration on page 16

Tasks

- Deploy Problem Isolation – Workflow on page 17
- Isolate a Problem – Workflow on page 19
- Deploy the Sitescope Problem Isolation Content.zip File on page 22
- Modify Default Suspect Algorithms and On-demand Monitor TQLs on page 25
- Modify Default Suspect CI Weights on page 26

Reference

- On-Demand Monitor SQL Scripts on page 26
- Reactive Analysis User Interface on page 27

Troubleshooting and Limitations on page 110

Reactive Analysis Overview

Problem Isolation includes both reactive analysis, for isolating enterprise problems discovered in HP Business Availability Center, and proactive analysis, for detecting application anomalies and their probable causes. For details on proactive analysis, see "Proactive Analysis Overview" on page 118.

Reactive Analysis enables you to isolate enterprise problems discovered in HP Business Availability Center, and to identify likely suspects, to help find the root cause of a problem. Problems are opened on a specific CI. To isolate a problem, you can:

- revalidate the problem to see if it is still actual, or if its status has changed. For details on revalidating a problem, see "Validation Page" on page 104.
- determine the impact of the problem on SLAs and users. For details on determining the impact of a problem, see "Impact Page" on page 37.
- run an initial analysis on the problem to learn about it from a user and application perspective. From the initial analysis, you can see the problem's behavior over time, which transactions and locations are affected and what errors were received. For details on initial analysis, see "Initial Analysis Page" on page 41.
- run a layer analysis to see the data collected about the problem organized into tiers and categories. From this, you can pinpoint specific layers and infrastructure components for further investigation. For details on layer analysis, see "Layer Analysis Page" on page 59.
- list suspected CIs and view their correlation with the problematic CI. For details on the suspect CIs, see "Suspects Page" on page 97, and for details on correlation, see "Correlation Graph" on page 31.

For a suggested working order for isolating a problematic CI and finding its root cause, see "Isolate a Problem – Workflow" on page 19.

You can display an isolation's properties and update details about the root cause of a problematic CI. For details on viewing and updating an isolation's properties, see "Problem Isolation Properties Page" on page 83. For each isolation you perform a record is saved, which you display and access using the Isolation History page. For details on displaying and accessing isolation records, see "Isolation History Page" on page 54.

You can integrate Problem Isolation with HP Service Manager to link isolation data with HP Service Manager incident or problem data, to create a complete problem management lifecycle. For details on integrating Problem Isolation with HP Service Manager, see "HP Service Manager Integration with Business Availability Center Components" in *Solutions and Integrations*.

You can generate a snapshot of system information pertaining to a problematic CI, which you can save, print, send to other people for later use, or upload to an HP Service Manager incident or problem. This enables you to see what was happening in the system at the time of the problem, even though the actual system status may have changed since then. For details on generating a Problem Snapshot report, see "Problem Snapshot Report" on page 86.

On-demand Monitors

You run on-demand monitors to gather in-depth data on system components, based on a problem's suspects.

On-demand monitors are executed via an intermediary monitor running tool for which, by default, Problem Isolation uses SiteScope.

Problem Isolation provides standard TQLs, SiteScope monitor templates, and correlation rules which are used by the on-demand monitors. The TQLs are automatically available once Problem Isolation has been installed, but the SiteScope monitor templates must be installed and imported manually. For details on installing the SiteScope monitor templates, see "Deploy the Sitescope Problem Isolation Content.zip File" on page 22.

For details on modifying standard correlation rules and TQLs, see "Modify Default Suspect Algorithms and On-demand Monitor TQLs" on page 25.

When a problem is opened, Problem Isolation examines the Universal CMDB and determines which CIs are most suspected of being the main cause of the problem. These CIs are called suspect CIs (for details, see "Suspects Page" on page 97).

For each suspect CI, Problem Isolation determines which monitors are configured to run on the suspect and then uses the Universal CMDB to populate monitor variables from relevant CI attributes.

When the On-demand Monitors page is accessed (for details, see "On-demand Monitors Results Pane" on page 78), the relevant monitors for the suspect CIs are displayed. Problem Isolation can be configured to run on-demand monitors automatically, or you can manually select and run them (for details, see "Notes and Limitations" on page 108).

When an on-demand monitor is selected to run, Problem Isolation uses the Universal CMDB to get the values of selected attributes from various TQL nodes. This data is passed, via variables, to the SiteScope monitor templates for use when running the on-demand monitors.

Note: Most on-demand monitors require the credentials (user name and password) of the resource they are monitoring. For resources that are discovered by Discovery and Dependency Mapping, these credentials are available, but for resources discovered by SiteScope, these credentials are available only for Hosts. For other resources discovered by SiteScope, such credentials are not reported. Without these credentials, the on-demand monitors cannot run successfully. For details on credentials in SiteScope, see "Credential Preferences" in *Using System Availability Management*.

The links between the Universal CMDB, the SiteScope monitor templates, and the Problem Isolation on-demand monitors are configured using the "Suspect CI Monitor Configuration Wizard" on page 93. Changes to existing monitor definitions for suspect CIs in a topology are made using the "Suspect CI Monitor Configuration Page" on page 91.

Calculating Suspect CI Weights

The weight of each suspect CI (that is, how suspect a specific CI is compared to the other suspect CIs), as displayed in the **Suspects** page, is calculated according to the following formula:

Monitors weight, as configured in Problem Isolation infrastructure settings, * (the number of monitors run on the CI that failed / the total number of monitors run on the CI)

plus

Changes weight, as configured in Problem Isolation infrastructure settings, * (log(1 + the number of changes made on the suspect CI) / log(1 + the number of changes made to the suspect CI that has the maximum number of changes of all the suspect CIs))

plus

On-demand monitors weight, as configured in Problem Isolation infrastructure settings, * (the number of on-demand monitors run on the CI that failed / the total number of on-demand monitors run on the CI)

plus

Correlation weight, as configured in Problem Isolation infrastructure settings, * (correlation score / 100). If the correlation score for a suspect CI is 0, it is omitted from the calculation entirely.

plus

Event correlation weight, as configured in Problem Isolation infrastructure settings, * (event correlation score / 100). If the event correlation score for a suspect CI is 0, it is omitted from the calculation entirely.

Failed monitors are those represented by a red circle.

You can modify the default weights used to determine the weighting of suspect CIs. For details, see “Modify Default Suspect CI Weights” on page 26.

Calculating On-demand Monitor Success Ratios

The success rate percentage of an on-demand monitor set to run on a CI, as displayed in the **On-demand Monitors** column on the **Suspects** page, is calculated as the percent of the total weight of the on-demand monitors that were successful, out of the total weight of all the on-demand monitors run for the CI.

For example: three on-demand monitors are run for a CI, with a weight of 2, 3, and 5 respectively. The first two monitors (with weights of 2 and 3) were successful, but the last monitor (with a weight of 5) was unsuccessful. The combined weight of successful monitors is 5 (2 + 3), and the total weight of the monitors run is 10 (2 + 3 + 5). The success ratio is 5 out of 10, or 50 percent.

Monitor weights are configured in monitor profiles. For details on the user interface, see "Edit Monitor Profile Page" on page 35 and "New Monitor Profile Page" on page 74.

Permissions

You must have the Problem Isolation **Advanced User** or **Administrator** role to run on-demand monitors, revalidate transactions, update problem properties, and invoke run books. You must have the Problem Isolation **Administrator** role to configure Problem Isolation. To access the Permissions page, select **Admin** > **Platform** > **Users and Permissions**. For details on this topic, see "Permissions Overview" in *Platform Administration*.

Problem Isolation and HP Service Manager Integration

You can integrate Problem Isolation and HP Service Manager so that isolation data from Problem Isolation is linked to incident or problem data in HP Service Manager. For details on how to perform this task, see "HP Service Manager Integration with Business Availability Center Components" in *Solutions and Integrations*.

Deploy Problem Isolation – Workflow

This task describes the working order for deploying and configuring Problem Isolation.

This task includes the following steps:

- "Prerequisites" on page 17
- "Model Applications" on page 17
- "Deploy the Sitescope Problem Isolation Content.zip File" on page 18
- "Configure the Problem Isolation On-demand Monitors" on page 18
- "Configure Problem Isolation and HP Service Manager Integration – Optional" on page 18
- "Configure Problem Isolation and HP Operations Orchestration Integration – Optional" on page 18
- "Configure Proactive Analysis" on page 18
- "Grant Permissions" on page 19
- "Results" on page 19

1 Prerequisites

The following prerequisites are needed to use the Problem Isolation module:

- SiteScope 8.7 or later
- Business Process Monitor (as supported by HP Business Availability Center)
- Real User Monitor (as supported by HP Business Availability Center) (Optional, if you want to include Real User Monitor data when isolating a problematic CI.)

2 Model Applications

In the HP Universal CMDB, create a view that includes your application and business transaction CIs and their related CIs (infrastructure, business transactions, and so forth). For details on creating views in the HP Universal CMDB, see "Create a Template Based View" in *Model Management*.

3 Deploy the Sitescope Problem Isolation Content.zip File

Deploy the Sitescope Problem Isolation Content.zip file included in Problem Isolation to install the Problem Isolation monitors template and SQL scripts. For details on how to perform this task, see "Deploy the Sitescope Problem Isolation Content.zip File" on page 22.

4 Configure the Problem Isolation On-demand Monitors

Add or change monitor settings to adapt the on-demand monitors for your needs. For details on the user interface, see "Suspect CI Monitor Configuration Wizard" on page 93.

5 Configure Problem Isolation and HP Service Manager Integration – Optional

You can integrate Problem Isolation and HP Service Manager so that isolation data from Problem Isolation is linked to incident or problem data in HP Service Manager. For details on how to perform this task, see "HP Service Manager Integration with Business Availability Center Components" in *Solutions and Integrations*.

6 Configure Problem Isolation and HP Operations Orchestration Integration – Optional

You can integrate HP Business Availability Center and HP Operations Orchestration (OO) so that you can invoke OO run books on suspect CIs. For details on how to perform this task, see "Integrate HP Business Availability Center and HP Operations Orchestration – Workflow" in *Solutions and Integrations*.

For an overview of Business Availability Center and HP Operations Orchestration integration, see "HP Operations Orchestration Integration Overview" in *Solutions and Integrations*.

7 Configure Proactive Analysis

You configure the applications and business services that you want the proactive analysis process to analyze for anomalies. For details on how to perform this task, see "Configure Proactive Analysis – Workflow" on page 122.

8 Grant Permissions

Grant permissions for users to run on-demand monitors, revalidate transactions, update problem properties, invoke run books, and configure Problem Isolation. For details on this topic, see “Permissions” on page 16.

9 Results

You are now able to use Problem Isolation for both reactive analysis, for isolating enterprise problems discovered in HP Business Availability Center, and proactive analysis, for detecting application anomalies and their probable causes.

Isolate a Problem – Workflow

This task describes a suggested working order for isolating a problematic CI and finding the root cause of the problem.

This task includes the following steps:

- “Start an Isolation” on page 20
- “Validate the Problem” on page 20
- “Determine the Impact of the Problematic CI on Your System” on page 20
- “Run an Initial Analysis” on page 20
- “Run a Layer Analysis” on page 21
- “View the Main Suspects Table” on page 21
- “Generate a Problem Snapshot Report” on page 21
- “Escalate the Problem” on page 21
- “View the Correlation Graph” on page 21
- “Update the Root Cause Details” on page 22

1 Start an Isolation

In Dashboard, right-click a problematic CI in the view tree and select **Go to Problem Isolation** from the displayed menu. The Validation page opens. For details on the user interface, see "Validation Page" on page 104.

2 Validate the Problem

Rerunning the transactions affected by the problematic CI enables you to see any changes to their status since the problem was first detected, and determine if the problem is still current.

If your system is configured for automatic revalidation (which is set by default), the transactions for the selected problematic CI are automatically rerun when the Validate page is first accessed. Transactions can also be rerun manually.

For details on the user interface, see "Validation Page" on page 104.

3 Determine the Impact of the Problematic CI on Your System

The Impact step helps you determine the business impact of the problem in your system, which is calculated based on the number of SLAs and users affected by the problematic CI. Knowing its impact helps you prioritize the problem.

For details on the user interface, see "Impact Page" on page 37.

4 Run an Initial Analysis

The Initial Analysis helps you determine possible causes of the problem, while eliminating others.

By checking transactions and locations, the Initial Analysis step enables you to see if a specific transaction or location is experiencing the problem.

You can also investigate errors and events that occurred on both virtual monitors (Business Process Monitors) and Real User Monitors. If your system is configured for snapshot on error, you can view the relevant snapshots.

The initial analysis also enables you to view the status of the problem's KPIs over time.

For details on the user interface, see "Initial Analysis Page" on page 41.

5 Run a Layer Analysis

The Layer Analysis analyzes the system characteristics of a problem and shows how each system layer affects a transaction. The back end layer is further broken down into tiers and categories and this enables you to focus on a specific layer, tier and category.

For details on the user interface, see "Layer Analysis Page" on page 59.

6 View the Main Suspects Table

For problems residing in the server layer, you view the list of main suspects to further analyze the CIs that are most likely causing the problem, from different perspectives (such as deployed monitors, discovered changes, on-demand monitor results, and so forth).

For details on the user interface, see "Suspects Page" on page 97.

7 Generate a Problem Snapshot Report

You can generate a snapshot of system information pertaining to a problematic CI, which you can save, print, send to other people for later use, or upload to an HP Service Manager incident or problem. This enables you to see what was happening in the system at the time of the problem, even though the actual system status may have changed since then.

For details on the user interface, see "Problem Snapshot Report" on page 86.

8 Escalate the Problem

Escalate the problem as needed for further investigation and resolution.

9 View the Correlation Graph

The correlation graph shows the correlation between the problematic CI and those CIs suspected of being the root cause of the problem, as well as any changes made to the problematic CI. This enables you to determine patterns that can assist in finding the root cause of the problem.

For details on the user interface, see "Correlation Graph" on page 31.

10 Update the Root Cause Details

Once determined, update the problem's root cause details for future reference and to help create a knowledge base.

For details on the user interface, see "Problem Isolation Properties Page" on page 83.

Deploy the Sitescope Problem Isolation Content.zip File

This task describes how to deploy the Sitescope Problem Isolation Content.zip file included in Problem Isolation to install the following:

- **Problem Isolation monitors template.** The template container of the SiteScope monitor templates used by Problem Isolation on-demand monitors to gather information on a problem's suspect CIs.
- **SQL scripts.** Used by a number of on-demand monitors when gathering information on a problem's suspect CIs. For details on the SQL scripts, see "On-Demand Monitor SQL Scripts" on page 26.

The Sitescope Problem Isolation Content.zip is located in the **Windows_Setup** and **Solaris_Setup** directories on the HP Business Availability Center DVD.

To deploy the Sitescope Problem Isolation Content.zip file:

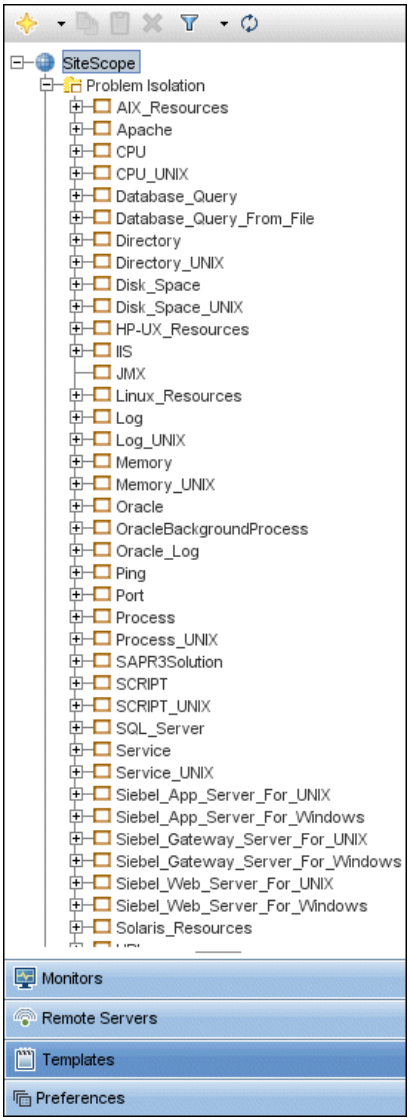
Extract the file content to the **SiteScope root directory** on each of the SiteScope machines in your system on which you plan to run Problem Isolation on-demand monitors. Make sure to use the folder names to keep the directory structure. Once the file is extracted, SiteScope automatically adds a template container called **Problem Isolation** to its configuration, and imports the Problem Isolation monitor templates.

If the Problem Isolation template container is not added automatically, you can create it manually and then import the **PMTemplates** file from the **SiteScope\export** directory. For details on importing template files in SiteScope, see "Import Template Dialog Box" in *Using System Availability Management*.

Note: Once the monitor templates have been imported, the templates, monitors, and variables can only be managed directly on the SiteScope machines, and not with System Availability Management Administration in HP Business Availability Center. For details on managing the templates, monitors, and variables directly in SiteScope, refer to the SiteScope documentation.

Example

After deploying the Sitescope Problem Isolation Content.zip file to the **SiteScope root directory** of a SiteScope machine, and importing the **PMTemplates** file, the templates, monitors, and variables can be viewed and managed on the SiteScope machine.



Modify Default Suspect Algorithms and On-demand Monitor TQLs

If you want to modify one of the default suspect algorithms (that is, a suspect correlation rule), or an on-demand monitor TQL, included in the standard Problem Isolation package, you should make a copy of the rule or TQL and modify the copy. This ensures that your changes are not overwritten if a new Problem Isolation package is deployed.

To copy a default suspect algorithm:

1. Select **Admin** > **Universal CMDB** > **Modeling** > **Correlation Manager**.
2. Right-click the rule you want to change under **Root** > **PM** and click the **Save As** option.
3. Enter a different name for the new rule. If the original rule is a suspect rule (that is, it begins with **PM_SUSPECTS**) make sure that the new rule's name also begins with **PM_SUSPECTS**.
4. Click **OK**.
5. Modify the new rule as required.

To copy an on-demand monitor TQL:

1. Select **Admin** > **Universal CMDB** > **Modeling** > **Query Manager**.
2. Right-click the TQL you want to change under **Root** > **Correlation** > **PM_Diagnostic** and click the **Save As** option.
3. Enter a different name for the new TQL.
4. Select **Integration** as the **type** of file to save.
5. Click **OK**.
6. Modify the new TQL as required.

Modify Default Suspect CI Weights

You can modify the default weights used in calculating the weight of suspect CIs. For details on how suspect CI weights are calculated, see "Calculating Suspect CI Weights" on page 15.

To modify the default values used in suspect CI weighting:

To modify the default weights used in determining the weighting of suspect CIs, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, locate the following entries in the **Main Suspects** table, and modify their values accordingly:

- Changes weight
- Correlation weight
- Event correlation weight
- On-demand monitors weight
- Monitors weight

On-Demand Monitor SQL Scripts

A number of Problem Isolation's on-demand monitors use SQL scripts when gathering information on a problem's suspect CIs. The SQL scripts are installed on SiteScope machines when you deploy Problem Isolation. For details on deploying Problem Isolation, see "Deploy the Sitescope Problem Isolation Content.zip File" on page 22.

The following table lists the on-demand monitors that use an SQL script, and the name of the script used.

On-demand Monitor	SQL Script
Oracle Number of Open Cursors	PMOracleAmountOfCursors.sql
Oracle Number of Open Processes	PMOracleAmountOfProcesses.sql

On-demand Monitor	SQL Script
Oracle Number of Open Sessions	PMOracleAmountOfSessions.sql
Oracle Tablespaces	PMOracleTablespaces.sql

Reactive Analysis User Interface

This section includes (in alphabetical order):

- Correlated Events for Suspect CI Page on page 28
- Correlation Graph on page 31
- Edit Monitor Profile Page on page 35
- Impact Page on page 37
- Initial Analysis Page on page 41
- Invoke Run Book Page on page 50
- Isolation History Page on page 54
- Layer Analysis Page on page 59
- List of Monitors on page 71
- List of On-demand Monitors on page 72
- Monitor Profile Configuration Page on page 73
- New Monitor Profile Page on page 74
- On-demand Monitor Details Dialog Box on page 76
- On-demand Monitor Parameters Dialog Box on page 77
- On-demand Monitors Results Pane on page 78
- Problem Isolation Entry Page for HP Service Manager on page 81
- Problem Isolation Properties Page on page 83
- Problem Snapshot Report on page 86
- Run Book Parameters Dialog Box on page 90
- Suspect CI Monitor Configuration Page on page 91

- ➤ Suspect CI Monitor Configuration Wizard on page 93
- ➤ Suspects Page on page 97
- ➤ Triage Steps - Standard User Interface Elements on page 102
- ➤ Validation Page on page 104

Correlated Events for Suspect CI Page

Description	Displays details of Enterprise Management System (EMS) events that are related to a suspect CI. **To access:** Click an event correlation value for a suspect CI in the **Suspects** page.
Important Information	➤ By default, correlation scores are calculated for EMS events with any status and of any severity level (from 0–5) that occurred from 30 minutes prior to the problem start time to 30 minutes after the problem start time. You can customize these settings. For details, see the customization details for the relevant field in the element table. ➤ Events are matched to a host's DNS name, which is obtained from the IP address using a predefined TQL. ➤ By default, events from all data sources excluding Netscout are included in event correlation. You can configure Problem Isolation to exclude events from specific data sources. To do this, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the **Event data sources to ignore** entry in the **Events Correlation** table. In the XML file that opens, add an additional line for each data source you want to ignore in the format: <EventDataSource>name of the data source to exclude</EventDataSource >.

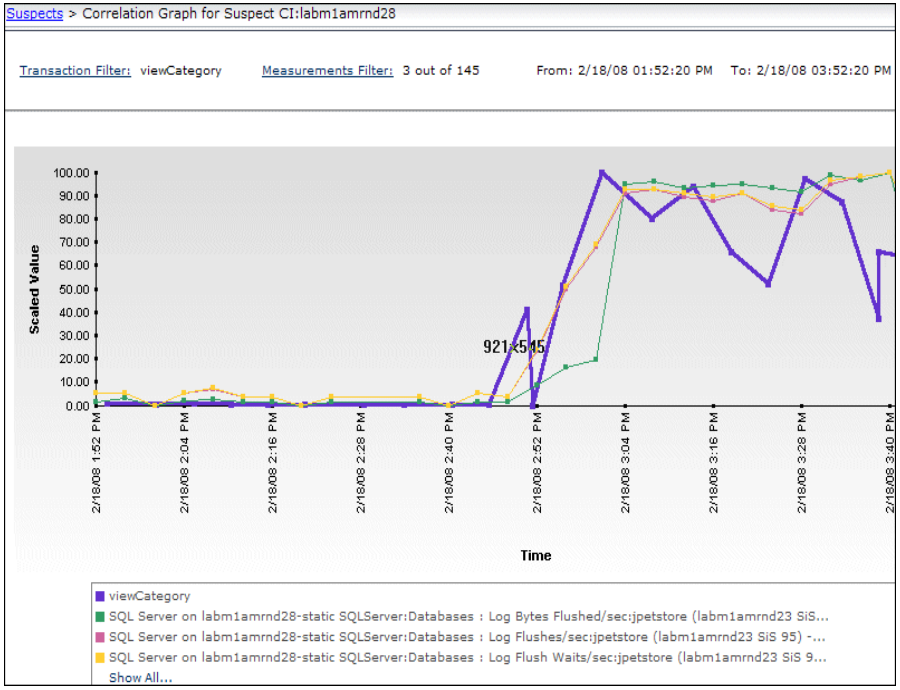
The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Description	The description of the event.
Distance	The distance, in minutes, from the problem start time at which the event occurred. **Customization:** By default, correlation scores are calculated for all events that occurred from 30 minutes before the problem start time to 30 minutes after the problem start time. To modify the time range for which event correlation scores are calculated, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the **Number of minutes before and after problem start time for correlated events** entry in the **Events Correlation** table. Modify the value to the number of minutes before and after the problem start time for which correlation scores are calculated for events. **Note:** Events not included in the configured time range are displayed with a correlation score of 0.
Event Source	The name of the source EMS from which the event was received.
Not Correlated	For events that are not included in the Event Correlation value on the Suspects page, the icon is displayed in this column. Such events are within the configured distance for events, but were received after the Event Correlation value was calculated.
Score	The event correlation percentage value as calculated by Problem Isolation.

GUI Element (A-Z)	Description
Severity	The severity of the event. **Customization:** By default, correlation scores are calculated for events with all levels of severity (from 0–5). To modify the severity level for which event correlation scores are calculated, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the **Minimum severity of the correlation events** entry in the **Events Correlation** table. Modify the value to the severity level for which correlation scores are calculated for events. **Note:** ➤ Events with a severity less than the configured level are displayed with a correlation score of 0. ➤ Problem Isolation only recognizes events with a severity level from 0–5. ➤ Events with a severity level of 0 (unknown) are displayed with a correlation score of 0.
Status	The event status. **Customization:** By default, correlation scores are calculated for events with any status. You can configure Problem Isolation not to calculate correlation scores for events that have been acknowledged or closed in the EMS before the problem start time. To do this, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the **Ignore acknowledged and closed events** entry in the **Events Correlation** table. Modify the value to **true**. **Note:** When you change this setting to true, acknowledged and closed events are displayed with a correlation score of 0.
Time	The date and time at which the event occurred.

Correlation Graph

The following is an example of the Correlation graph.



Description	Displays the correlation between a problematic CI's Business Process transactions or Real User Monitor pages and a selected suspect CI's measurements. Also shows changes made to the selected suspect CI. **To access:** Click the **Correlation Score** value for a suspect CI in the **Suspects** page.
Important Information	➤ The time range used for the Correlation graph is determined by Problem Isolation and differs according to the type of data being compared. The default time range is two hours for Real User Monitor pages and six hours for Business Process transactions. ➤ Raw data is displayed for transactions and aggregated data (aggregated every five minutes) is shown for pages.
Included in Tasks	"Isolate a Problem – Workflow" on page 19

Graph Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
<**Common report elements**>	For details on the user interface, see "Common Report Elements" in *Reports*.
Measurements Filter	Displays the number of the suspect CI's measurements that are included in the graph out of the total number of the suspect CI's measurements. Click to open the **Measurements Filter** dialog box that lists all the measurements for the selected suspect CI, sorted by correlation score. Select the check boxes of the measurements you want to include in the graph. **Default value:** The first ten measurements in the list are selected. **Customization:** To modify the default number of suspect CI measurements included in the Correlation graph, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the **Default number of measurements to include in graph** entry in the **Correlation Graph** table. Modify the value to the required number of measurements.
Transaction Filter	Displays the problematic CI's Business Process transaction or Real User Monitor page that is included in the graph. Click to open the **Transaction Filter** dialog box that lists all of the problematic CI's Business Process transactions and Real User Monitor pages, and select the radio button next to the transaction or page you want to include in the graph. **Default value:** All of the problematic CI's transactions and Real User Monitor pages are displayed in the Transaction Filter dialog box (sorted by correlation score), and the one with the highest correlation score is selected.

Graph Content

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
<Bars>	Show changes made to the selected suspect CI, over the time period for which the Correlation graph is displayed. **Tooltip:** The relevant time period from the first to the last change, the contained CI names and the number of changes for each one.
<Legend>	Describes the color coding used in the graph.
<Thick line connecting data points>	Shows the status of the selected Business Process transaction or Real User Monitor page for the problematic CI, over the time period for which the Correlation graph is displayed. For Business Process transactions, the displayed value is based on a combination of the transaction response time and availability, and for Real User Monitor pages, the displayed value is based on the maximum server time for the page. **Tooltip:** The transaction or page name, the monitor value, and the relevant time.
<Thin lines connecting data points>	Show the status of the selected measurements for the selected suspect CI, over the time period for which the Correlation graph is displayed. **Tooltip:** The measurement name, the measurement value, the monitored CI name, the correlation score, and the relevant time.
Scaled Value <y-axis>	The measurement and end-user monitor values, scaled as percentage units, with the highest value represented as 100% and the lowest value as 0%.
Time <x-axis>	The time division units for the time range specified when generating the report.

Edit Monitor Profile Page

Description	Enables you to edit existing monitor profiles for Problem Isolation on-demand monitors. The page comprises the Monitor Profile General Properties pane (for details, see page 35) and the SiteScope Template pane (for details, see page 36). **To access:** Click the **Edit** button for a specific monitor profile in the Monitor Profile Configuration page.
Important Information	You create a new monitor profile on the New Monitor Profile Page (for details, see page 74).

Monitor Profile General Properties Pane

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
Monitor Category	Select the category to which the monitor belongs. Valid options are: ➤ Connectivity ➤ Critical Services ➤ Health ➤ Other **Default value:** Other
Monitor Profile Name	The name you choose for the new monitor profile. **Note:** This is a compulsory field and the name must be unique.

GUI Element (A–Z)	Description
Note	A free text field for any notes you want to associate with the monitor.
Weight	The weight of the monitor to be used when calculating the success rate percentage of the monitor set. For details on how the success rate percentage is calculated, see "Calculating On-demand Monitor Success Ratios" on page 16. **Default Value:** 1 **Note:** The weight must be a positive integer between 0 and 100.

SiteScope Template Pane

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
Parameter Default Value	Enter a default value to be used for the monitor parameter.
Parameter Name	Displays the parameters available for the monitor in the selected SiteScope template.
SiteScope Template	Select the name of an existing SiteScope Problem Isolation template. **Note:** You cannot change the SiteScope template of an existing monitor profile if the profile is included in more than one monitor configuration.

Impact Page

Description	Displays a problem's impact on business and also shows the SLAs and number of users impacted by the problem. **To access:** Click the **Impact** option in the Problem Isolation flow bar on any Problem Isolation page.
Included in Tasks	"Isolate a Problem – Workflow" on page 19
Useful Links	"Triage Steps - Standard User Interface Elements" on page 102

This section includes the following topics:

- "Impact Pane" on page 37
- "SLAs Impact Pane" on page 38
- "User Volume Pane" on page 39

Impact Pane

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
Highlight	Displays the number of SLAs and the number of users impacted by the problem.
Info - SLAs Impact	Displays the number of SLAs impacted by the problematic CI, and the number of them that are about to be breached. Click the message to display the impacted SLAs in the right pane.

GUI Element (A–Z)	Description
Info - User Volume	Displays the number of users currently using Real User Monitor applications associated with the problematic CI, and the number of users that are forecasted to use these applications in the next hour. Also displays the deviation for the number of forecasted users. Click the message to display the **User Volume** report in the right pane, which shows the number of users currently on the system, how many of them are experiencing problems, and the number of forecasted users.
Recommendation	Compares the impact of the problem to that of other open problems and recommends what steps to take.

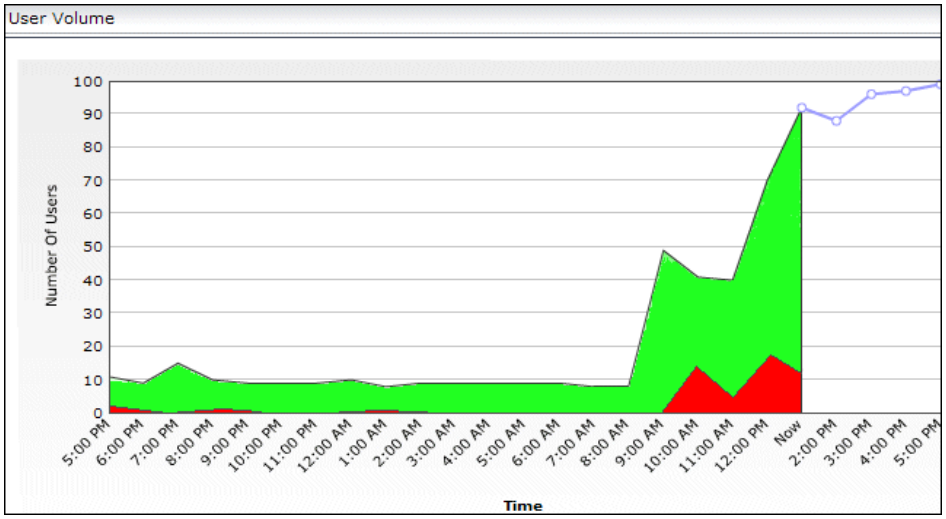
SLAs Impact Pane

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
<Legend>	Describes the different SLA statuses shown.
SLA Description	Displays the description, customer, and provider of the impacted SLA. **Tooltip:** Full SLA description.
SLA Name	Displays the name of the impacted SLA. **Tooltip:** Full SLA name.
SLA Status	The status shows a dial, indicating the worst status of the SLA for a specific period of time (day, week, month, or quarter). To the right of the dial, each time period is listed, and its worst status is displayed. **Tooltip:** Hold the cursor over the dial, or status icon, to display the status and the relevant time period.

User Volume Pane

The following is an example of the User Volume pane.



Important Information	The graph's time range is always 24 hours. By default, the current number of users for the previous 20 hours and the forecasted number of users for the next 4 hours are displayed. You can customize the number of hours for which to display the forecasted number of users, which automatically changes the number of hours for which to display the current number of users to make a total of 24 hours. To modify the number of hours for which to display the forecasted number of users, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the **User volume forecast hours** entry in the **User Volume** table. Modify the value to the number of hours for which to display the forecasted number of users.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
<Blue line connecting data points>	Displays the forecasted number of users at each point in the graph's time range. **Tooltip:** The number of forecasted users and the applicable date and time.
<Legend>	Describes the color coding used in the graph.
<Shaded green area>	Indicates the number of current users for each point in the graph's time range. **Tooltip:** The number of current users and the applicable date and time.
<Shaded red area>	Indicates the number of current users that are experiencing problems for each point in the graph's time range. **Tooltip:** The number of current users experiencing problems and the applicable date and time.
Number of Users (y-axis)	The total number of users.
Time (x-axis)	The time division units for the graph's time range.

Initial Analysis Page

Description	Performs an initial analysis of the problem, and provides useful information to help you determine possible causes of the problem. The initial analysis includes the following: ➤ Checks transactions and locations to determine if a specific transaction or location is experiencing the problem. ➤ Displays the distribution and behavior over time of errors and events that occurred on virtual monitors, and if your system is configured for snapshot on error, displays the relevant snapshots. ➤ Displays a summary of Real User Monitor events. ➤ Displays the problem's KPIs over time. The page comprises two panes. The right pane is the main display area which displays relevant data for the option selected in the Info section of the Initial Analysis pane on the left. The main display area includes one of the following panes: ➤ Error Summary Pane (for details, see page 43). ➤ Error Over Time Pane (for details, see page 46). ➤ Event Summary Pane (for details see page 48). ➤ Problem Scope Pane (for details, see page 48). ➤ Problem Over Time Pane (for details see page 49). **To access:** ➤ Click the **Initial Analysis** option in the Problem Isolation flow bar on any Problem Isolation page. ➤ The default page displayed when accessing Problem Isolation by clicking the **Triage** button for an existing isolation record.
Included in Tasks	"Isolate a Problem – Workflow" on page 19
Useful Links	"Triage Steps - Standard User Interface Elements" on page 102

Initial Analysis Pane

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
Highlight	Displays the general scope of the problem, including whether the problem is a real problem, if it is occurring in more than one location, and if there are persistent errors over time.
Info - Error Summary	If the problematic CI is monitored by Business Process Monitors, and at least one Business Process Monitor has errors or performance events in the configured time period, a message is displayed indicating the number and type of errors detected. Click the message to display the Error Summary Pane in the main display area (for details, see page 43).
Info - Event Summary	If the problematic CI is monitored by Real User Monitor, a message is displayed with a link to the Real User Monitor Event Summary report. Click the message to display the Event Summary Pane in the main display area (for details, see page 48).
Info - Problem Over Time	If the problematic CI is monitored by end-user monitors, and KPI data over time exists for the problematic CI, a message indicating the number of related KPIs that have a problematic status is displayed. Click the message to display the Problem Over Time Pane in the main display area (for details, see page 49).
Info - Problem Scope	If the problematic CI is monitored by Business Process Monitors and errors are detected, two messages are displayed indicating the number of transactions experiencing problems, and the number of locations experiencing problems. Click either message to display the Problem Scope Pane in the main display area (for details, see page 48).

GUI Element (A–Z)	Description
Info- Error Over Time	Click the message to display the Error Over Time Pane in the main display area, where you can view a graph of the errors and events that occurred on Business Process Monitors over a period of time (for details, see page 46).
Recommendation	Displays the recommended steps to take, to help solve the problem.

Error Summary Pane

Description	The Error Summary pane displays one of the following: ➤ Error Summary Report (for details, see page 44). The default view when the pane is first accessed. ➤ Error List (for details, see page 45). Accessed from the Virtual User (Business Process Monitor) Error Summary report.
Important Information	The default time period for the Error Summary report is from the problem start time to 24 hours after the problem start time. To modify the default time period used by the Error Summary report, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the **Error Summary Report Time Frame Hours Length (forward)** entry in the **Initial Analysis** table. Modify the value to the required number of hours after the problem start time.

Error Summary Report

Report Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
<Common report elements>	For details on the user interface, see "Common Report Elements" in *Reports*.

Report Content

Description	The Error Summary report displays three pie charts, one each for: ➤ HTTP errors ➤ application errors ➤ general errors Each slice of a chart represents a specific error or event within the pie chart's category, and displays the number of occurrences of that error or event in the selected time frame. A legend at the bottom of each chart describes the color coding of the slices. **Tooltip:** Hold the cursor over a slice to display the error or event name and the number of occurrences of that error or event.
Important Information	Click a slice to open the Error list for that error or event. For details, see "Error List" on page 45.

Error List

Report Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
<Common report elements>	For details on the user interface, see "Common Report Elements" in *Reports*.

Report Content

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
	Click to display a snapshot of the page on which the error occurred. For details on this topic, see "Snapshot on Error"in *Using End User Management*. **Note:** This button is only enabled if a snapshot of the page exists.
	Click to open a zip file of a page's snapshot. For details on this topic, see "Snapshot on Error"in *Using End User Management*. **Note:** This button is only enabled if a zip file of the page's snapshot exists.
Time	Displays the time that the error occurred.

Error Over Time Pane

Description	The Error Over Time pane displays one of the following: ➤ Error Summary Report (for details, see page 44). The default view when the pane is first accessed. ➤ Error List (for details, see page 45). Accessed from the Virtual User (Business Process Monitor) Event Over Time report.
Important Information	The default time period for the Event Over Time report is from 12 hours before the problem start time to 12 hours after the problem start time. To modify the default time period used by the Event Over Time report, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the **Event summary report Time Frame Hours Length (+/-)** entry in the **Initial Analysis** table. Modify the value to the required number of hours to be used before and after the problem start time.

Report Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
<Common report elements>	For details on the user interface, see "Common Report Elements" in *Reports*.

Report Content

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
<Lines connecting data points>	Each line represents a different category of error (HTTP errors, application errors, and general errors) and shows the number of errors in that category that occurred at a specific time. Click a data line to change the display to show the same graph, but for all the different error types included in that category. Click a specific error type to display the Error list for that specific error. For details on the Error list, see "Error List" on page 45. **Tooltip:** Hold the cursor over a data point to display the number of errors for a category or type for a specific time.
Legend	Describes the color coding used in the report.
Number of Errors <y-axis>	The total number of errors experienced by virtual users.
Time <x-axis>	The time division units for the time range specified when generating the report.

Event Summary Pane

Description	The Event Summary Report pane displays the Real User Monitor Event Summary report for the problematic CI. For details on the Real User Monitor Event Summary report, see "Event Summary Report" in *Using End User Management*.
Important Information	The default time period for the Real User Monitor Event Summary report is from one hour before the problem start time to one hour after the problem start time. To modify the time period, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the **Rum Event summary report Time Frame Hours Length (+/-)** entry in the **Initial Analysis** table. Modify the value to the number of hours to be used before and after the problem start time.

Problem Scope Pane

Description	The Problem Scope pane displays the Transaction by Location section of the Business Process Monitor Triage report. For details on the Triage report, see "Triage Raw Data Report" in *Using End User Management*.
Important Information	➤ The report displayed in the Problem Scope pane differs from the standard Triage Raw Data report as it only includes transactions that are relevant to the problematic CI. ➤ The default time period for the Business Process Monitor Triage report is from the problem start time to one hour after the problem start time. To modify the default time period used by the Business Process Monitor Triage report, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the **Problem Scope Time Frame Hours Length (forward)** entry in the **Initial Analysis** table. Modify the value to the required number of hours after the problem start time.

Problem Over Time Pane

Description	The Problem Over Time Report pane displays the KPI Over Time report for the problematic CI, for the selected time period. For details on the KPI Over Time report, see "KPIs Over Time Report" in *Using Dashboard*.
Important Information	The default time period for the KPI Over Time report is from 24 hours prior to the problem start time to 24 hours after the problem start time. To modify the default time period used by the KPI Over Time report, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the **Problem Over Time - Time Frame Hours Length (+/-)** entry in the **Initial Analysis** table. Modify the value to the required number of hours to be used before and after the problem start time.

Invoke Run Book Page

Description	Enables you to view and run the HP Operations Orchestration (OO) run books linked to a selected suspect CI's type and any CI types of which it is a descendant. Also enables you to view details of previous runs of the run books. **To access:** ➤ In the **Suspects** page, click the value in the **Run Books Invocations** column for a selected suspect CI. ➤ In the **Suspects** page, click the icon.
Important Information	➤ This page is available only if Business Availability Center and OO are integrated. For details on this topic, see "HP Operations Orchestration Integration Overview" in *Solutions and Integrations*. ➤ When you first access the page and no filters are set for the tables, all relevant data is listed. After entering a string in a column's filter, press ENTER or click another element on the page to generate the list of matching records. If a column's filter is empty, all records are matched for that column and are included in the generated list. You can use the asterisk (*) wildcard to represent any string in a column's filter.

Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
	Click to reset the table columns' width to their default setting. You can adjust the width of the table's columns by dragging the borders of the column to the right or the left.
	Click the **Select Columns** button to open the Select Columns dialog box and select the columns you want to be displayed on the table. For details on the Select Columns dialog box, see "Working with Tables" in *Reference Information*.

Related Run Books Area

Description	Enables you to view the HP Operations Orchestration (OO) run books linked to a selected suspect CI's type, and to run them.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
	Click the **Invoke Run Book** button to run a selected run book on a suspect CI's type. Operations Orchestration opens in a new window and displays a flow graph of the run book and the **Run Flow** page. For details on working with Operations Orchestration, see the Operations Orchestration documentation.
	Click the **Edit Run Book Parameters** button to open the **Run Book Parameters** dialog box, where you can view and edit the parameters used by the selected run book. For details on the user interface, see "Run Book Parameters Dialog Box" on page 90.

GUI Element (A-Z)	Description
CI Type	Displays the CI type to which the run book is mapped. This is the CI type of the suspect CI. **Note:** This column is hidden by default.
Description	Displays the description of the run book.
Path	Displays the path of the run book in the OO flow library. **Note:** This column is hidden by default.
Run Book Name	Displays the name of the OO run books that are mapped to the suspect CI's type. Each run book is displayed as a separate entry in the table. Click a run book name to display a flow graph of the run book in a new window. **Tooltip:** The full path of the run book in the OO flow library and the CI type mapped to the run book.

Run Books Invocations Area

Description	Enables you to view details of previous runs of the run books.
Important Information	By default, the entries in the table are sorted by date. If there are empty date fields (for example, if a run book was invoked but did not actually start) the entries are sorted by ID, which is a hidden column by default.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
Date	Displays the date that the OO run book was run for the suspect CI type. **Note:** This field is empty until the run book actually starts running.
ID	Displays the internal OO run book instance Id number. **Note:** This column is hidden by default.

GUI Element (A-Z)	Description
Run Book Name	Displays the name of the OO run book that was run for the suspect CI type. **Tooltip:** The full path of the run book in the OO flow library.
Status	Displays the status of the specific instance of the OO run book that was run on the suspect CI type. Click the status icon to open the OO Flow Run report in a new window. For details on the OO Flow Run report, see the Operations Orchestration documentation. The valid statuses are: ➤ **Failed to run.** The run book instance did not successfully complete its run. ➤ **Cancelled.** The run book instance was cancelled in OO. The instance cannot be rerun. ➤ **Running.** The run book instance is currently running. ➤ **Paused.** The run book instance is waiting for manual input or has been paused. ➤ **Unknown.** The status is unknown due to no connection with the OO server, or an unknown status is received from OO. ➤ **Resolved.** The run book instance completed successfully. ➤ **No action taken.** The run book instance completed successfully, but no action was taken during the run. ➤ **Error.** The run book instance encountered one or more errors and did not complete successfully. **Tip:** In the OO Flow Run report, display **Recorded Bound Inputs** to see the variable names and values used in the run book instance.
User	Displays the name of the user who ran the OO run book on the suspect CI type.

Isolation History Page

Description	Displays a list of isolation records for problematic CIs, as well as the problematic CI properties for a selected record. Enables you to triage a problematic CI from the list, update a problematic CI's isolation properties, attach an isolation record to an existing HP Service Manager incident or problem, and open a new HP Service Manager incident or problem. Click a row in the table to select an isolation record. **To access:** Select **Applications** > **Problem Isolation** > **Reactive Analysis** tab
Important Information	An isolation record is added to isolation history when you access Problem Isolation from Dashboard or HP Service Manager for a problematic CI with a unique problem start time.

Isolation History Pane

Important Information	➤ After entering a string in a column's filter, press ENTER or click another element on the page to generate the list of matching records. ➤ If a column's filter is empty, all records are matched for that column and are included in the generated list. ➤ You can use the asterisk (*) wildcard to represent any string in a column's filter.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
<Common report elements>	For details on the user interface, see "Common Report Elements" in *Reports*.
CI Name	Lists the names of problematic CIs that start with the string in the CI Name filter. **Note:** ➤ For details on working with the column filters, see "Important Information" on page 54. ➤ This column is displayed by default.
CI Type	Lists the CI types of problematic CIs that start with the string in the CI Type filter. **Note:** ➤ For details on working with the column filters, see "Important Information" on page 54. ➤ This column is displayed by default.
Isolated By	Lists the login names of the users that created the isolation record for problematic CIs that start with the string in the Isolated By filter. **Note:** ➤ For details on working with the column filters, see "Important Information" on page 54. ➤ This column is not displayed by default.
Isolation Date	Lists the creation dates of the isolation record of problematic CIs that start with the string in the Isolation Date filter. **Note:** ➤ For details on working with the column filters, see "Important Information" on page 54. ➤ This column is displayed by default.

GUI Element (A–Z)	Description
Isolation ID	Lists the internal problem isolation ID numbers of problematic CIs that start with the string in the Isolation ID filter. **Note:** ➤ For details on working with the column filters, see "Important Information" on page 54. ➤ This column is not displayed by default.
Problem Start Time	Lists the problem start date and time for problematic CIs that start with the string in the Problem Start Time filter. **Note:** ➤ For details on working with the column filters, see "Important Information" on page 54. ➤ This column is not displayed by default.
Root Cause CI Name	Lists the names of the CIs considered the root cause of problematic CIs that start with the string in the Root Cause CI Name filter. **Note:** ➤ For details on working with the column filters, see "Important Information" on page 54. ➤ This column is displayed by default.
Root Cause CI Type	Lists the CI type of the CIs considered the root cause of problematic CIs that start with the string in the Root Cause CI Type filter. **Note:** ➤ For details on working with the column filters, see "Important Information" on page 54. ➤ This column is not displayed by default.

GUI Element (A–Z)	Description
Root Cause Description	Lists the root cause description of problematic CIs, that start with the string in the Root Cause Description filter. **Note:** ➤ For details on working with the column filters, see "Important Information" on page 54. ➤ This column is not displayed by default.
Root Cause Layer	Lists the network or infrastructure layers of the CI you consider to be the root cause of problematic CIs, that start with the string in the Root Cause Layer filter. **Note:** ➤ For details on working with the column filters, see "Important Information" on page 54. ➤ This column is not displayed by default.
Ticket ID	Lists the HP Service Manager ticket Ids associated with problematic CIs that start with the string in the Ticket ID filter. Click an incident or problem ticket Id link to open the HP Service Manager login page in a new browser window. Enter a valid HP Service Manager user name and password. The HP Service Manager Update Incident or Problem Management page opens, where you can view and update the incident or problem. For details on working in HP Service Manager, see the HP Service Manager documentation. **Note:** ➤ For details on working with the column filters, see "Important Information" on page 54. ➤ This column is displayed by default, if HP Service Manager is integrated with HP Business Availability Center. For details on integrating HP Service Manager with HP Business Availability Center, see "HP Service Manager Integration with Business Availability Center Components" in *Solutions and Integrations*.

GUI Element (A–Z)	Description
Ticket Type	Lists the record types in HP Service Manager (incident or problem) with which isolation records are associated, that start with the string in the Ticket Type filter. **Note:** ➤ For details on working with the column filters, see "Important Information" on page 54. ➤ This column is not displayed by default.
Triage	Click the **Triage** button to go to the triage steps in Problem Isolation for a selected CI. **Note:** By default, the Problem Isolation Validation page opens. For details on the user interface, see "Validation Page" on page 104.

Properties Pane

Description	For details on the Properties pane, see "Problem Isolation Properties Page" on page 83.

Layer Analysis Page

Description	Determines if the problem is in the network or infrastructure layer, and performs a layer analysis of the transactions affected by the problem, to isolate the problematic layer causing the problem you are investigating. The page comprises two panes. The right pane is the main display area which displays relevant data for the option selected in the Info section of the Layer Analysis pane on the left. The main display area includes one of the following panes: ➤ Layer Deviation Analysis Pane (for details, see page 61) ➤ System Status Pane (for details, see page 63) ➤ Transactions Layer Breakdown Pane (for details, see page 70) **To access:** Click the **Layer Analysis** option in the Problem Isolation flow bar on any Problem Isolation page.
Included in Tasks	"Isolate a Problem – Workflow" on page 19
Useful Links	"Triage Steps - Standard User Interface Elements" on page 102

Layer Analysis Pane

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
Highlight	Displays the layer with the worst result in the Layer Analysis report, in which the problem most likely resides.
Info - Layer Deviation Analysis	A message is displayed showing the worst transaction layer together with its average standard deviation time (in milliseconds) in comparison to the base line. Click the message to display the Layer Deviation Analysis Pane in the main display area (for details, see page 61).
Info - System Status	A message is displayed showing the number of errors encountered in each on-demand monitor category, out of the total number of monitors in that category. Click the message to display the System Status Pane in the main display area (for details, see page 63).
Info - Transactions Layer Breakdown	A message is displayed showing the impact of the worst transaction layer, that is, the ratio of the layer's response time to the total transaction response time. Click the message to display the Transactions Layer Breakdown Pane in the main display area (for details, see page 70).
Recommendation	Displays the recommended steps to take, to help solve the problem.

Layer Deviation Analysis Pane

Description	Shows the difference in time between the average standard deviation in response times for the selected current time range and the average layer response time for the selected base line time range.
Important Information	The report includes data only for transactions that are affected by the problematic CI.

Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
<Common report elements>	For details on the user interface, see "Common Report Elements" in *Reports*.
Active Filters	Click to open a dialog box in which you can view and select the transactions and locations to include in the report. Only transactions and locations that might affect the problematic CI are displayed.

GUI Element (A–Z)	Description
Compare To	Select the time period for which to calculate the base line average layer response times. Use the default value, or in the **View** field select a predefined time period. **Default value:** A period of 6 hours, starting from 27 hours prior to the time that the problem was opened, to 21 hours prior to the time that the problem was opened. **Customization:** To modify the default time period on which to calculate the base line average layer response times, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the following entries in the **Layers Analysis** table: ➤ **Base Line Time Frame Hours Back.** Modify the number of hours prior to the time that the problem was opened to use as the starting time for the base line time period. ➤ **Base Line Time Frame Hours Long.** Modify the ending time of the base line time period by specifying its duration, in hours.
Current	Select the time period for which to calculate the current average layer response times. Use the default value, or in the **View** field select a predefined time period or select **Custom** and specify a time period using the **From** and **To** fields. **Default value:** A period of 12 hours, starting from half and hour prior to the time that the problem was opened, to 11.5 hours after the time that the problem was opened.

Content

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
<Dials>	Each dial represents a different transaction layer. The median of the base line response time for that layer is indicated by the center of the green shaded area of the dial. The dial arrow indicates the median of the base line response time plus the average standard deviation in response times for the selected current time range. The actual measurements are also displayed above the dial. The color shading in the dial allows you to easily see the difference between the two measurements and to obtain a quick picture of the layer status. The further away from the base line average response time that the dial arrow is, the more problematic is the layer, especially when the arrow is in the red shaded area of the dial.

System Status Pane

Description	The System Status pane displays the System Status report, which shows data collected from on-demand monitors, deployed monitors, and changes, sliced by tiers (such as network, infrastructure, Web server, Application server, and Database server). For each tier, the data is broken down into categories relevant to the tier. From the System Status report, you can drill down to see a detailed list of the monitors for each category in the selected tier.

The System Status pane displays the following reports:

➤ "System Status Report" on page 64

➤ "Category Status for a Tier Report" on page 66

System Status Report

Report Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
<Common report elements>	For details on the user interface, see "Common Report Elements" in *Reports*.

Report Content

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
# of Fails <y-axis>	Displays the number of failures detected by the monitors for each category in the tier.
<Legend>	Describes the color coding used for the different categories in the tiers.

GUI Element (A–Z)	Description
Tiers **<x-axis>**	Each bar represents a different tier, which is named and denoted graphically underneath the bar. The height of the bar indicates how problematic the tier is, with the highest bar being the most problematic tier. Each bar comprises a section for each monitor category as well as sections for deployed monitors and changes. Each section is denoted by a different color, described in the legend. The following list shows the sections that comprise a bar and how their proportion of the tier is calculated: ➤ **Connectivity.** The weighted sum of failed connectivity on-demand monitors, divided by the weighted sum of all connectivity on-demand monitors for the tier. ➤ **Critical Services.** The weighted sum of failed critical services on-demand monitors, divided by the weighted sum of all critical services on-demand monitors for the tier. ➤ **Health.** The weighted sum of failed health on-demand monitors, divided by the weighted sum of all health on-demand monitors for the tier. ➤ **Miscellaneous.** The weighted sum of other failed on-demand monitors, divided by the weighted sum of all other on-demand monitors for the tier. ➤ **Deployed monitors.** The failed monitors for the tier, divided by the total monitors for the tier. ➤ **Changes.** The changes for the tier, divided by the total changes for all tiers. Click a bar to display the Category Status for a Tier Report (for details, see page 66), showing the status of the suspect CIs included in each of the categories that comprise the tier.

Category Status for a Tier Report

Important Information	The cells that display the weighted percentage of the failed on-demand monitors for the CI, in the categories of a tier, are color coded according to their weighted percentage, as described in the legend. To modify the percentage range for the color coding, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the following entries in the **Layers Analysis:System Status** table: ➤ **System status warning threshold.** Modify the weighted percent that starts the warning (yellow) range. ➤ **System status error threshold.** Modify the weighted percent that starts the error (red) range.

Report Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
<Common report elements>	For details on the user interface, see "Common Report Elements" in *Reports*.

Report Content

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
<Legend>	Describes the color coding of the statuses included in the report.
Changes	Displays the number of discovered changes made to the suspect CI. Click the value displayed to see the Changes report for the CI. For details on the Changes report, see "Change Report" in *Model Management*.
CI Name	Displays the name of the suspect CI. **Tooltip:** The full CI name, the weighted percentage of failed monitors for the CI, and the number of failed monitors out of the total number of monitors run for the CI in each category in the tier.
CI Type	Displays the CI type icon of the suspect CI.
Connectivity	Displays the weighted percentage of the failed on-demand monitors for the CI, in the Connectivity category of the tier. Each cell is color coded according to its weighted percentage, as described in the legend. Click the **Connectivity** category to see the List of On-demand Monitors for the category. **Default value:** The default color coding is: ➤ **Green.** 0% ➤ **Yellow.** 1% - 30% ➤ **Red.** 31% - 100% **Tooltip:** The weighted percentage of failed monitors, the number of failed monitors, and the total number of monitors run for the CI.

GUI Element (A–Z)	Description
Critical Services	Displays the weighted percentage of the failed on-demand monitors for the CI, in the Critical Services category of the tier. Each cell is color coded according to its weighted percentage, as described in the legend. Click the **Critical Services** category to see the List of On-demand Monitors for the category. **Default value:** The default color coding is: ➤ **Green.** 0% ➤ **Yellow.** 1% - 30% ➤ **Red.** 31% - 100% **Tooltip:** The weighted percentage of failed monitors, the number of failed monitors, and the total number of monitors run for the CI.
Deployed Monitors	Displays the number of failed monitors out of the total number of monitors deployed on the suspect CI in the selected tier. Click the number of monitors to see the List of Monitors.

GUI Element (A–Z)	Description
Health	Displays the weighted percentage of the failed on-demand monitors for the CI, in the Health category of the tier. Each cell is color coded according to its weighted percentage, as described in the legend. Click the **Health** category to see the List of On-demand Monitors for the category. **Default value:** The default color coding is: ➤ **Green.** 0% ➤ **Yellow.** 1% - 30% ➤ **Red.** 31% - 100% **Tooltip:** The weighted percentage of failed monitors, the number of failed monitors, and the total number of monitors run for the CI.
Miscellaneous	Displays the weighted percentage of the failed on-demand monitors for the CI, in the Miscellaneous category of the tier. Each cell is color coded according to its weighted percentage, as described in the legend. Click the **Miscellaneous** category to see the List of On-demand Monitors for the category. **Default value:** The default color coding is: ➤ **Green.** 0% ➤ **Yellow.** 1% - 30% ➤ **Red.** 31% - 100% **Tooltip:** The weighted percentage of failed monitors, the number of failed monitors, and the total number of monitors run for the CI.

Transactions Layer Breakdown Pane

Description	Displays the average response times for transaction categories. For more information on the Transaction Breakdown report, see "Triage Raw Data Report" in *Using End User Management*.
Important Information	The report only includes data for transactions that are affected by the problematic CI.

Report Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
<Common report elements>	For details on the user interface, see "Common Report Elements" in *Reports*.
Active Filters	Click the Active Filters link to select transactions and locations by which to filter the report. For details on using Active Filters, see "Active Filters Dialog Box" in *Using End User Management*.
Profile	Click the Profile link to select a profile for which to generate the report. For details on choosing a profile, see "Profiles Dialog Box" in *Using End User Management*.

Report Content

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
<Bars>	Each bar represents the average response time for all included transactions for the relevant time period, broken down into individual layer categories.
<Legend>	Describes the color coding used for the different layer categories.

GUI Element (A–Z)	Description
Response Time	The response time (in milliseconds) for each layer category included in the bar.
Time	The applicable date and time for the layer category data included in the bar.

List of Monitors

Description	Displays the monitors for the suspect CI and its descendants. **To access:** Click the value displayed for problem monitors in the Current Status column on the Suspects page.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
CI Name	The name of the suspect CI.
CI Type	The type of the suspect CI.
Monitor Name	The name of the monitor that was run on the suspect CI.
Monitor Status	The Dashboard status of the monitor that was run on the suspect CI. **Tooltip:** Status details.
Monitor Type	The type of the monitor that was run on the suspect CI.

List of On-demand Monitors

Description	Displays the on-demand monitors that were run on the suspect CI. **To access:** Click a category in the Category Status for a Tier report, which is part of the System Status report.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
Category	The monitor category as configured in the monitor profile. For details on configuring monitor profiles, see "New Monitor Profile Page" on page 74.
Details	A link to a popup window displaying additional information returned from the monitor environment.
Elapsed Time	The amount of time since the monitor started execution.
Monitor Name	The name of the monitor that was run on the suspect CI.
Status	A color denoting the result of the monitor test. Valid results are: ➤ **Green.** Test succeeded. ➤ **Red.** Test failed. ➤ **Grey.** Monitor could not be run.
Topology Pattern	The topology to which the CI belongs.
Weight	The importance weight of each monitor as configured in the monitor profile. For details on configuring monitor profiles, see "New Monitor Profile Page" on page 74.

Monitor Profile Configuration Page

Description	Displays existing monitor profiles for Problem Isolation on-demand monitors. Enables you to edit existing monitor profiles and configure new ones. **To access:** Select **Admin** > **Problem Isolation** > **Monitor Profiles** tab

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
	Click to access the Edit Monitor Profile Page, where you edit an existing monitor profile configuration.
Category	Displays the category to which the monitor belongs. Valid options are: ➤ Connectivity ➤ Critical Services ➤ Health ➤ Other
Monitor Profile Name	Displays the name of the new monitor profile.
New Monitor Profile	Click the **New Monitor Profile** button to open the New Monitor Profile page. For details on the user interface, see “New Monitor Profile Page” on page 74.
Note	Displays any notes you entered to be associated with the monitor.
SiteScope Template	Displays the name of the SiteScope Problem Isolation template used by the on-demand monitor.
Weight	Displays the weight of the monitor to be used when calculating the success rate percentage of the monitor set.

New Monitor Profile Page

Description	The page for creating new monitor profiles for Problem Isolation on-demand monitors. The page comprises the Monitor Profile General Properties pane (for details, see page 74) and the SiteScope Template pane (for details, see page 75). **To access:** Click the **New Monitor Profile** button in the Monitor Profile Configuration page.
Important Information	You edit an existing monitor profile on the Edit Monitor Profile Page (for details, see page 35).

Monitor Profile General Properties Pane

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
Monitor Profile Name	The name you choose for the new monitor profile. **Note:** This is a compulsory field and the name must be unique.
Monitor Category	Select the category to which the monitor belongs. Valid options are: ➤ Connectivity ➤ Critical Services ➤ Health ➤ Other **Default value:** Other

GUI Element (A–Z)	Description
Note	A free text field for any notes you want to associate with the monitor.
Weight	The weight of the monitor to be used when calculating the success rate percentage of the monitor set. For details on how the success rate percentage is calculated, see "Calculating On-demand Monitor Success Ratios" on page 16. **Default Value:** 1 **Note:** The weight must be a positive integer between 0 and 100.

SiteScope Template Pane

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
Parameter Default Value	Enter a default value to be used for the monitor parameter.
Parameter Name	Displays the parameters available for the monitor in the selected SiteScope template.
SiteScope Template	Select the name of an existing SiteScope Problem Isolation template.

On-demand Monitor Details Dialog Box

Description	Dialog box to view the details of an on-demand monitor run. **To access:** Click the status of a monitor from the list in the **On-demand Monitors Results** pane.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
<Parameter name>	Each monitor parameter used in the run is displayed with its value.
CI	The suspect CI on which the monitor is configured to run.
End time	The end time of the monitor run.
Monitor	The name of the monitor.
Monitor category	The monitor category as configured in the monitor profile.
Open in new window	Click the **Open in new window** button to open another window that displays the raw data formatted for output (for example, as HTML).
Raw data	The raw data included in the monitor run is displayed, if available.
Result description	The result of the monitor run.
Start time	The start time of the monitor run.

On-demand Monitor Parameters Dialog Box

Description	Dialog box to change the parameters of on-demand monitors, before running them. **To access:** Click a monitor from the list in the **On-demand Monitors Results** pane.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
	Click to restore the default value of a parameter.
CI	The suspect CI on which the monitor is configured to run.
Monitor	The name of the monitor.
Monitor category	The monitor category as configured in the monitor profile.
Monitor Parameters	For each monitor parameter listed, its current value is displayed. **Default Value:** The default value configured in the suspect CI monitor configuration, or a changed value, provided the problem has remained as the current problem since the value was changed.
Restore Parameters	Click the **Restore Parameters** button to restore the default value of all parameters.

On-demand Monitors Results Pane

Description	Lists the on-demand monitors that are run on suspect CIs and shows their status. Also enables you to run the monitors. **To access:** ➤ Click the **On-demand Monitors** button on any Problem Isolation page. ➤ Click a success ratio percentage in the **On-demand Monitor Results** column in the **Suspects** page.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
	Click to refresh the displayed list of monitors.
Abort	Click the **Abort** button to cancel all pending, selected monitors. Monitors that are currently running are not cancelled.
Details	Displays the details of the monitor run, excluding raw data.
Expand	Click the **Expand** button to open the On-demand Monitors Results pane in the main display pane of the page.

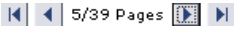
GUI Element (A–Z)	Description
Group by	Select the filter by which to group the displayed monitors. Valid options are: ➤ Monitor type ➤ Suspect CI ➤ Topology pattern **Default value:** ➤ Suspect CI – when you access the pane by clicking the **On-demand Monitors** button on a Problem Isolation page. ➤ Monitor type – when you access the pane by clicking a success ratio percentage in the **On-demand Monitor Results** column in the **Suspects** page. **Note:** The **Suspect CI** option is available only when you access the pane by clicking the **On-demand Monitors** button on a Problem Isolation page.
Monitor Type	Displays the on-demand monitors valid for the suspect CI. Each monitor is listed underneath the monitor type in a tree. Click a monitor to open the On-demand Monitor Parameters Dialog Box, where you can change the values of on-demand monitor parameters. For details on the On-demand Monitor Parameters dialog box, see "On-demand Monitor Parameters Dialog Box" on page 77. **Tooltip:** The CI type of the suspect CI on which the monitor runs, the topology pattern used by the monitor, and the monitor weight. **Note:** This column is visible only when the **Group by** field is set to **Suspect CI** or **Topology pattern**. Each monitor is listed under the suspect CI on which it runs, or the topology pattern that the monitor uses.
Run Monitors	Click the **Run Monitors** button to run the selected on-demand monitors.

GUI Element (A–Z)	Description
Status	Displays the status of the monitor. The valid statuses are: ➤ **Pending.** Selected and waiting to run ➤ **Running.** Currently running ➤ **Failed to run.** The monitor did not successfully complete its run. ➤ **Idle.** ➤ **OK.** The monitor ran successfully. ➤ **Bad.** The monitor ran, but was not successful. Click the status to open the On-demand Monitor Details Dialog Box for the monitor, where you can view detailed data about the monitor run. For details on the Monitor Details dialog box, see "On-demand Monitor Details Dialog Box" on page 76. **Tooltip:** The monitor run results.
Suspect CI	Displays the suspect CI and each monitor that runs on it. Click a monitor to open the On-demand Monitor Parameters Dialog Box, where you can change the values of on-demand monitor parameters. For details on the On-demand Monitor Parameters dialog box, see "On-demand Monitor Parameters Dialog Box" on page 77. **Tooltip:** The suspect CI type, the topology pattern used by the monitor that runs on it, and the monitor weight. **Note:** This column is visible only when the **Group by** field is set to **Monitor type**. Each suspect CI is listed under the monitor that runs on it.

Problem Isolation Entry Page for HP Service Manager

Description	Enables you to select and triage a CI from the HP Business Availability Center Universal CMDB when accessing Problem Isolation directly from HP Service Manager. When you select and triage a CI, a new isolation record is created. **To access:** See the HP Service Manager documentation.
Important Information	➤ When you first access the entry page and no filters are set, the most relevant business related CIs are listed. ➤ After entering a string in a column's filter, press ENTER or click another element on the page to generate the list of matching records. ➤ If a column's filter is empty, all records are matched for that column and are included in the generated list. ➤ You can use the asterisk (*) wildcard to represent any string in a column's filter.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
	Click to reset the table columns' width to their default setting. You can adjust the width of the table's columns by dragging the borders of the column to the right or the left.
	Click the **Select Columns** button to open the Select Columns dialog box and select the columns you want to be displayed on the table.
	Divides the table of data into pages. You move from page to page by clicking the relevant button: ➤ To view more pages, click the **Next page** or **Last page** buttons. ➤ To view previous pages, click the **Previous page** or **First page** buttons.

GUI Element (A–Z)	Description
CI Id	Lists the CI Ids that start with the string in the CI Id filter. **Note:** ➤ For details on working with the column filters, see "Important Information" on page 81. ➤ This column is not displayed by default.
CI Name	Lists the CI names that start with the string in the CI Name filter. **Note:** ➤ For details on working with the column filters, see "Important Information" on page 81. ➤ This column is displayed by default.
CI Type	Lists the CI types that start with the string in the CI Type filter. **Note:** ➤ For details on working with the column filters, see "Important Information" on page 81. ➤ This column is displayed by default.
Triage	Click the **Triage** button to go to the triage steps in Problem Isolation for a selected CI. **Note:** ➤ Click a row in the table to select a CI. ➤ By default, the Problem Isolation Impact page opens. For details on the user interface, see "Impact Page" on page 37.

Problem Isolation Properties Page

Description	Displays detailed information about the problematic CI currently selected in the Isolation History pane and enables you to update the information. **To access:** ➤ Automatically displayed when you access the Isolation History page. ➤ Click the **Properties** button from any triage step.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
	Refresh button. Click to refresh the incident or problem details displayed for the problematic CI.
<**Incident details**>	For isolation records that are associated with an HP Service Manager incident, lists the HP Service Manager ticket Id, title, status, severity and assigned operator. For details on HP Service Manager incidents, see the HP Service Manager documentation. **Note:** ➤ This section of the pane is displayed only if HP Service Manager is integrated with HP Business Availability Center. ➤ You can set **Incident details** as the default display mode for unassociated isolation records. For details on configuring HP Service Manager and HP Business Availability Center integration, see "HP Service Manager Integration with Business Availability Center Components" in *Solutions and Integrations*.

GUI Element (A–Z)	Description
<Problem details>	For isolation records that are associated with an HP Service Manager problem, lists the HP Service Manager problem Id, title, status, and severity. For details on HP Service Manager problems, see the HP Service Manager documentation. **Note:** ➤ This section of the pane is displayed only if HP Service Manager is integrated with HP Business Availability Center. ➤ You can set **Problem details** as the default display mode for unassociated isolation records. For details on configuring HP Service Manager and HP Business Availability Center integration, see "HP Service Manager Integration with Business Availability Center Components" in *Solutions and Integrations*.
Associate	Click the arrow to the right of the **Associate** button and select **Associate incident** or **Associate problem** to link the problematic CI to an existing HP Service Manager incident or problem. A login page for HP Service Manager opens where you enter your HP Service Manager login and password. For details on working with HP Service Manager, see the HP Service Manager documentation. **Note:** Click the **Associate** button directly to access HP Service Manager for the default action—associate an incident or associate a problem. For details on setting the default action, see "HP Service Manager Integration with Business Availability Center Components" in *Solutions and Integrations*.
CI	Displays the name of the CI you determine to be the root cause of the problematic CI. Click the **CI** link to open a window that displays the CIs suspected of being the root cause of the problematic CI and select the radio button for the CI you want to include.
CI name	Displays the name of the problematic CI.

GUI Element (A–Z)	Description
CI Type	Displays the CI type of the problematic CI.
Clear	Click the **Clear** button to clear the root cause CI and reset the field to "Not yet determined".
Description	A free text description of the isolation. For example, you may want to enter details about the root cause of the problem and possible solutions.
Detach	Click the **Detach** button to detach a problematic CI from an HP Service Manager incident or problem to which it is already attached.
Isolation performed by	Displays the login name of the user who performed the initial problem isolation on the problematic CI.
Isolation started at	Displays the creation date and time of the isolation record for the problematic CI.
Layer	Displays the network or infrastructure layer of the CI you consider to be the root cause of the problem. Select a layer from the drop-down list.
New	Click the arrow to the right of the **New** button and select **New incident** or **New problem** to open a new incident or problem in HP Service Manager and associate it with the selected isolation record. A login page for HP Service Manager opens where you enter your HP Service Manager login and password. For details on working with HP Service Manager, see the HP Service Manager documentation. **Note:** Click the **New** button directly to access HP Service Manager for the default action—open a new incident or open a new problem. For details on setting the default action, see "HP Service Manager Integration with Business Availability Center Components" in *Solutions and Integrations*.

GUI Element (A–Z)	Description
Problem start time	Displays the problem start date and time for the problematic CI.
Update Root Cause	Click the **Update Root Cause** button to save any changes you make to the root cause fields (CI, Layer, and Description).

Problem Snapshot Report

Description	Displays a snapshot of system information pertaining to a problem at a given point of time, which you can print, save, email to other people for later use, or attach to an HP Service Manager incident or problem. **To access:** Click the **Snapshot Report** button from any Problem Isolation triage step.
Important Information	The Problem Snapshot report is created in .PDF format and automatically opens in a new browser window. Follow the Adobe Acrobat instructions to print, save or send the file.
Included in Tasks	"Isolate a Problem – Workflow" on page 19

Attach Problem Snapshot

Description	When you generate the Problem Snapshot report, the **Attach** button is displayed at the top of the browser window, above the actual report. Click the **Attach** button to upload the Problem Snapshot report and attach it to an HP Service Manager incident or problem. **Note:** The **Attach** button is enabled only if HP Business Availability Center is integrated with HP Service Manager and an HP Service Manager incident or problem is already attached to the isolation record you are triaging.

Summary

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
CI name	The name of the problematic CI. An icon displaying the CIs status in Dashboard is displayed next to the name.
CI type	The CI type of the problematic CI.
Click to triage using Problem Isolation	Click to go to Problem Isolation on the HP Business Availability Center machine on which the report was generated. The Validation page for the problematic CI opens by default. For details on the user interface, see "Validation Page" on page 104.
Report generated by	The login name of the user who generated the report.
Report generated on	The date and time when the report was generated.
User volume	If the problematic CI is an application monitored by Real User Monitor, or is related to a CI that is an application monitored by Real User Monitor, the following information is listed: ➤ The number of users currently using the application. ➤ The number of users currently experiencing problems when using the application. ➤ The number of users expected to use the application in the next hour. **Note:** If more than one application is applicable, the values shown are the total values for all applicable applications.

Suspects Table

Description	Displays a table with summary data for all the CIs suspected of being the root cause of the problem, sorted by the probability of their being the root cause.
Important Information	For details on the fields included in the Suspects table, see "Suspects Table Pane" on page 98. **Note:** Not all the elements described in the Suspects page are included in the Suspects table in the Problem Snapshot report

On-demand Monitor Details

Description	Includes a separate section for each suspect CI and lists the on-demand monitors run on each one. Failed monitors are displayed before successful monitors.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
Details	Displays the start and end run times of the on-demand monitor as well as any error messages received by the monitor during its run.
Monitor Type	Displays the name of the monitor profile that was run on the suspect CI as well as its status. For details on configuring on-demand monitor profiles, see "New Monitor Profile Page" on page 74.
Parameters	Displays the values of the parameters used by the on-demand monitor during its run.

Discovered Changes Details

Description	Includes a separate section for each suspect CI and lists the discovered changes for the suspect CI and its contained CIs.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
Change date	Displays the date and time at which the update was performed.
Change details	Displays old and new CI values, as well as the names of changed CI attributes, depending on the type of change made.
Change type	Displays the type of change that occurred.
Changed by	Displays the name of the user that manually modified the CI's property, or the name of the DDM Probe or SiteScope monitor that automatically discovered a change made to the CI's property.
Changed CI	Displays the name and type of the CI that was changed.

Events

Description	Includes a separate section for each suspect CI and lists the 10 worst correlated events (that is, the events with the 10 highest event correlation scores) from integrated Enterprise Management Systems (EMS).
Important Information	For details on the fields included in the Events table, see “Correlated Events for Suspect CI Page” on page 28.

Run Books Invoked

Description	Displays information on the HP Operations Orchestration (OO) run book instances that were run on all of a problem's suspect CIs.
Important Information	➤ For details on the fields included in the Run Books Invoked table, see "Run Books Invocations Area" on page 52. ➤ For each run book instance listed in the table, the name of the suspect CI on which it was run is also displayed. ➤ This table is included only if Business Availability Center and OO are integrated. For details on this topic, see "HP Operations Orchestration Integration Overview" in *Solutions and Integrations*.

Run Book Parameters Dialog Box

Description	Enables you to view the parameters used by a run book that is mapped to a selected suspect CI, edit their values, and invoke the run book using the new values. **To access:** Click the **Edit Run Book Parameters** button in the **Invoke Run Book** page.
Useful Links	"Invoke Run Book Page" on page 50 "Run Book Mapping Configuration Wizard" in *Solutions and Integrations*. "HP Operations Orchestration Integration Overview" in *Solutions and Integrations*.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
CI	Displays the selected suspect CI's type.
Description	Displays the description of the run book.

GUI Element (A-Z)	Description
Invoke	Click **Invoke** to launch the run book using the configured parameters.
Run Book	Displays the selected run book's name.
Run Book Parameters	Displays all the parameters used by the run book and the currently configured value for each. You can edit the value. **Note:** Changed parameter values are not saved and are used only when you click the **Invoke** button to launch the run book.

Suspect CI Monitor Configuration Page

Description	Displays the configured on-demand monitors that can run on suspect CIs, and enables you to configure new ones. **To access:** Select **Admin** > **Problem Isolation** > **On-demand Monitors** tab

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
	Click to access the Suspect CI Monitor Configuration Wizard, where you edit an existing suspect CI monitor configuration.
Monitors	Displays the monitors that are run on the selected CI type in the selected topology.
New Suspect CI Monitor Configuration	Click the **New Suspect CI Monitor Configuration** button to open the Suspect CI Monitor Configuration Wizard. For details on the user interface, see "Suspect CI Monitor Configuration Wizard" on page 93.

GUI Element (A–Z)	Description
Suspect CI Node	Displays the node within the selected topology for the CI type on which the monitor is run.
Suspect CI Topology Name	Displays the topology to use when running the monitor.

Suspect CI Monitor Configuration Wizard

Description	Enables you to create on-demand monitors to be run on suspect CIs when isolating a problem, and to edit previously configured on-demand monitors. The link between SiteScope templates, TQLs, and Problem Isolation on-demand monitors is made using the Suspect CI Monitor Configuration Wizard. **To access:** ➤ Click the **New Suspect CI Monitor Configuration** button in the Suspect CI Monitor Configuration page. ➤ Click the **Edit** button in the Suspect CI Monitor Configuration page.
Important Information	➤ When using the Suspect CI Monitor Configuration Wizard to edit a previously configured on-demand monitor: ➤ the title of the wizard is displayed as **Edit Suspect CI Monitor Configuration Wizard**. ➤ the Welcome and Summary pages of the wizard are not displayed. ➤ you do not have to access the wizard pages in a specific order. Click a wizard page name on the left to go directly to that page. ➤ from any of the wizard pages, click the **OK** button to save the monitor configuration and exit the wizard. ➤ When using the Suspect CI Monitor Configuration Wizard to create an on-demand monitor, the title of the wizard is displayed as **New Suspect CI Monitor Configuration Wizard**.
Included in Tasks	"Deploy Problem Isolation – Workflow" on page 153
Wizard Map	The Suspect CI Monitor Configuration Wizard contains: Welcome Page > Select Suspect CI Topology Page > Select Suspect CI Monitors Page > Configure Monitor Parameters Page > Summary Page

Select Suspect CI Topology Page

Description	Enables you to configure the topology name and nodes, as well as the CI type, to be used by the monitors run on suspect CIs. You use this page to link the suspect CI type with a specific node in a selected topology.
Wizard Map	The Suspect CI Monitor Configuration Wizard contains: Welcome Page > **Select Suspect CI Topology Page** > Select Suspect CI Monitors Page > Configure Monitor Parameters Page > Summary Page **Note:** The Welcome and Summary pages are not included in the wizard when editing a previously configured on-demand monitor.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
Select Suspect CI node within the topology	Select the node from within the selected topology for the CI type. Only nodes that are part of the selected topology, and which are of the selected CI type, are displayed.
Select Suspect CI topology	Select the topology to use when running the monitor. Only available Problem Isolation topologies that include the selected CI type are displayed.
Select Suspect CI type	Select the CI type on which the monitor is run. Only CI types that are included in available Problem Isolation topologies are displayed.

Select Suspect CI Monitors Page

Description	Enables you to select the monitors to be run on a specific CI type, in a selected topology.
Important Information	➤ To configure a monitor to be run on the selected CI type in the selected topology, select the check box to the left of the monitor name. ➤ At least one monitor must be selected. ➤ The CI type and topology are selected in the Select Suspect CI Topology page.
Wizard Map	The Suspect CI Monitor Configuration Wizard contains: Welcome Page > Select Suspect CI Topology Page > **Select Suspect CI Monitors Page** > Configure Monitor Parameters Page > Summary Page **Note:** The Welcome and Summary pages are not included in the wizard when editing a previously configured on-demand monitor.

Configure Monitor Parameters Page

Description	Enables you to configure the parameters for the monitors run on suspect CIs. You use this page to map monitor parameters to node attributes in the topology, and set default values for them.
Important Information	Changes made to a SiteScope template on which a monitor profile has already been created are not seen on this page. To include changes made to a SiteScope template, delete the existing monitor profile and recreate it. For details on creating monitor profiles, see "New Monitor Profile Page" on page 74.
Wizard Map	The Suspect CI Monitor Configuration Wizard contains: Welcome Page > Select Suspect CI Topology Page > Select Suspect CI Monitors Page > **Configure Monitor Parameters Page** > Summary Page **Note:** The Welcome and Summary pages are not included in the wizard when editing a previously configured on-demand monitor.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
Attribute	Select the configured node's attribute from which the monitor retrieves parameter values.
Default Value	The default value used by the variable. The default value from the monitor profile is displayed, but can be overwritten.
Monitor/Parameter Name	For each monitor that is run on the suspect CI, the parameters used to pass data from the selected attribute to the monitor are listed.
Node	Select the node in the topology, other than the source node, containing the attributes used by the monitor.

Suspects Page

Description	Displays a table with summary data for all the CIs suspected of being the root cause of the problem, sorted by the probability of their being the root cause. **To access:** Click the **Suspects** option in the Problem Isolation flow bar on any Problem Isolation page.
Included in Tasks	"Isolate a Problem – Workflow" on page 19
Useful Links	"Triage Steps - Standard User Interface Elements" on page 102

Suspects Pane

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
Highlights	Displays whether or not distinct suspect CIs have been found.
Info - Suspects Table	Displays the three suspect CIs considered most likely to be the root cause of the problem, based on their weight. Click to display the **Suspects** table in the Suspects Table Pane.
Recommendation	Displays the recommended steps to take, to help solve the problem.

Suspects Table Pane

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
	Click the **Recalculate Correlations** button to recalculate the **Correlation Score** values with updated metrics data and the **Event Correlation** values with updated events data. The Correlation Score values and the Correlation graph (accessed by clicking a Correlation Score value) are based on the metrics data received up to the time of the last update. Events within the configured time period that were received after the last update, appear in the **Correlated Events for Suspect CI** page, but are not included in the event correlation value displayed. Recalculating correlations updates the displayed values with such events. For details on the user interface, see "Correlated Events for Suspect CI Page" on page 28. **Tooltip:** The date and time that the **Correlation Score** and **Event Correlation** values were last updated.
	Click to open the **Invoke Run Book** page, where you can view and run all the HP Operations Orchestration (OO) run books mapped to the selected suspect CI's type, as well as view reports for previous runs of the run books. For details on the user interface, see "Invoke Run Book Page" on page 50. **Note:** ➤ This icon is displayed only if Business Availability Center and OO are integrated. For details on this topic, see "HP Operations Orchestration Integration Overview" in *Solutions and Integrations*. ➤ This icon is disabled if no run books are mapped to the selected suspect CI.
CI Name	Displays the name of the suspect CI.

GUI Element (A–Z)	Description
CI Type	Displays the CI type icon and name for the suspect CI.
Correlation Score	Displays, in percent, the correlation between the behavior over time of the problematic CI and the suspect CI. The behavior of the suspect CI is based on measurements taken from SiteScope monitors attached to the suspect CI, as configured in the Universal CMDB. The time period used for comparison is determined by Problem Isolation and differs according to the type of data being compared. The default time period is two hours for Real User Monitor pages and six hours for Business Process transactions. Click a correlation score value greater than 0 to open the Correlation graph for the suspect CI. For details on the Correlation graph, see "Correlation Graph" on page 31. **Note:** If no SiteScope monitors are attached to the suspect CI, insufficient data is obtained, or no correlation is found, the correlation score is 0, or in some instances 0.5.
Deployed Monitors Current Status	Displays the status icon for the suspect CI, based on the status of the worst monitor in the group of monitors run on the CI. Also displays the percentage of successful monitors, out of the total number of monitors run on the CI and its descendants. Click the value displayed to see the List of Monitors. For details on the List of Monitors, see "List of Monitors" on page 71. **Tooltip:** The number of problem monitors and the number of total monitors for the suspect CI.
Discovered Changes	Displays the number of changes made to the suspect CI and its descendant CIs. Click the value displayed to see the Change report for the CI. For details on the Change report, see "Change Report"in *Model Management*. **Tooltip:** The number of discovered changes and the time frame in which they were discovered.

GUI Element (A–Z)	Description
Event Correlation	Displays, in percent, the correlation between the behavior over time of the problematic CI and events related to the suspect CI, received from integrated Enterprise Management Systems (EMS). For details on integrating HP Business Availability Center with EMS, see "Integration Administration Application Overview" in *Solutions and Integrations*. The event correlation value is determined from the distance in time of the event to the problem start time, and the severity of the event as received from the EMS. The highest value from all the related events is used. Click an event correlation value greater than 0 to open the Correlated Events for Suspect CI page, where you can see details of all the EMS events related to the suspect CI. For details on the user interface, see "Correlated Events for Suspect CI Page" on page 28. **Note:** ➤ By default, correlation scores are calculated for EMS events with any status and of any severity that occurred from 30 minutes prior to the problem start time to 30 minutes after the problem start time. These settings can be customized. For details on the user interface, see "Correlated Events for Suspect CI Page" on page 28. ➤ If Business Availability Center is not integrated with an EMS, insufficient data is obtained, or no correlation is found, the event correlation value is 0. ➤ Correlation scores are calculated only for suspect CIs with a CI type of Host.
Last update:	Displays the date and time that the **Correlation Score** and **Event Correlation** values were last updated. You can force an update by clicking the **Recalculate Correlations** button.

GUI Element (A–Z)	Description
On-demand Monitor Results	Displays the success ratio of the on-demand monitors run on the suspect CI. Click the success ratio percentage to display the On-demand Monitors Results pane for the suspect CI, from which you can select and run the monitors. For details on the On-demand Monitors Results pane, see "On-demand Monitors Results Pane" on page 78. **Tooltip:** The number of failed on-demand monitors out of the total number of monitors run, and the calculated weighted score.
Run Books Invocations	Displays the number of OO run books that have been run on the suspect CI. Click the value to open the **Invoke Run Book** page, where you can view and invoke all the run books mapped to the suspect CI type, as well as view reports for previous runs of the run books. For details on the user interface, see "Invoke Run Book Page" on page 50. **Note:** This column is displayed only if Business Availability Center and OO are integrated. For details on this topic, see "HP Operations Orchestration Integration Overview" in *Solutions and Integrations*.
Weighted Score	Displays the weighted average of all the displayed data for the suspect CI. The weight is correlated to the chances of the suspect CI being the root cause of the problem. For details on suspect CI weighting, see "Calculating Suspect CI Weights" on page 15. **Tooltip:** The weight and score for each column of data for the suspect CI.

Triage Steps - Standard User Interface Elements

Description	The user interface for the triage steps used to isolate a problem has a standard layout and includes common elements in each step. **To access:** Click the **Triage** button for a selected isolation record in the **Isolation History** page. For details on the Isolation History page, see "Isolation History Page" on page 54.
Included in Tasks	"Isolate a Problem – Workflow" on page 19

Isolation Steps and Flow Bar

Description	At the top of each page, the different triage steps are listed in the recommended order for isolating a problem. Click a step to access the relevant user interface page. Under the steps is a flow bar with an indicator that shows you which isolation step is current.

Left Pane

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
Highlights	Contains the general status of the problem or system, that is relevant to the current triage step.
Info	Contains specific data relating to the current triage step and provides links for displaying detailed data and reports in the main display area of the page.
Recommendation	Based on the data collected and analyzed for the current triage step, displays the recommended triage steps with which to continue, to help solve the problem.

Right Pane

Description	The right pane is the main display area of the page and displays data and reports for the current triage step, that are accessed by clicking the Info messages in the left pane.

Common User Interface Elements

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element	Description
	Click to display both the left and right panes.
	Click to maximize a pane so that it uses the entire display area and hides the second pane.
	Click to minimize a pane so that it is hidden by the other pane, that uses the entire display area.
<Breadcrumb>	At the top of each page, above the flow bar, the path you used to access Problem Isolation is displayed, together with the name of the problematic CI and the status icon of its worst status KPI. Click a link in the path to return to that page. **Tooltip:** Hold the cursor over the status icon to display the problematic CI's name, CI type and the date and time from which the status has been held.
Snapshot Report	Click the **Snapshot Report** button to generate a report of the current system status for a problem, which you can send to other people for further analysis at a later time. For details on the Problem Snapshot report, see "Problem Snapshot Report" on page 86.

GUI Element	Description
On-demand Monitors	Click the **On-demand Monitors** button to open the On-demand Monitors Results pane, where you can view the status of, and run, the on-demand monitors for suspect CIs. For details on the On-demand Monitors results pane, see "On-demand Monitors Results Pane" on page 78.
Properties	Click the **Properties** button to open the Properties pane, where you can view and update a problem's properties. For details on the Properties pane, see "Properties Pane" on page 58.

Validation Page

Description	Revalidates the transactions affected by the problematic CI, and displays the change between their current status and their status at the time the problem was opened. **To access:** ➤ Click the **Validate** option in the Problem Isolation flow bar on any Problem Isolation page. ➤ The default page displayed when accessing Problem Isolation from the right-click menu of a CI in Dashboard.
Important Information	For important information, see "Notes and Limitations" on page 108.
Included in Tasks	"Isolate a Problem – Workflow" on page 19
Useful Links	"Triage Steps - Standard User Interface Elements" on page 102

Left Pane

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
Highlights	Displays the current status of the problem, after revalidation.
Info - Validation	Displays the number and percentage of monitors run, that showed the same or worse status compared to their original status when the problem was opened. Click to display a list of transactions affected by the problem in the Right Pane, which you can manually select and run.
Recommendation	Displays the recommended steps to take, to help solve the problem.

Right Pane

Description	Lists the transactions affected by the problem, which you can select for revalidation. Click a column name to sort the list of transactions by that column. **To access:** Click the information message in the Left Pane.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A–Z)	Description
	Click to refresh the list of transactions displayed.
<Legend>	Describes the icons used to denote the open and current statuses.

GUI Element (A–Z)	Description
Current Status	The current status of the transaction, based on the thresholds configured for the transaction in End User Management Administration. The valid statuses are: ➤ **Idle.** ➤ **Pending.** Selected and waiting to run ➤ **Running.** Currently running ➤ **OK.** The transaction ran successfully, with the measurement calculated for the KPI falling within the value range for the OK objective. ➤ **Minor.** The transaction ran successfully, with the measurement calculated for the KPI falling within the value range for the Minor objective. ➤ **Critical.** The transaction ran successfully, with the measurement calculated for the KPI falling within the value range for the Critical objective. ➤ **Failed.** The transaction did not run successfully. **Tooltip:** A summary of the transaction's statuses during the relevant time period.
Host Name	The name of the agent machine on which the transaction is run.
Location Name	The logical location for which the transaction is run.

GUI Element (A–Z)	Description
Open Status	Displays the most severe status of the transaction during the configured time period, based on the thresholds configured for the transaction in End User Management Administration. The valid statuses are: ➤ **OK.** The transaction ran successfully, with the measurement calculated for the KPI falling within the value range for the OK objective. ➤ **Minor.** The transaction ran successfully, with the measurement calculated for the KPI falling within the value range for the Minor objective. ➤ **Critical.** The transaction ran successfully, with the measurement calculated for the KPI falling within the value range for the Critical objective. ➤ **Failed.** The transaction did not run successfully. **Tooltip:** A summary of the transaction's statuses during the relevant time period. **Note:** If the problem has a status of **Open**, the configured time period relates to the time that the problem was opened. Otherwise, the period of time relates to the current system time.
Run Transaction	Click the **Run Transaction** button to start manual revalidation of selected transactions.
Script Name	The name of the script in which the transaction is included.

GUI Element (A–Z)	Description
Transaction Name	The name of the transaction.
Trend	Displays the trend of the change between the Open Status and the Current Status. The valid trend options are: ➤ **No available data.** ➤ **No Change.** The current status has not changed since the problem was opened. ➤ **Improved.** The current status is better than the status when the problem was opened. ➤ **Worse.** The current status is worse than the status when the problem was opened. **Tooltip:** The trend status.

Notes and Limitations

The following notes and limitations apply to the Validation page:

- Transactions for revalidation are selected based on their relationship with the problematic CI in the Universal CMDB.
- Transactions for a selected problem are automatically revalidated when accessing Problem Isolation from Dashboard. To disable automatic revalidation, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the **Auto Run Diagnostic Monitors** entry in the **On-demand Monitoring** table. Modify the value to **false**.
- By default, only problematic transactions (that is, transactions with a status of failed, minor, or critical when the problem was opened) are automatically revalidated. To change the default setting of which kind of transactions are automatically revalidated, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the **Transaction status for automatic revalidation** entry in the **Revalidation** table. Modify the value from the drop-down list as required.
- Successful transactions (that is, transactions that had a status of OK when the problem was opened) are not automatically revalidated.

- You can select transactions and manually run the revalidation process on them.
- When a transaction is run, the script in which the transaction is included is run, so other transactions included in the script are also run. This means that you may see other transactions running, that you did not select.
- Transactions are revalidated according to their status. Failed transactions are revalidated first, followed by those with a status of critical, minor, and OK, in that order.
- Each host runs one transaction at a time.
- A script is revalidated on a configured number of hosts only. To change the number of hosts on which a script is revalidated, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the **Maximum number of agents** entry in the **Revalidation** table. Modify the value as required. An entry of -1 causes scripts to be revalidated on all relevant hosts, without limitation.
- To select a transaction for manual revalidation, click the transaction name. You can select multiple transactions by holding the CTRL key down (for multiple individual selections), or the Shift key (for multiple sequential selections) when selecting transactions.
- By default, the current status used to revalidate a transaction is based on the transaction's worst status in the period of 30 minutes before the problem start time to 30 minutes after the problem start time. To modify the default time period, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the **Revalidation time range** entry in the **Revalidation** table. Modify the value to the required number of hours to be used before and after the problem start time.

Troubleshooting and Limitations

This chapter includes troubleshooting and limitations for Problem Isolation Reactive Analysis.

SiteScope Template Changes not Included in Suspect CI Monitor Configurations

Once a monitor profile has been created on a SiteScope template, and the monitor profile is included in a Suspect CI Monitor configuration, changes made to the SiteScope template are not shown in the Suspect CI Monitor configuration. To include the changes, delete and recreate the monitor profile. For details on creating monitor profiles, see "New Monitor Profile Page" on page 74.

On-demand Monitors Fail to Retrieve User Names and Passwords

On-demand monitors cannot retrieve a user name and password for manually created CIs. This causes the monitors to fail when run on such CIs. Before running an on-demand monitor, you can specify a user name and password to be used by the monitor. For details on specifying monitor parameters, see "On-demand Monitor Parameters Dialog Box" on page 77.

Revalidation Cannot be Made on Business Process Monitor Transactions That Use Basic Authentication

The Problem Isolation Validation step is unable to revalidate transactions on virtual users (Business Process Monitors) that use basic authentication.

Node Attributes Without Display Labels are not Displayed as Available Attributes

When configuring monitor parameters in the Suspect CI Monitor Configuration Wizard, a node's attributes that do not have a display label defined in the Universal CMDB CI type manager are not displayed in the list of available attributes for the node.

Oracle Monitors Cannot Connect to an Oracle Server

In some instances, Problem Isolation Oracle monitors may be unsuccessful in connecting to an Oracle server. In such cases, you should change the driver used by SiteScope to one that is specific for your Oracle server. For details on changing the driver used by SiteScope, refer to the relevant SiteScope documentation.

On-demand Monitors Fail Due to Missing CI Types

Problem Isolation assumes the automatic discovery of ports, Windows services, and Unix processes. If these CI types are not discovered, or cannot be found in the Universal CMDB, some of the on-demand monitors may fail.

To fix this problem, use the Query Manager to remove all port, service, and process nodes from all the TQLs in the Correlation\PM_Diagnostic folder, and remove all references to these nodes from the configured on-demand monitors. For details on working with the Query Manager, see "Query Manager Window" in *Model Management*. For details on configuring on-demand monitors, see "Suspect CI Monitor Configuration Wizard" on page 93.

The following is a list of the discovery patterns assumed to be run, in the order displayed, for Problem Isolation:

- ICMP_NET_Dis_IpC
- Host_ID_Discover
- NTCMD_NET_Dis_Connection
- SNMP_NET_Dis_Connection
- TTY_Net_Dis_Connection
- WMI_NET_Dis_Connection
- TCP_NET_Dis_Port
- WMI_HR_Service
- WMI_HR_Disk
- WMI_HR_Software
- TTY_HR_All

- TTY_HR_Process
- TTY_HR_Software
- TTY_HR_Disk
- FILE_Mon
- TCP_Webserver_Detection
- Apache
- SQL_NET_Dis_Connection

Problem Isolation TQLs are not Visible

If the Problem Isolation **PM.zip** file was not properly deployed, you may experience problems such as the Problem Isolation TQLs not being visible. In such an instance, you should redeploy the file. For details on redeploying the PM.zip file, see "Package Manager Window" in *Model Management*.

The User Volume Report Does not Display Properly

If you are having trouble viewing the User Volume report, you may require Flash player to properly view the report. Install Flash player on your machine, and then try accessing the report again. For details on viewing reports with Adobe Flash player, see "Viewing Reports with Adobe Flash Player" in *Reports*.

No On-demand Monitors are Shown for a Suspect CI

Suspect topologies that are created automatically by SiteScope do not include credential related CIs (such as telnet, ssh, wmi, and ntcmd), which are required by SiteScope to retrieve credential information such as user names and passwords. The credential information is used by SiteScope when running on-demand monitors. On-demand monitors using topologies that are missing credential related CIs do not appear in the list of on-demand monitors for a suspect CI.

To fix this problem, edit the suspect topology and change the cardinality of the related credential CIs so that they are not mandatory, and configure the required credentials manually for the on-demand monitors. For details on changing cardinality in a TQL, see "Topology Query Language User Interface" in *Model Management*. For details on configuring on-demand monitors, see "Suspect CI Monitor Configuration Wizard" on page 93.

Part II

Proactive Analysis

2

Problem Isolation Proactive Analysis

This chapter includes the main concepts, tasks, and reference information for proactive analysis in Problem Isolation.

This chapter includes:

Concepts

- Proactive Analysis Overview on page 118
- Expected Transaction Behavior on page 120
- Permissions on page 122

Tasks

- Configure Proactive Analysis – Workflow on page 122
- Configure Expected Transaction Behavior on page 123

Reference

- Proactive Analysis User Interface on page 123

Proactive Analysis Overview

Problem Isolation includes both reactive analysis, for isolating enterprise problems discovered in HP Business Availability Center, and proactive analysis, for detecting application anomalies and their probable causes. For details on reactive analysis, see "Reactive Analysis Overview" on page 12.

The proactive analysis process analyzes data from various sources (such as monitors, changes, and incidents) to detect anomalies in selected applications and business services, and by correlating all the data tries to determine the probable causes of these anomalies.

The proactive analysis process analyzes the events (samples) for the Business Process Monitor transactions and Real User Monitor pages that are connected to the applications and business services that you select, that were created since the previous run of the proactive analysis process. The process compares the actual performance and availability of the transactions and pages with the expected transaction behavior for each hour of the day, to determine problematic behavior. For details on expected transaction behavior, see "Expected Transaction Behavior" on page 120. Similar sequential hours are combined. For example, three consecutive good hours (that is, without any problematic behavior), followed by two consecutive bad hours (that is, with problematic behavior), are combined into one good segment and one bad segment. The bad segments are called anomalies and contain any combination of transaction or page availability problems and breaches in expected transaction behavior. For each application or business service, the proactive analysis process determines the CIs it considers to be the most likely causes of the problematic behavior. For each anomaly, the process examines SiteScope measurements for these CIs and correlates them with the behavior of the transactions and pages in the anomaly during the relevant time range.

You use the Proactive Analysis page to list the anomalies that have been identified and to view the data for a selected anomaly. You view data for a specific transaction or page that occurred in an anomaly's time range (by default, the transaction or page with the most severe anomaly, as calculated by the proactive analysis process, is displayed) and can see any discovered changes or requests for change (RFCs), incidents, and events received from integrated Enterprise Management Systems (EMS), that occurred in the same time range. You can also see the number of users that accessed the application during the anomaly's time range and of those, the number of users that experienced problems. The measurements returned by SiteScope monitors run on the CIs suspected of causing an anomaly, that are most correlated to the selected transaction or page, are also displayed and you can select the measurements you want to display together with the transaction or page data in the same graph. This enables you to see the correlation between the transaction or page data, the suspect CI measurements, changes (both discovered and planned), incidents, users, and events. You can also display the expected transaction behavior, which enables you to see the actual behavior compared to the expected behavior. For details on the Proactive Analysis page, see "Proactive Analysis Page" on page 128.

You configure proactive analysis by selecting the applications and business services to be analyzed and setting a time for the process to run on a daily basis. Each day, at the configured time, the proactive analysis process runs, as a new thread, for each selected application and business service. For details on configuring proactive analysis, see "Proactive Analysis Configuration Page" on page 125.

Expected Transaction Behavior

Proactive Analysis determines anomalies based on actual transaction behavior in comparison to expected transaction behavior. Expected transaction behavior is calculated for each hour of the day (from 00:00 to 23:59), for each business process transaction and Real User Monitor page, for each application configured for proactive analysis. Expected transaction behavior is based on up to 35 days worth of actual transaction behavior data.

A daily process examines the previous day's hourly aggregated data and for each hour, calculates the transaction behavior for each transaction and page. The day's figures are compared to previously calculated and stored transaction behavior data to ensure that they are within acceptable limits (that is, there are no aberrations) and are then themselves added to the stored transaction behavior data. Up to 35 days of calculated transaction behavior data is stored, at which point a rolling date policy is used. That is, for each new day's data added, the earliest date's stored data is removed.

Each day of the week is categorized as either a working day or non working day. By default, non working days are Saturday and Sunday. You can configure which days you want to be considered as non working days. For details on how to perform this task, see "Configure Expected Transaction Behavior" on page 123. Proactive analysis determines anomalies only when there is reliable expected transaction behavior data for the relevant type of day—working or non working. By default, expected transaction behavior data is considered reliable when there are at least four stored entries for a specific hour (in effect, data for four days) for a specific category of day. For example, using the default setting of Saturday and Sunday configured as non working days, one week of transaction behavior data is considered reliable for working days (as there are five working days in the week), but is not considered reliable for non working days (as there are only two non working days in the week). To have reliable transaction behavior data for non working days, you would need two week's data. You can configure the minimum number of days for transaction behavior data to be considered reliable. For details on how to perform this task, see "Configure Expected Transaction Behavior" on page 123.

By default, the daily process of calculating the previous day's transaction behavior data is run at 03:000. You can configure the time at which the process runs. For details on how to perform this task, see "Configure Expected Transaction Behavior" on page 123. It is recommended that you configure the process to run at 03:00 or later, but before the proactive analysis process runs. If you configure the process to run before 03:00 or after the proactive analysis process runs, transaction behavior data is calculated for the day before the previous day, instead of for the previous day. For example, if you configure the process to run at 02:00, then on the 16th. of the month, transaction behavior data is calculated for the 14th. of the month. This results in only 34 days of transaction behavior data being stored, instead of 35 days of data.

When there is sufficient transaction behavior data stored for reliable expected transaction behavior data to be calculated, the proactive analysis process calculates anomalies for transactions and pages by comparing actual performance data with expected transaction behavior data. By default, expected transaction behavior data for a specific hour is the average of all the stored transaction behavior data for that hour, plus four standard deviations. You can configure the number of standard deviations to add. For details on how to perform this task, see "Configure Expected Transaction Behavior" on page 123. If there is insufficient data to calculate reliable expected transaction behavior for a specific hour, anomalies are not calculated for that hour and also, a gap will appear for that hour when you display expected transaction behavior in the proactive analysis graph.

For details on proactive analysis, see "Proactive Analysis Overview" on page 118.

For details on the proactive analysis graph, see "Proactive Analysis Page" on page 128.

Permissions

You must have the Problem Isolation **Advanced User** or **Administrator** role to view proactive analysis. You must have the Problem Isolation **Administrator** role or the **System Modifier** role to configure proactive analysis. To access the Permissions page, select **Admin** > **Platform** > **Users and Permissions**. For details on this topic, see "Permissions Overview" in *Platform Administration*.

Configure Proactive Analysis – Workflow

This task describes the working order for configuring proactive analysis.

This task includes the following steps:

- "Configure the Proactive Analysis Process" on page 122
- "Configure Expected Transaction Behavior" on page 122
- "Results" on page 122

1 Configure the Proactive Analysis Process

Configure the applications that the proactive analysis process analyzes, as well as the time that the process runs each day. For details on the user interface, see "Proactive Analysis Configuration Page" on page 125.

2 Configure Expected Transaction Behavior

Configure the settings that determine how expected transaction behavior is determined. For details on how to perform this task, see "Configure Expected Transaction Behavior" on page 123.

3 Results

Proactive analysis is now configured and the proactive analysis process will run on a daily basis. You use the Proactive Analysis page to view proactive analysis data. For details on the user interface, see "Proactive Analysis Page" on page 128.

Configure Expected Transaction Behavior

This task describes how to change the default settings that determine how expected transaction behavior is calculated in proactive analysis.

To configure expected transaction behavior:

Select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and modify the values of the following entries in the **Proactive** table:

Name	Description	Default Value
Anomaly deviation threshold	The number of standard deviations to add to the calculated average transaction behavior to determine expected transaction behavior.	4
Baseline task run time	The hour at which the daily process that calculates expected transaction behavior runs.	3
Minimum day count	The minimum number of data entries for a specific hour for expected transaction behavior to be considered reliable.	4
Weekend and rest days	The days of the week considered as non work days. Enter a comma separated list using the values 1–7, where 1 represents Sunday.	1,7

Proactive Analysis User Interface

This section includes (in alphabetical order):

- Anomaly Menu Options on page 124
- Proactive Analysis Configuration Page on page 125
- Proactive Analysis Page on page 128

Anomaly Menu Options

Description	Enables you perform various actions on a selected anomaly listed in the **Anomalies** pane of the **Proactive Analysis** page. **To access:** Right-click an anomaly
Useful Links	"Proactive Analysis Page" on page 128

The available options for an anomaly can be a subset of the following:

Menu Option (A-Z)	Description
Add Name	Enter a name for an anomaly. The name is added to the details displayed in the anomaly list. **Syntax exceptions:** Cannot exceed 255 characters.
Delete Anomaly	Delete an anomaly.
Edit Name	Edit an anomaly name. **Syntax exceptions:** Cannot exceed 255 characters. **Note:** ➤ This option is enabled only if the selected anomaly has a name. ➤ You can delete an anomaly's name by clearing it when editing the name.
Read	Mark an anomaly as read. This results in the anomaly and its details being displayed in a regular font. **Note:** This option is enabled only if the selected anomaly is marked as unread.
Unread	Mark an anomaly as unread. This results in the anomaly and its details being displayed in a bold font. **Note:** This option is enabled only if the selected anomaly is marked as read.

Proactive Analysis Configuration Page

Description	Enables you to configure the applications and business services that the proactive analysis process analyzes, as well as the time that the process runs each day. **To access:** ➤ Select **Admin** > **Problem Isolation** > **Proactive Analysis** tab ➤ Click the **Configure Proactive Analysis** button in the **Anomalies** pane of the **Proactive Analysis** page.
Important Information	By default, you can configure a maximum of ten applications and business services for proactive analysis. To modify the maximum number of applications and business services you can configure, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the **Maximum number of CIs for analysis** entry in the **Proactive** table. Modify the value to the required number.
Useful Links	"Proactive Analysis Overview" on page 118

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
	Click the right or left facing arrow to move a selected application from one pane to the other.
	Click the right or left facing arrow to move all applications from one pane to the other.

GUI Element (A-Z)	Description
<Left pane>	Displays the name and type of all the applications and business services available for proactive analysis. Click an application name to select it. **Default value:** CIs with the following CI types are displayed: ➤ logical_application ➤ business_service_for_catalog ➤ sap_resource ➤ siebel_application ➤ websphere **Customization:** To modify the default list of CI types, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the **Display CI types** entry in the **Proactive** table. Enter the required CI types as a comma separated list.
<Right pane>	Displays the name and type of all the applications already configured for proactive analysis. Click an application name to select it.

GUI Element (A-Z)	Description
Run daily at	Select the time (hours and minutes) that you want the proactive analysis process to run each day. **Tip:** ➤ It is recommended not to configure the proactive analysis process to run on the hour (for example, at 01:00, or 04:00) so that it does not coincide with HP Business Availability Center aggregation. Instead, set the process to run at a time that includes minutes (for example, at 01:20, or 04:40). ➤ It is recommended to run the proactive analysis process after the discovery process has run so that discovered changes are included in proactive analysis data. ➤ It is recommended to run the proactive analysis process at a time when there is low utilization by HP Business Availability Center.
Server Time	Displays the time and time zone set for your HP Business Availability Center Gateway Server.

Proactive Analysis Page

Description	Enables you to view anomalies in the behavior of transactions and pages for selected applications, as well as measurements that have a high correlation to the transaction or page behavior. Also shows incidents, requests for change (RFCs), and discovered changes that may be related to the application. **To access:** Select **Applications** > **Problem Isolation** > **Proactive Analysis** tab
Important Information	➤ When data is displayed for a time range that is within one day prior to the anomaly start time to one day after the anomaly end time, raw data is displayed for business process transactions at 15 minute intervals and aggregated data is displayed for Real User Monitor pages at 5 minute intervals. In all other instances, aggregated data is displayed at hourly intervals. In the Incidents and Changes graphs, aggregated data is displayed at daily intervals when the graph time range is for a week or more. ➤ Hourly and daily aggregated data may not show the same results as raw data or data aggregated at 5 minute intervals, and may not reflect the actual data for a single anomaly. ➤ All references to HP Service Manager are also applicable to HP ServiceCenter.
Useful Links	"Proactive Analysis Overview" on page 118 "Expected Transaction Behavior" on page 120

This section includes the following topics:

➤ "Anomalies Pane" on page 129

➤ "Proactive Analysis Graph Pane" on page 133

➤ "Correlation Measurements Pane" on page 143

➤ "Correlated Events Pane" on page 145

Anomalies Pane

Description	Displays the anomalies identified by the proactive analysis process and enables you to set a filter to view anomalies of certain types, for a specific application, or for selected dates. The anomalies that match the filter you set are displayed in the lower part of the pane. The anomalies are grouped by date or application and are sorted. **Default value:** The first time you access this page, no filter is set and all the anomalies that have been identified and saved are displayed. When you subsequently access this page, the last filter you set is automatically used, unless you logged out of HP Business Availability Center from the Proactive Analysis page, in which case the last filter settings are not saved.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
	Hide/Show button. Toggle between showing and hiding the **Anomalies** pane.
	Filter button. Toggle between showing and hiding the filter fields, which you use to filter the displayed anomalies.
	Sort button. Toggle between showing the anomalies in ascending or descending order.
	Configure Proactive Analysis button. Click to open the **Proactive Analysis Configuration** dialog box, where you configure the applications to be analyzed and the analysis schedule. For details on the Proactive Analysis Configuration dialog box, see “Proactive Analysis Configuration Page” on page 125.
	Delete Anomaly button. Click to delete a selected anomaly permanently from the anomalies list.

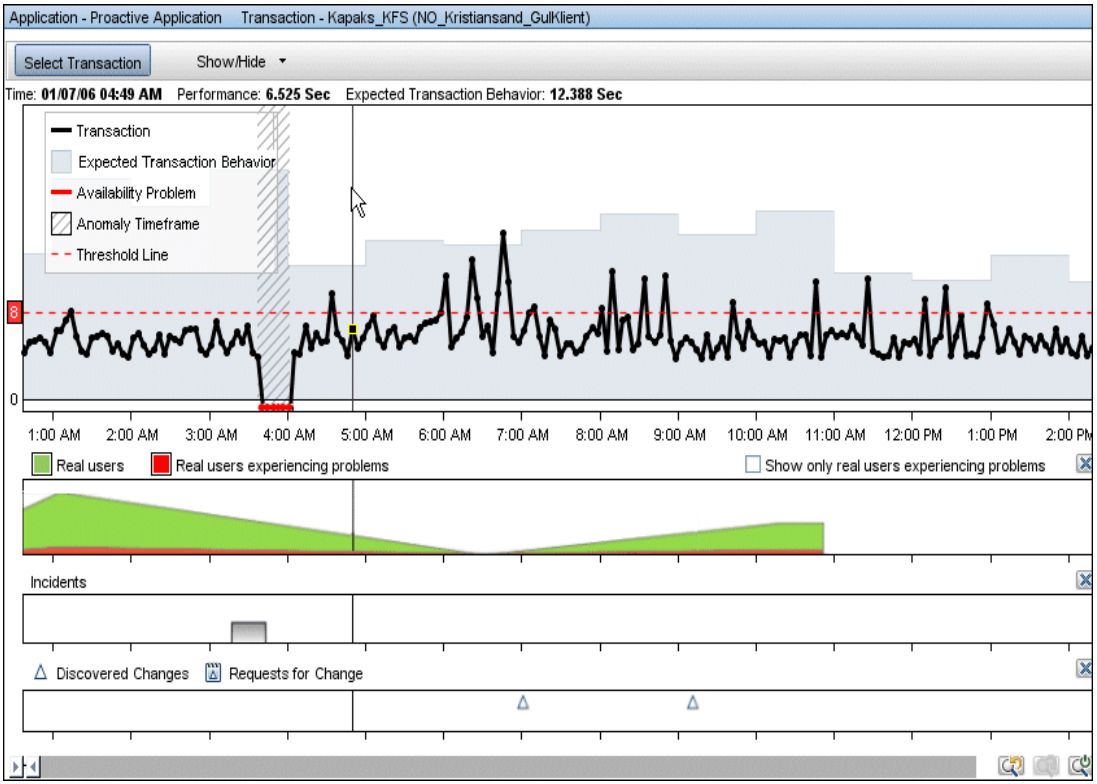
GUI Element (A-Z)	Description
	Anomalies button. Place your cursor on this button to temporarily display the **Anomalies** pane when it is hidden. **Note:** This button is only displayed when the Anomalies pane is hidden.
	Availability Problems icon. Indicates that an anomaly contains transactions or pages with availability problems.
	Performance Problems icon. Indicates that an anomaly contains transactions or pages that exceeded their expected transaction behavior.
	Increased Response Time Anomaly icon. Indicates that an anomaly contains transactions or pages with a significant increase in their response time. **Note:** This icon is applicable only to anomalies found in Problem Isolation in Business Availability Center version 7.50. You cannot use this icon when setting the anomaly type in the filter.
	Changes icon. Indicates that there are discovered changes in the time range starting 24 hours prior to the anomaly start time and ending 24 hours after the anomaly end time.
	Incidents icon. Indicates that there are HP Service Manager incidents during the anomaly time period.

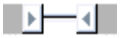
GUI Element (A-Z)	Description
<Anomalies>	The anomalies that match the filter you set are displayed in the bottom half of the pane, sorted by application or date. For each anomaly, the application name, date range, and icons for the applicable anomaly types are displayed. Click an anomaly in the list to display it in the **Proactive Analysis** graph. Right-click an anomaly to access its context menu options. For details on the user interface, see "Anomaly Menu Options" on page 124. Double-click an anomaly to add a name to the anomaly, or edit an existing name. The name cannot exceed 255 characters. **Tooltip:** The application name, anomaly name, anomaly date range, anomaly type icons and descriptions, and the number of incidents and changes. **Note:** Anomalies that you have not viewed (unread anomalies) are displayed in a bold font and anomalies that you have viewed (read anomalies) are displayed in a regular font. When you move from one anomaly to another, the previous anomaly is automatically marked as read.
Anomaly Type	Select the anomaly type by which to filter the displayed anomalies. Select **None** to display all anomaly types.
Application	Select an application from the drop-down list to filter the displayed anomalies for a specific application. Select **None** to display anomalies for all applications. **Default value:** None
Arrange by	Select the criteria by which you want to group the anomalies—start date or application name.
From	Select this radio button to filter the anomalies whose start date is within a configured range. Click the down arrow to display a calendar from which you select the start date and time for the filter range.

GUI Element (A-Z)	Description
Last	Select this radio button to filter the anomalies whose start date is within a selected number of weeks back. Select the number of weeks back to use from the drop down list.
Show only anomaly types with Incidents indicators	Select this check box to display anomalies for which there are HP Service Manager incidents.
Show only anomaly types with Changes indicators	Select this check box to display anomalies for which there are discovered changes in the time range starting 24 hours prior to the anomaly start time and ending 24 hours after the anomaly end time.
To	Click the down arrow to display a calendar from which you select the end date and time for the filter range. **Note:** This field is only enabled when the **From** radio button is selected.

Proactive Analysis Graph Pane

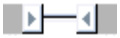
The following is an example of the Proactive Analysis graph.



Description	Enables you to view the response times of a business process transaction or the server time of a Real User Monitor page during a period of time identified as an anomaly for an application. You can also view expected transaction behavior, incidents, requests for change (RFCs), and discovered changes, as well as measurements returned by SiteScope monitors run on the CIs suspected of causing the anomaly, for the same time range. This enables you to correlate the data visually.
Important Information	➤ Transaction data and expected transaction behavior are displayed in the Proactive graph for 90 days by default (45 days prior to and 45 days after the middle of the anomaly time frame). If the anomaly time frame is longer than this period, transaction data and expected transaction behavior are displayed for the entire anomaly time frame. To modify the default number of days for which transaction data and expected transaction behavior are displayed, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the **Transaction view period** entry in the **Proactive** table. Modify the value to the total number of days required. ➤ You can change the time range or zoom of the graph by using the following methods: ➤ Left-click anywhere in the graph and drag the cursor to the right or left to select an area. The graph display zooms in to the selected time range. ➤ Right-click anywhere in the graph and drag the cursor to the left to move to an earlier time range, or to the right to move to a later time range. The zoom remains the same. ➤ Use the **Time Scroll** bar  to change the time range or zoom.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
	The horizontal dashed line on the graph indicates the critical transaction time threshold configured for a transaction included in the graph, or the server time threshold configured for a page included in the graph. To the left of the line, a small, red square displays the number of seconds configured as the threshold. **Default value:** Hidden **Note:** You can hide or display the threshold line by clicking the **Threshold** option in the **Show/Hide** menu.
	Previous Zoom button. Click to display the graph with the previous time range used.
	Next Zoom button. Click to display the graph with the next time range used.
	Reset Zoom button. Click to display the graph with the original time range used.
	Discovered Changes icon. Indicates that there are discovered changes at a given point of time. Click the icon to display details of the discovered changes in a new window. **Tooltip:** The number of discovered changes for the given point of time.
	Requests For Change icon. Indicates that there are requests for change (RFCs) in HP Service Manager at a given point of time. Click the icon to display details of the RFCs in a new window. **Tooltip:** The number of RFCs for the given point of time.

GUI Element (A-Z)	Description
	**Time Scroll bar.** Click the bar between the two arrows and drag the bar to the left to display an earlier time range, or to the right to display a later time range. Click the left arrow and drag it to the left to change the start time of the time range to an earlier time, or to the right to change it to a later time. Click the right arrow and drag it to the left to change the end time of the time range to an earlier time, or to the right to change it to a later time. **Note:** As the length of the time range changes, the time units displayed may change between minutes, hours, days, and weeks to accommodate the relevant data.
	Located above the User Volume, Incidents, and Changes graphs. Click to hide the relevant graph. Use the **Show/Hide** option to show the graphs again.
<Anomaly time frame> (Blocked area with gray lines)	Denotes the anomaly time frame.

GUI Element (A-Z)	Description
<Changes>	The Changes graph is located below the main proactive analysis graph and displays icons for any date and time in the graph's time range for which there are discovered changes in HP Business Availability Center, or requests for change (RFCs) in HP Service Manager. Click a change icon to display details of the changes in a new window. **Tooltip:** The number of changes for the applicable date and time. **Note:** ➤ The Changes graph uses the same time range as the main proactive analysis graph. ➤ RFCs and discovered changes data is aggregated hourly or daily, depending on the graph's time range. Click a change icon to display details of all the changes included in the aggregated data, in a new window. ➤ Changes might be displayed in the Changes graph, even though no changes are indicated for the anomaly in the Anomalies pane. Changes are displayed for the entire time range of the Changes graph, although the change icon is only displayed in the Anomalies pane if there were changes in the time range starting 24 hours prior to the anomaly start time and ending 24 hours after the anomaly end time. ➤ You can hide or display the Changes graph by clicking the **Changes** option in the **Show/Hide** menu.
<Correlation measurements> (Thin colored lines connecting data points)	Display the values of the correlation measurements you select in the **Correlation Measurements** pane to include in the graph.

GUI Element (A-Z)	Description
<Date and response time indicator> (vertical black line)	A vertical black line appears on the graph when you place the cursor in the main area of the graph. This line indicates a specific data point in the graph and the relevant date and time, as well as the applicable performance measurement and expected transaction behavior for the data point, are displayed at the top of the graph. A small black square on the line shows the data point in the graph. **Tooltip:** The relevant date and time and the applicable performance measurement.
<Expected Transaction Behavior> (Blocked gray area)	Denotes the expected transaction behavior for the displayed transaction or page. **Tooltip:** The expected transaction behavior threshold time and value. **Note:** You can hide or display the expected transaction behavior by clicking the **Expected Transaction Behavior** option in the **Show/Hide** menu.
<Legend>	Describes the color coding used in the graph. **Note:** You can hide or display the legend by clicking the **Legend** option in the **Show/Hide** menu. The legend is displayed by default.
<Time> (x-axis)	Displays the time division units applicable for the graphs's time range.
<Transaction behavior> (Thick black line connecting data points)	Indicates the behavior (response time and availability) of the transaction or page included in the graph, during the graph's time range. The line is displayed in red when representing an availability problem. **Tooltip:** For each data point, the transaction or page's response time is displayed, or details of availability problems (the number of passes, failures, and timeouts). **Note:** If no sample is received for an hour, a break in the black line is displayed for the relevant point in the time range.

GUI Element (A-Z)	Description
<User Volume graph>	The User Volume graph is located below the main proactive analysis graph. It displays colored areas that indicate the total number of users for an application (green area) and the number of those users that experienced problems (red area) for any date and time in the graph's time range. To display only the users that experienced problems in the application, select the **Show only real users experiencing problems** check box. **Tooltip:** The applicable date and time, the total number of users for the application, the total number of users that experienced problems, the number of users that experienced availability problems, and the number of users that experienced performance problems. **Note:** ➤ The User Volume graph uses the same time range as the main proactive analysis graph. ➤ User volume data is aggregated by five minute or hourly intervals, depending on the graph's time range. ➤ You can hide or display the User Volume graph by clicking the **User Volume** option in the **Show/Hide** menu.

GUI Element (A-Z)	Description
Incidents	The **Incidents** graph is located below the main proactive analysis graph and displays a gray bar for any date and time in the graph's time range for which there are incidents in HP Service Manager. The bar's height is determined by the number of incidents it represents. Click a bar to display details of the incidents in a new window. **Tooltip:** The number of incidents in HP Service Manager for the applicable date and time. **Note:** ➤ The Incidents graph uses the same time range as the main proactive analysis graph. ➤ Incidents data is aggregated hourly or daily, depending on the graph's time range. Click a bar to display details of all the incidents included in the aggregated data, in a new window. ➤ You can hide or display the Incidents graph by clicking the **Incidents** option in the **Show/Hide** menu.
Performance	Located above the graph, displays the transaction response time or page server time indicated by the vertical black line.

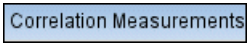
GUI Element (A-Z)	Description
Select Transaction	Click **Select Transaction** to display a list of an application's business process transactions and Real User Monitor pages that showed anomalous behavior during the anomaly's time range (that is, had availability or performance problems). The transactions and pages are sorted in descending order according to the extent of their anomaly and also show their type (**Virtual** for business process transactions or **Real** for Real User Monitor pages), location (for transactions only) and anomaly types. Click a transaction or page name in the list to display the Proactive Analysis graph for that transaction or page and to change the Correlation Measurement list to the measurements with the highest correlation to that transaction or page during the anomaly time period. **Default value:** The most anomalous transaction or page during the anomaly's time range is automatically selected when the Proactive Analysis graph is first displayed for an anomaly. **Tooltip:** Place the cursor over a transaction or page name in the list to display its full name, as well the URL of Real User Monitor pages.

GUI Element (A-Z)	Description
Show/Hide	Click **Show/Hide** to display a list of additional graphs you can include in the Proactive Analysis Graph pane, and additional elements you can include in the main Proactive Analysis graph. You hide or display a graph or element by clicking the relevant option in the **Show/Hide** menu to select or unselect it. Selected options are denoted by a check mark. The following options are available: ➤ **Changes.** Displays the Changes graph, which indicates requests for change (RFCs) and discovered changes during the main graph's time frame. ➤ **Incidents.** Displays the Incidents graph, which indicates HP Service Manager incidents during the main graph's time frame. ➤ **User Volume.** Displays the User Volume graph, which indicates the number of users for an application, and the number of those experiencing problems, during the main graph's time frame. ➤ **Legend.** Displays the main graph's legend. ➤ **Threshold.** Display's the critical transaction time threshold configured for a transaction, or the server time threshold configured for a page, included in the main graph. ➤ **Expected Transaction Behavior.** Displays the expected transaction behavior for the displayed transaction or page.
Time	Located above the graph, displays the specific time indicated by the vertical black line.

Correlation Measurements Pane

Description	Lists the measurements returned by SiteScope monitors run on the CIs suspected of causing an anomaly, that are most correlated to the transaction or page displayed in the main proactive analysis graph. You can select measurements to be included in the main proactive analysis graph.
Important Information	➤ Correlation measurements are displayed in the Proactive graph for 14 days by default (7 days prior to and 7 days after the middle of the anomaly time frame). If the anomaly time frame is longer than this period, correlation measurements are displayed for the entire anomaly time frame. To modify the default number of days for which correlation measurements are displayed, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the **Metric view period** entry in the **Proactive** table. Modify the value to the total number of days required. ➤ By default, the measurements are displayed in descending order, according to their correlation to the transaction or page displayed in the main proactive analysis graph. Click any column header in the pane to sort the list of displayed measurements by that column. Click the header of the column by which the list is already sorted to reverse the sort order. ➤ In the same area of the page, you can display either the Correlation Measurements pane or the Correlated Events pane by clicking the appropriate tab. For details on the Correlated Events pane, see "Correlated Events Pane" on page 145.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
	Hide/Show button. Toggle between showing and hiding the **Correlation Measurements** pane.
	**Correlation Measurements button.** Place your cursor on this button to temporarily display the **Correlation Measurements** pane when it is hidden. **Note:** This button is only displayed when the Correlation Measurements pane is hidden.
<Check box>	Select a check box next to a correlation measurement to include it in the main proactive analysis graph.
CI Name	Displays the CI name of the suspect CI.
CI Type	Displays the CI type of the suspect CI.
Correlated Events	Click the **Correlated Events** tab at the bottom of the pane to view a table of events correlated to the selected anomaly's start time. For details on the user interface, see "Correlated Events Pane" on page 145.
Correlation (%)	Displays the correlation percentage of the measurement to the selected transaction.
Legend	Describes the color coding used for the correlation measurements when they are displayed in the main proactive analysis graph.
Measurement Name	Displays the name of the measurement returned by the monitor when run on the suspect CI.
Monitor Name	Displays the name of the SiteScope monitor that was run on the suspect CI.

Correlated Events Pane

Description	Lists the EMS events that are correlated to the selected anomaly's start time.
Important Information	➤ Events are displayed for the time period starting from a configured number of minutes prior to the anomaly start time and ending 30 minutes after the anomaly start time. The number of minutes prior to the anomaly start time is the same as the number of minutes for events correlated to problems, as configured in the Infrastructure Settings page. For details on how to configure this setting, see the description of the **Distance** element in the "Correlated Events for Suspect CI Page" on page 28. ➤ In the same area of the page, you can display either the Correlated Events pane or the Correlation Measurements pane by clicking the appropriate tab. For details on the Correlation Measurements pane, see "Correlation Measurements Pane" on page 143.

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
	Hide/Show button. Toggle between showing and hiding the **Correlated Events** pane.
	Correlated Events button. Place your cursor on this button to temporarily display the **Correlated Events** pane when it is hidden. **Note:** This button is only displayed when the Correlated Events pane is hidden.
CI Name	The name of the CI on which the event occurred.
CI Type	The CI type of the CI on which the event occurred.

GUI Element (A-Z)	Description
Correlation Measurements	Click the **Correlation Measurements** tab at the bottom of the pane to view a table of the measurements returned by SiteScope monitors run on the CIs suspected of causing an anomaly, that are most correlated to the transaction or page displayed in the main proactive analysis graph. For details on the user interface, see "Correlation Measurements Pane" on page 143.
Description	The description of the event.
Distance	The distance, in minutes, from the anomaly start time at which the event occurred.
Event Source	The name of the source EMS from which the event was received.
Score	The event correlation percentage value as calculated by Problem Isolation.
Severity	The severity of the event. **Customization:** By default, correlation scores are calculated for events with all levels of severity (from 0–5). To modify the severity level for which event correlation scores are calculated, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the **Minimum severity of the correlation events** entry in the **Events Correlation** table. Modify the value to the severity level for which correlation scores are calculated for events. **Note:** ➤ Events with a severity less than the configured level are displayed with a correlation score of 0. ➤ Problem Isolation only recognizes events with a severity level from 0–5. ➤ Events with a severity level of 0 (unknown) are displayed with a correlation score of 0.

GUI Element (A-Z)	Description
Status	The event status. **Customization:** By default, correlation scores are calculated for events with any status. You can configure Problem Isolation not to calculate correlation scores for events that have been acknowledged or closed in the EMS before the problem start time. To do this, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the **Ignore acknowledged and closed events** entry in the **Events Correlation** table. Modify the value to **true**. **Note:** When you change this setting to true, acknowledged and closed events are displayed with a correlation score of 0.
Time	The date and time at which the event occurred.

Part III

Reports

3

Problem Isolation Reports

This chapter includes the main concepts and reference information for Problem Isolation reports.

This chapter includes:

Concepts

➤ Problem Isolation Reports Overview on page 151

Reference

➤ Problem Isolation Reports User Interface on page 152

Problem Isolation Reports Overview

Problem Isolation includes application anomaly reports that enable you to see general information about an application's anomalies for a selected time range, as well as the change in an application's anomalies between two similar time periods.

The available reports are:

- **Application Anomaly Summary report.** This report enables you to see the number of anomalies for selected applications in a selected time range, as well as the average duration of the anomalies and the number of affected users. For details on the user interface, see "Application Anomaly Summary Report" on page 153.
- **Application Anomaly Trend report.** This report enables you to detect trends in an application's anomalies (such as changes in the number of anomalies and their duration) between two similar time periods. For details on the user interface, see "Application Anomaly Trend Report" on page 156.

You access the Problem Isolation reports by selecting **Applications** > **Problem Isolation** > **Reports** tab.

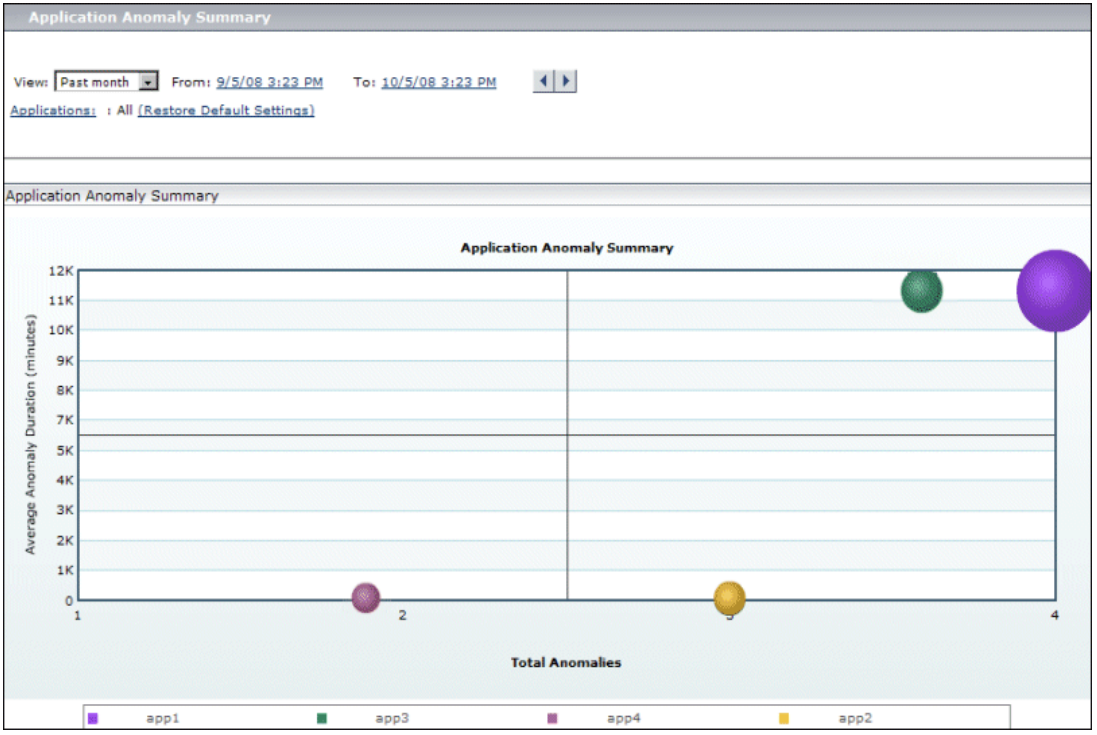
Problem Isolation Reports User Interface

This section includes (in alphabetical order):

- Application Anomaly Summary Report on page 153
- Application Anomaly Trend Report on page 156
- Applications Dialog Box on page 160

Application Anomaly Summary Report

The following is an example of the Application Anomaly Summary report.



Description	Displays the number of anomalies for selected applications in a selected time range, as well as the average duration of the anomalies and the average number of affected users. **To access:** Select **Applications** > **Problem Isolation** > **Reports** tab > **Application Anomaly Summary**
Important Information	You can set a favorite filter for the report and include it as a scheduled report. For details on how to perform this task, see "Create a Schedule" in *Reports*.
Useful Links	"Proactive Analysis Overview" on page 118 "Application Anomaly Trend Report" on page 156

Report Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<Common report elements>	For details on the user interface, see "Common Report Elements" in *Reports*.
Applications	Indicates which applications are selected for the report. To select applications, click the **Applications** link. The **Applications** dialog box opens in a new window. For details on the user interface, see "Applications Dialog Box" on page 160. **Default value:** All applications are selected.
Restore Default Settings	Click to restore the default setting in which all applications are selected for the report.

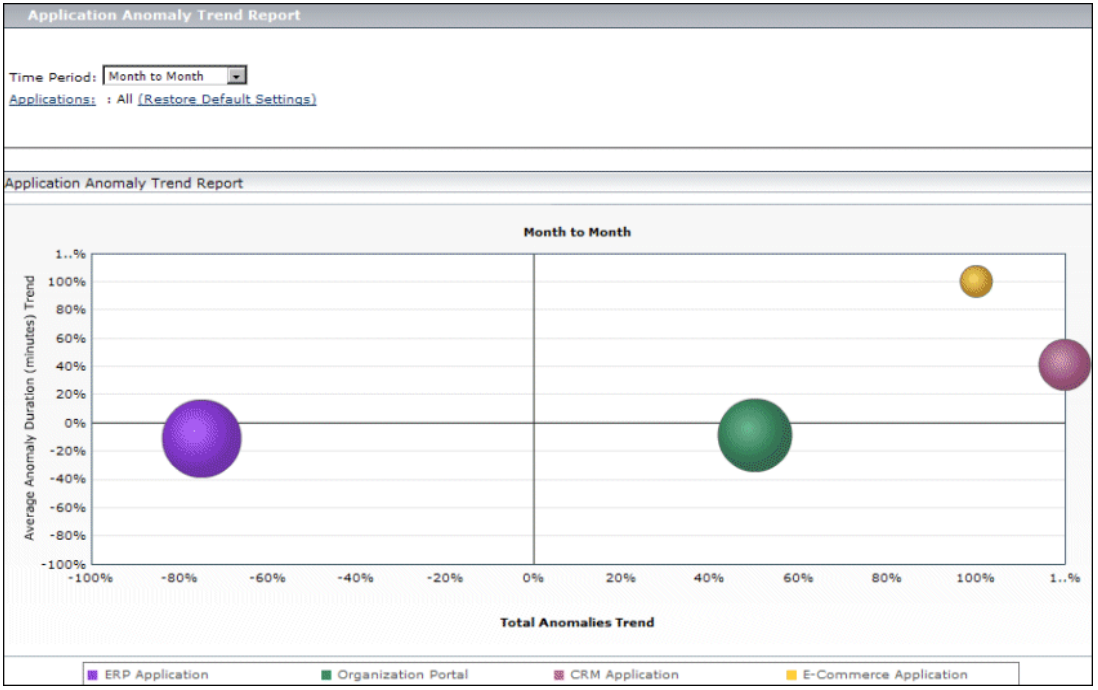
Report Content

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<Average anomaly duration midpoint line>	A horizontal, black line indicating the midpoint of the average anomaly duration axis (the y-axis). This enables you to see at a glance, which of the colored circles are higher than the midpoint, and which are lower.
<Colored circles>	Indicate the average anomaly duration, in minutes, for an application's problems within the selected time range for the report, as well as the total number of anomalies for an application within the time range. Each application is denoted by a different colored circle and the size of the circle depends on the average number of users impacted by the application's anomalies (the higher the number of users that are impacted, the larger the circle). **Tooltip:** The application name, the average anomaly duration time, the number of anomalies, and the average number of users impacted.
<Legend>	Describes the color coding used in the report.
<Total anomalies midpoint line>	A vertical, black line indicating the midpoint of the total anomalies axis (the x-axis). This enables you to see at a glance, which of the colored circles are higher than the midpoint, and which are lower.
Average Anomaly Duration (minutes) (y-axis)	The average anomaly duration, in minutes, of an application's anomalies within the report's time range.
Total Anomalies (x-axis)	The total number of anomalies for an application within the report's time range.

Application Anomaly Trend Report

The following is an example of the Application Anomaly Trend report.



Description	Displays the percentage change in the average number of anomalies, the average anomaly duration time, and the average number of affected users for selected applications between two similar time periods (that is, the last week, month, or quarter compared to the previous week, month, or quarter). This enables you to detect trends in an application's anomalies (such as more or less anomalies, and longer or shorter anomalies) over time. **To access:** Select **Applications** > **Problem Isolation** > **Reports** tab > **Application Anomaly Trend Report**

Important Information	You can set a favorite filter for the report and include it as a scheduled report. For details on how to perform this task, see "Create a Schedule" in *Reports*.
Useful Links	"Proactive Analysis Overview" on page 118 "Application Anomaly Summary Report" on page 153

Report Settings

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<Common report elements>	For details on the user interface, see "Common Report Elements" in *Reports*.
Applications	Indicates which applications are selected for the report. To select applications, click the **Applications** link. The **Applications** dialog box opens in a new window. For details on the user interface, see "Applications Dialog Box" on page 160. **Default value:** All applications are selected.

GUI Element (A-Z)	Description
Restore Default Settings	Click to restore the default setting in which all applications are selected for the report.
Time Period	Select the time period for comparison from the drop-down list. You can select **week to week**, **month to month**, or **quarter to quarter**. The comparison is made between the last complete, selected time period and the previous same time period. For example, if you select **week to week**, the comparison is made between the last full week and the week before it. By default, Business Availability Center takes Monday as the first day of the week, the 1st. as the first day of the month, and January as the first month of the first quarter. To modify these settings, select **Admin** > **Platform** > **Setup and Maintenance** > **Infrastructure Settings**, choose **Foundations**, select **Calendar**, and modify the required setting in the **Calendar Options** table. **Note:** If you change the default calendar settings, you must recalculate service level agreements. For details on this topic, see "Recalculation for Agreements" in *Using Service Level Management*.

Report Content

The following elements are included (unlabeled GUI elements are shown in angle brackets):

GUI Element (A-Z)	Description
<Average anomaly duration time change line>	A horizontal, black line indicating the zero change mark. This enables you to see at a glance which applications have a longer average duration time this period compared to the previous period, and which have a shorter time.
<Colored circles>	Each colored circle represents an application and indicates the percentage changes in the average anomaly duration time and the total number of anomalies between the current selected time period and the previous, same period. The size of the circle depends on the percentage change in the number of users impacted by the application's anomalies (the worse the change, the larger the circle). **Tooltip:** The application name, the average anomaly duration trend, the number of anomalies trend, and the average number of impacted users trend.
<Legend>	Describes the color coding used in the report.
<Total anomalies change line>	A vertical, black line indicating the zero change mark. This enables you to see at a glance which applications have more anomalies this period compared to the previous period, and which have less.

GUI Element (A-Z)	Description
Average Anomaly Duration (minutes) Trend (y-axis)	The percentage change in the average anomaly duration time, in minutes, of an application's anomalies for the selected time period, compared to the previous, same time period. **Note:** The axis ranges from -100% to +100%, with points labelled at 20% intervals, as well as one additional point labelled 1..% for all values that are greater than 100%.
Total Anomalies Trend (x-axis)	The percentage change in the total number of anomalies for an application for the selected time period, compared to the previous, same time period. **Note:** The axis ranges from -100% to +100%, with points labelled at 20% intervals, as well as one additional point labelled 1..% for all values that are greater than 100%.

Applications Dialog Box

Description	Enables you to select which applications you want to include in the Application Anomaly Summary and Application Anomaly Trend reports, from those applications configured for Proactive Analysis. Select the check box next to each application you want to include in the report, or clear the check box to exclude an application. **To access:** Click the **Applications** link in the report settings area of the Application Anomaly Summary report or Application Anomaly Trend report.
Important Information	By default, all applications are selected for the Application Anomaly Summary report.
Useful Links	"Application Anomaly Summary Report" on page 153 "Application Anomaly Trend Report" on page 156 "Proactive Analysis Configuration Page" on page 125

Index

A

anomaly menu options 124
Application Anomaly Summary report 153
Application Anomaly Trend report 156
Applications dialog box 160

C

Configure Monitor Parameters page 96
Correlated Events for Suspect CI page 28
Correlation graph 31

E

Edit Monitor Profile page 35
expected transaction behavior
    configure 123
    Problem Isolation proactive analysis 120

I

Impact page 37
Initial Analysis page 41
integration
    Problem Isolation and HP Service Manager 16
Invoke Run Book page 50
isolate a problem 19
Isolation History page 54

L

Layer Analysis page 59

M

Monitor Profile Configuration page 73
monitors list 71

N

New Monitor Profile page 74

O

On-demand Monitor Details dialog box 76
On-demand Monitor Parameters dialog box 77
on-demand monitors 13
    list 72
    SQL scripts 26
    success ratio 16
On-demand Monitors Results pane 78

P

permissions
    Problem Isolation 16, 122
proactive analysis 118
    configure 122
    expected transaction behavior 120
    user interface 123
Proactive Analysis Configuration page 125
Proactive Analysis page 128
Problem Isolation
    configure expected transaction behavior 123
    configure proactive analysis 122
    deploy 17

deploy Sitescope Problem Isolation Content.zip file 22
expected transaction behavior 120
isolate a problem 19
modify default on-demand monitor TQLs 25
modify default suspect algorithms 25
modify default suspect CI weights 26
on-demand monitor SQL scripts 26
on-demand monitors 13
permissions 16, 122
proactive analysis 118
proactive analysis user interface 123
reactive analysis 12
reactive analysis user interface 27
reports 151
reports user interface 152
standard user interface elements 102
troubleshooting and limitations 110
Problem Isolation entry page from HP Service Manager 81
Problem Isolation Properties page 83
Problem Snapshot report 86

R

reactive analysis 12
user interface 27
reports
Problem Isolation 151
Run Book Parameters dialog box 90

S

Select Suspect CI Monitors page 95
Select Suspect CI Topology page 94
Sitescope Problem Isolation Content.zip file
deploy 22
SQL scripts
for Problem Isolation on-demand monitors 26
success ratio
on-demand monitors 16
Suspect CI Monitor Configuration page 91
Suspect CI Monitor Configuration wizard 93
suspect CIs
weighting 15
Suspects page 97

T

troubleshooting and limitations
Problem Isolation 110

U

user interface
proactive analysis 123
Problem Isolation reports 152
reactive analysis 27

V

Validation page 104

W

weighting
suspect CIs 15