

HP Business Availability Center

for the Windows and Solaris operating systems

Software Version: 7.50

Using Problem Isolation

Document Number: BACPRI7.50/01

Document Release Date: May 2008

Software Release Date: May 2008



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.

Third-Party Web Sites

HP provides links to external third-party Web sites to help you find supplemental information. Site content and availability may change without notice. HP makes no representations or warranties whatsoever as to site content or availability.

Copyright Notices

© Copyright 2005 - 2008 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

This manual's title page 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>

Support

You can visit the HP Software Support Web site at: **www.hp.com/go/hpsoftwaresupport**

HP Software online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support 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 find more information about access levels, go to:

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

To register for an HP Passport ID, go to:

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

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
Weighting and On-demand Monitors Success Ratio	14
Problem Isolation and HP ServiceCenter Integration.....	16
Permissions.....	18
Deploy Problem Isolation – Workflow.....	18
Isolate a Problem – Workflow	20
Deploy the sis_for_pi_v7_5.zip File	23
Configure Problem Isolation and HP ServiceCenter Integration.....	25
Modify Default Suspect Algorithms and On-demand Monitor TQLs	26
On-Demand Monitor SQL Scripts	27
Suspect CI Monitor Configuration Wizard.....	28
Reactive Analysis User Interface.....	29
Troubleshooting and Limitations	100

PART II: PROACTIVE ANALYSIS

Chapter 2: Problem Isolation Proactive Analysis	107
Proactive Analysis Overview	107
Permissions.....	109
Configure Proactive Analysis – Workflow.....	109
Proactive Analysis User Interface	110
Index.....	127

Table of Contents

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.

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
- ▶ Weighting and On-demand Monitors Success Ratio on page 14
- ▶ Problem Isolation and HP ServiceCenter Integration on page 16
- ▶ Permissions on page 18

Tasks

- ▶ Deploy Problem Isolation – Workflow on page 18
- ▶ Isolate a Problem – Workflow on page 20
- ▶ Deploy the sis_for_pi_v7_5.zip File on page 23
- ▶ Configure Problem Isolation and HP ServiceCenter Integration on page 25
- ▶ Modify Default Suspect Algorithms and On-demand Monitor TQLs on page 26

Reference

- ▶ On-Demand Monitor SQL Scripts on page 27
- ▶ Suspect CI Monitor Configuration Wizard on page 28
- ▶ Reactive Analysis User Interface on page 29

Troubleshooting and Limitations on page 100

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 107.

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 94.
- ▶ determine the impact of the problem on SLAs and users. For details on determining the impact of a problem, see “Impact Page” on page 36.
- ▶ 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 40.
- ▶ 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 53.
- ▶ list suspected CIs and view their correlation with the problematic CI. For details on the suspect CIs, see “Suspects Page” on page 88, and for details on correlation, see “Correlation Graph” on page 30.

For a suggested working order for isolating a problematic CI and finding its root cause, see “Isolate a Problem – Workflow” on page 20.

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 76. 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 48.

You can integrate Problem Isolation with HP ServiceCenter to link isolation data with HP ServiceCenter incident or problem data, to create a complete problem management lifecycle. For details on integrating Problem Isolation with HP ServiceCenter, see "Problem Isolation and HP ServiceCenter Integration" on page 16.

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 ServiceCenter 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 79.

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 "On-Demand Monitor SQL Scripts" on page 27.

For details on modifying standard correlation rules and TQLs, see "Modify Default Suspect Algorithms and On-demand Monitor TQLs" on page 26.

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 88).

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 “Validation Page” on page 94), 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.

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.

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 84. Changes to existing monitor definitions for suspect CIs in a topology are made using the “Suspect CI Monitor Configuration Page” on page 82.

Weighting and On-demand Monitors Success Ratio

The following calculations are used in determining the weighting of suspect CIs, and the success ratio of on-demand monitors:

Suspect CIs Weighting

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, *
 $(\log(1 + \text{the number of changes made on the suspect CI}) / \log(1 + \text{the number of changes made to the first of the other suspect CIs}) + \log(1 + \text{the number of changes made to the next of the other suspect CIs}) + \dots + \log(1 + \text{the number of changes made to the last of the other suspect CIs}))$

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)

Failed monitors are those represented by a red circle.

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
- On-demand monitors weight
- Monitors weight

On-demand Monitor Success Ratio

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, see “Edit Monitor Profile Page” on page 34 and “New Monitor Profile Page” on page 67.



Problem Isolation and HP ServiceCenter Integration

This section has been replaced by the similarly named section in the “Problem Isolation and HP Service Manager Integration” chapter in the SM_integration.pdf file distributed with the 7.53 Service Pack.

You can integrate Problem Isolation with HP ServiceCenter to link isolation data (from Problem Isolation) with incident or problem data (from HP ServiceCenter), to create a complete problem management lifecycle. To integrate the two applications, you must configure the connectivity settings between them. For details on configuring the integration in HP Business Availability Center, see “Configure Problem Isolation and HP ServiceCenter Integration” on page 25. For details on configuring the integration in HP ServiceCenter, see “Configure HP ServiceCenter for Integration with HP Business Availability Center” in *Solutions and Integrations*.

Note: You can also integrate Problem Isolation with HP Service Manager. All references to HP ServiceCenter in this section and in the relevant user interface pages are also applicable to HP Service Manager.

When Problem Isolation and HP ServiceCenter are integrated, you can do the following:

- ▶ When isolating a problematic CI in Problem Isolation, link the isolation details to an existing HP ServiceCenter incident or problem. For details, see “Isolation History Page” on page 48.
- ▶ When isolating a problematic CI in Problem Isolation, create a new HP ServiceCenter incident or problem and link the isolation details to it. For details, see “Isolation History Page” on page 48.
- ▶ In Problem Isolation, upload the Problem Snapshot report, which contains data about suspect CIs, on-demand monitor results, and changes for a problematic CI, to an HP ServiceCenter incident or problem. For details, see “Problem Snapshot Report” on page 79.
- ▶ View basic information from an HP ServiceCenter incident or problem in a problematic CI’s isolation properties. For details, see “Properties Pane” on page 52.
- ▶ From an HP ServiceCenter incident or problem, isolate a CI in Problem Isolation. For details, see “Problem Isolation Entry Page for HP ServiceCenter” on page 74.

Note:

- ▶ For details on working in HP ServiceCenter, see the HP ServiceCenter documentation.
 - ▶ You can collect performance and availability data from an existing HP ServiceCenter Server and view the data in HP Business Availability Center applications. For details, see “Understanding the HP ServiceCenter Integration” in *Solutions and Integrations*.
-

Permissions

You must have the Problem Isolation **Advanced User** or **Administrator** role to run on-demand monitors, revalidate transactions, and update problem properties. 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 permissions, see “Permissions Overview” in *Platform Administration*.

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 18
- “Model Applications” on page 19
- “Deploy the sis_for_pi_v7_5.zip File” on page 19
- “Configure the Problem Isolation On-demand Monitors” on page 19
- “Configure Problem Isolation and HP ServiceCenter Integration – Optional” on page 19
- “Configure Proactive Analysis” on page 19
- “Grant Permissions” on page 19
- “Results” on page 20

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 and Populate an Instance View” in *Model Management*.

3 Deploy the sis_for_pi_v7_5.zip File

Deploy the sis_for_pi_v7_5.zip file included in Problem Isolation to install the Problem Isolation monitors template and SQL scripts. For details, see “Deploy the sis_for_pi_v7_5.zip File” on page 23.

4 Configure the Problem Isolation On-demand Monitors

Add or change monitor settings to adapt the on-demand monitors for your needs. For details, see “Suspect CI Monitor Configuration Wizard” on page 28.

5 Configure Problem Isolation and HP ServiceCenter Integration – Optional

You can integrate Problem Isolation and HP ServiceCenter. For details, see “Configure Problem Isolation and HP ServiceCenter Integration” on page 25.

For an overview of Problem Isolation and HP ServiceCenter integration, see “Problem Isolation and HP ServiceCenter Integration” on page 16.

6 Configure Proactive Analysis

For details, see “Configure Proactive Analysis – Workflow” on page 108.

7 Grant Permissions

Grant permissions for users to run on-demand monitors, revalidate transactions, update problem properties, and configure Problem Isolation. For details, see “Permissions” on page 18.

8 Results

You are now able to use Problem Isolation for both reactive and proactive analysis.

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 21
- “Run an Initial Analysis” on page 21
- “Run a Layer Analysis” on page 21
- “View the Main Suspects Table” on page 22
- “Generate a Problem Snapshot Report” on page 22
- “Escalate the Problem” on page 22
- “View the Correlation Graph” on page 22
- “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 Validation page, see “Validation Page” on page 94.

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 validating a problem, see “Validation Page” on page 94.

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 determining the impact of a problematic CI, see “Impact Page” on page 36.

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 Initial Analysis, see “Initial Analysis Page” on page 40.

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 Layer Analysis, see “Layer Analysis Page” on page 53.

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 Suspects, see “Suspects Page” on page 88.

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 ServiceCenter 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 79.

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 the 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 correlation graph, see “Correlation Graph” on page 30.

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 updating the root cause details, see “Problem Isolation Properties Page” on page 76.

Deploy the sis_for_pi_v7_5.zip File

This task describes how to deploy the sis_for_pi_v7_5.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 27.

The sis_for_pi_v7_5.zip file is located in the Windows_Setup and Solaris_Setup directories on the HP Business Availability Center DVD.

To deploy the sis_for_pi_v7_5.zip file:

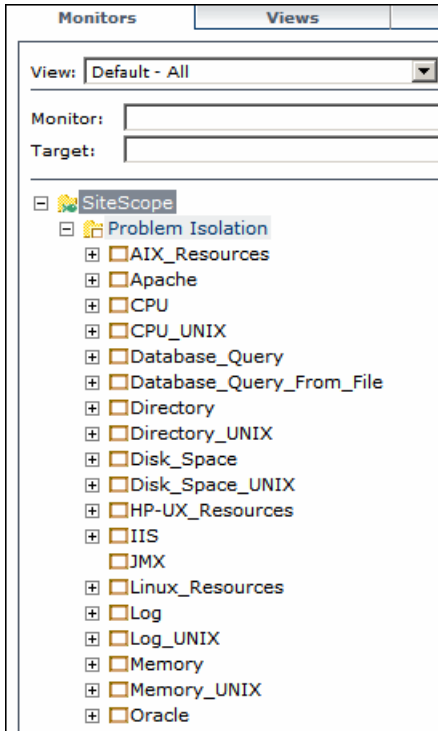
Extract the file content to the **SiteScope root directory** on each of the SiteScope machines in your system on which you plan to run Problem Isolation on-demand monitors. Make sure to use the folder names to keep the directory structure. Once the file is extracted, SiteScope automatically adds a template 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 Page” 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 sis_for_pi_v7_5.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.



Configure Problem Isolation and HP ServiceCenter Integration

This section has been replaced by the similarly named section in the "Problem Isolation and HP Service Manager Integration" chapter in the SM_integration.pdf file distributed with the 7.53 Service Pack.

This task describes how to configure HP Business Availability Center for the integration of HP ServiceCenter and Problem Isolation. For details on configuring the integration in HP ServiceCenter, see "Configure HP ServiceCenter for Integration with HP Business Availability Center" in *Solutions and Integrations*.

This task includes the following steps:

- ▶ "Configure Connection Settings" on page 25
- ▶ "Change the Default HP ServiceCenter Entity – Optional" on page 26
- ▶ "Federate HP Business Availability Center and HP ServiceCenter Data" on page 26

1 Configure Connection Settings

To configure the connection settings from Problem Isolation to HP ServiceCenter, select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, choose **Foundations**, select **Integrations with other applications**, and modify the values of the following entries in the **Problem Isolation-ServiceCenter Integration** table:

- ▶ **HP ServiceCenter UI endpoint URL.** The URL used to access the HP ServiceCenter Web server from Problem Isolation. Enter the URL in the format <http://<fully qualified server name>:<port>/SymphonyAdapter/ui>.
- ▶ **HP ServiceCenter Web services endpoint URL.** The URL used to access the HP ServiceCenter Web services from Problem Isolation. Enter the URL in the format <http://<fully qualified server name>:<port>/SymphonyAdapter/inbound/ws>.
- ▶ **HP ServiceCenter Web services timeout (milliseconds).** The connection timeout for HP ServiceCenter Web services.

2 Change the Default HP ServiceCenter Entity – Optional

The configured default entity determines the default title for displaying incident or problem details in the Properties page, as well as the default action when you click the **Associate** or **New** buttons on the page. For details on the Properties page, see “Problem Isolation Properties Page” on page 76.

To change the default HP ServiceCenter entity:

To modify the default HP ServiceCenter entity, select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the **Default ServiceCenter entity** entry in the **ServiceCenter** table. Modify the value to Incident or Problem.

3 Federate HP Business Availability Center and HP ServiceCenter Data

Use the HP ServiceCenter/Service Manager Adapter to federate Universal CMDB data with HP ServiceCenter CMDB data. For details on working with the HP ServiceCenter/Service Manager Adapter, see “The HP ServiceCenter/Service Manager Adapter” in *Model Management*.

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.

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 sis_for_pi_v7_5.zip File" on page 23.

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
Oracle Number of Open Sessions	PMOracleAmountOfSessions.sql
Oracle Tablespaces	PMOracleTablespaces.sql

Suspect CI Monitor Configuration Wizard

The link between SiteScope templates, TQLs, and Problem Isolation on-demand monitors is made using the Suspect CI Monitor Configuration Wizard. For details, see “Suspect CI Monitor Configuration Wizard” on page 84).

To create a new Suspect CI monitor, you start the Suspect CI Monitor Configuration Wizard by clicking **New Suspect CI Monitor Configuration** on the Suspect CI Monitor Configuration page. To edit an existing Suspect CI Monitor, you start the Suspect CI Monitor Configuration Wizard by clicking the **Edit** button for the applicable monitor configuration on the Suspect CI Monitor Configuration page. For details on the Suspect CI Monitor Configuration page, see “Suspect CI Monitor Configuration Page” on page 82.



The Suspect CI Monitor Configuration Wizard comprises the following pages:

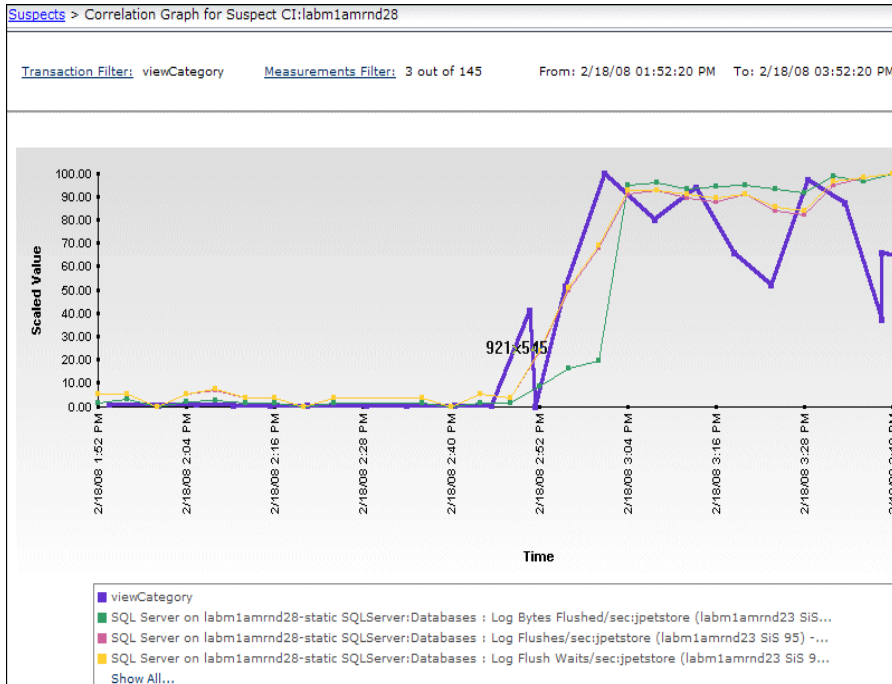
- ▶ **Welcome.** Explains the purpose of the wizard and describes the main steps. This page is not available when editing an existing suspect CI monitor configuration.
- ▶ **Select Suspect CI Topology.** Links the suspect CI type with a specific node in a selected topology. For details, see “Select Suspect CI Topology Page” on page 85.
- ▶ **Select Suspect CI Monitors.** Links specific monitors to be run on the suspect CI type in the selected topology. For details, see “Select Suspect CI Monitors Page” on page 86.
- ▶ **Define Monitor Parameters.** Maps monitor parameters to node attributes in the topology, and sets default values for them. For details, see “Configure Monitor Parameters Page” on page 87.
- ▶ **Summary.** Displays and saves the configured data. This page is not available when editing an existing suspect CI monitor configuration.

Reactive Analysis User Interface

This section describes:

- Correlation Graph on page 30
- Edit Monitor Profile Page on page 34
- Impact Page on page 36
- Initial Analysis Page on page 40
- Isolation History Page on page 48
- Layer Analysis Page on page 53
- List of Monitors on page 64
- List of On-demand Monitors on page 65
- Monitor Profile Configuration Page on page 66
- New Monitor Profile Page on page 67
- On-demand Monitor Details Dialog Box on page 68
- On-demand Monitor Parameters Dialog Box on page 69
- On-demand Monitors Results Pane on page 70
- Problem Isolation Entry Page for HP ServiceCenter on page 74
- Problem Isolation Properties Page on page 76
- Problem Snapshot Report on page 79
- Suspect CI Monitor Configuration Page on page 82
- Suspect CI Monitor Configuration Wizard on page 84
- Suspects Page on page 88
- Triage Steps - Standard User Interface Elements on page 91
- Validation Page on page 94

Correlation Graph



<p>Description</p>	<p>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.</p> <p>To access: Click the Correlation Score value for a suspect CI in the Suspects page.</p>
---------------------------	---

Important Information	<ul style="list-style-type: none"> ▶ 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 20

Graph Settings

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

<Common report settings>	For details, see “Common Report Elements” in <i>Reports</i> .
--------------------------	---

<p>Transaction Filter</p>	<p>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.</p> <p>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.</p>
<p>Measurements Filter</p>	<p>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.</p> <p>Default value: The first ten measurements in the list are selected.</p> <p>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.</p>

Graph Content

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

GUI Element (A–Z)	Description
<Bars>	<p>Show changes made to the selected suspect CI, over the time period for which the Correlation graph is displayed.</p> <p>Tooltip: The relevant time period from the first to the last change, the contained CI names and the number of changes for each one.</p>
<Legend>	Describes the color coding used in the graph.
<Thick line connecting data points>	<p>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.</p> <p>Tooltip: The transaction or page name, the monitor value, and the relevant time.</p>
<Thin lines connecting data points>	<p>Show the status of the selected measurements for the selected suspect CI, over the time period for which the Correlation graph is displayed.</p> <p>Tooltip: The measurement name, the measurement value, the monitored CI name, the correlation score, and the relevant time.</p>
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	<p>Enables you to edit existing monitor profiles for Problem Isolation on-demand monitors.</p> <p>The page comprises the Monitor Profile General Properties pane (for details, see page 34) and the SiteScope Template pane (for details, see page 35).</p> <p>To access: Click the Edit button for a specific monitor profile in the Monitor Profile Configuration page.</p>
Important Information	You create a new monitor profile on the New Monitor Profile page.

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	<p>Select the category to which the monitor belongs. Valid options are:</p> <ul style="list-style-type: none"> ▶ Connectivity ▶ Critical Services ▶ Health ▶ Other <p>Default value: Other</p>
Monitor Profile Name	<p>The name you choose for the new monitor profile.</p> <p>Note: This is a compulsory field and the name must be unique.</p>

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. 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 20
Useful Links	“Triage Steps - Standard User Interface Elements” on page 91

This section includes the following topics:

- “Impact Pane” on page 36
- “SLAs Impact Pane” on page 37
- “User Volume Pane” on page 38

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 on the message to display the impacted SLAs in the right pane.

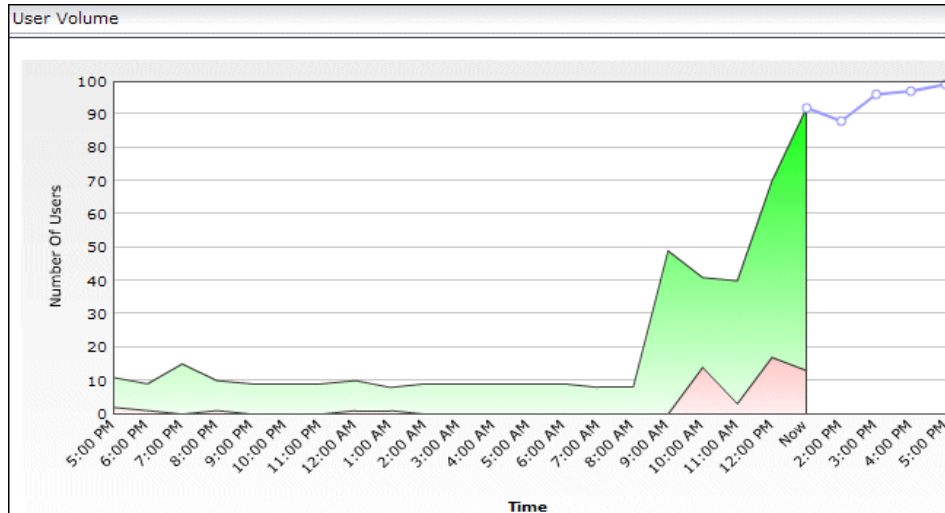
GUI Element (A–Z)	Description
Info - User Volume	<p>Displays the number of users currently using Real User Monitor applications associated with the problematic CI, and the number of users that are forecasted to use these applications in the next hour. Also displays the deviation for the number of forecasted users.</p> <p>Click on 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.</p>
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	<p>Displays the description, customer, and provider of the impacted SLA.</p> <p>Tooltip: Full SLA description.</p>
SLA Name	<p>Displays the name of the impacted SLA.</p> <p>Tooltip: Full SLA name.</p>
SLA Status	<p>The status shows a fuel gauge, indicating the worst status of the SLA for a specific period of time (day, week, month, or quarter). To the right of the speedometer, each time period is listed, and its worst status is displayed.</p> <p>Tooltip: Hold the cursor over the speedometer, or status icon, to display the status and the relevant time period.</p>

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: Hold the cursor over a data point to display 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: Hold the cursor on the top line of the shaded area, for a specific time, to display 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: Hold the cursor on the top line of the shaded area, for a specific time, to display 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

<p>Description</p>	<p>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:</p> <ul style="list-style-type: none"> ▶ 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. <p>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 left pane. The main display area includes one of the following panes:</p> <ul style="list-style-type: none"> ▶ Error Summary Pane (for details, see page 42). ▶ Error Over Time Pane (for details, see page 45). ▶ Event Summary Pane (for details see page 47). ▶ Problem Scope Pane (for details, see page 47). ▶ Problem Over Time Pane (for details see page 48). <p>To access:</p> <ul style="list-style-type: none"> ▶ 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.
<p>Included in Tasks</p>	<p>"Isolate a Problem – Workflow" on page 20</p>
<p>Useful Links</p>	<p>"Triage Steps - Standard User Interface Elements" on page 91</p>

Left 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 on the message to display the Error Summary Pane in the main display area (for details, see page 42).
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 47).
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 on the message to display the Problem Over Time Pane in the main display area (for details, see page 48).
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 on either message to display the Problem Scope Pane in the main display area (for details, see page 47).

GUI Element (A–Z)	Description
Info- Error Over Time	Click on 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 45).
Recommendation	Displays the recommended steps to take, to help solve the problem.

Error Summary Pane

Description	<p>The Error Summary pane displays one of the following:</p> <ul style="list-style-type: none"> ▶ Error Summary Report (for details, see page 42). The default view when the pane is first accessed. ▶ Error List (for details, see page 43). Accessed from the Virtual User (Business Process Monitor) Error Summary report.
Important Information	<p>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.</p>

Error Summary Report

Report Settings

<Common report settings>	For details, see “Common Report Elements” in <i>Reports</i> .
--------------------------	---

Report Content



Description	<p>The Error Summary report displays three pie charts, one each for:</p> <ul style="list-style-type: none"> ▶ HTTP errors ▶ application errors ▶ general errors <p>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.</p> <p>A legend at the bottom of each chart describes the color coding of the slices.</p> <p>Tooltip: Hold the cursor over a slice to display the error or event name and the number of occurrences of that error or event.</p>
Important Information	<p>Click on a slice to open the Error list for that error or event. For details, see "Error List" on page 43.</p>

Error List**Report Settings**

<Common report settings>	<p>For details, see "Common Report Elements" in <i>Reports</i>.</p>
--------------------------	---

Report Content

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

GUI Element (A-Z)	Description
	<p>Click to display a snapshot of the page on which the error occurred. For details on snapshots, see “Snapshot on Error” in End User Management.</p> <p>Note: This button is only enabled if a snapshot of the page exists.</p>
	<p>Click to open a zip file of a page’s snapshot. For details on snapshots, see “Snapshot on Error” in End User Management.</p> <p>Note: This button is only enabled if a zip file of the page’s snapshot exists.</p>
<p>Time</p>	<p>Displays the time that the error occurred.</p>

Error Over Time Pane

Description	<p>The Error Over Time pane displays one of the following:</p> <ul style="list-style-type: none"> ▶ Error Summary Report (for details, see page 42). The default view when the pane is first accessed. ▶ Error List (for details, see page 43). Accessed from the Virtual User (Business Process Monitor) Event Over Time report.
Important Information	<p>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.</p>

Report Settings

<Common report settings>	For details, see “Common Report Elements” in <i>Reports</i> .
--------------------------	---

Report Content

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

GUI Element (A-Z)	Description
<Lines connecting data points>	<p>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.</p> <p>Click on a data line to change the display to show the same graph, but for all the different error types included in that category.</p> <p>Click on a specific error type to display the Error list for that specific error. For details on the Error list, see “Error List” on page 43.</p> <p>Tooltip: Hold the cursor over a data point to display the number of errors for a category or type for a specific time.</p>
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	<p>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 End User Management.</p>
Important Information	<p>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.</p>

Problem Scope Pane

Description	<p>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 <i>Using End User Management</i>.</p>
Important Information	<ul style="list-style-type: none"> ▶ 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 <i>Using Dashboard</i> .
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.

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 ServiceCenter incident or problem, and open a new HP ServiceCenter incident or problem. Click a row in the table to select an isolation record. To access: Applications > Problem Isolation > Reactive Analysis
Important Information	An isolation record is added to isolation history when you access Problem Isolation from Dashboard or HP ServiceCenter for a problematic CI with a unique problem start time.

This section includes the following topics:

- “Isolation History Pane” on page 49
- “Properties Pane” on page 52

Isolation History Pane

Important Information	<ul style="list-style-type: none"> ➤ 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 settings>	For details, see “Common Report Elements” in <i>Reports</i> .
CI Name	Lists the names of problematic CIs that start with the string in the CI Name filter. Note: <ul style="list-style-type: none"> ➤ For details on working with the column filters, see “Important Information” on page 49. ➤ 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: <ul style="list-style-type: none"> ➤ For details on working with the column filters, see “Important Information” on page 49. ➤ This column is displayed by default.

GUI Element (A–Z)	Description
<p>Isolated By</p>	<p>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.</p> <p>Note:</p> <ul style="list-style-type: none"> ➤ For details on working with the column filters, see “Important Information” on page 49. ➤ This column is not displayed by default.
<p>Isolation Date</p>	<p>Lists the creation dates of the isolation record of problematic CIs that start with the string in the Isolation Date filter.</p> <p>Note:</p> <ul style="list-style-type: none"> ➤ For details on working with the column filters, see “Important Information” on page 49. ➤ This column is displayed by default.
<p>Isolation ID</p>	<p>Lists the internal problem isolation ID numbers of problematic CIs that start with the string in the Isolation ID filter.</p> <p>Note:</p> <ul style="list-style-type: none"> ➤ For details on working with the column filters, see “Important Information” on page 49. ➤ This column is not displayed by default.
<p>Problem Start Time</p>	<p>Lists the problem start date and time for problematic CIs that start with the string in the Problem Start Time filter.</p> <p>Note:</p> <ul style="list-style-type: none"> ➤ For details on working with the column filters, see “Important Information” on page 49. ➤ This column is not displayed by default.

GUI Element (A–Z)	Description
Root Cause CI Name	<p>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.</p> <p>Note:</p> <ul style="list-style-type: none"> ▶ For details on working with the column filters, see “Important Information” on page 49. ▶ This column is displayed by default.
Root Cause CI Type	<p>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.</p> <p>Note:</p> <ul style="list-style-type: none"> ▶ For details on working with the column filters, see “Important Information” on page 49. ▶ This column is not displayed by default.
Root Cause Description	<p>Lists the root cause description of problematic CIs, that start with the string in the Root Cause Description filter.</p> <p>Note:</p> <ul style="list-style-type: none"> ▶ For details on working with the column filters, see “Important Information” on page 49. ▶ This column is not displayed by default.
Root Cause Layer	<p>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.</p> <p>Note:</p> <ul style="list-style-type: none"> ▶ For details on working with the column filters, see “Important Information” on page 49. ▶ This column is not displayed by default.

GUI Element (A–Z)	Description
<p>Ticket ID</p>	<p>Lists the HP ServiceCenter 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 ServiceCenter login page in a new browser window. Enter a valid HP ServiceCenter user name and password. The HP ServiceCenter Update Incident or Problem Management page opens, where you can view and update the incident or problem. For details on working in HP ServiceCenter, see the HP ServiceCenter documentation.</p> <p>Note:</p> <ul style="list-style-type: none"> ▶ For details on working with the column filters, see “Important Information” on page 49. ▶ This column is displayed by default, if HP ServiceCenter is integrated with HP Business Availability Center. For details on integrating HP ServiceCenter with HP Business Availability Center, see “Configure Problem Isolation and HP ServiceCenter Integration” on page 25.
<p>Ticket Type</p>	<p>Lists the record types in HP ServiceCenter (incident or problem) with which isolation records are associated, that start with the string in the Ticket Type filter.</p> <p>Note:</p> <ul style="list-style-type: none"> ▶ For details on working with the column filters, see “Important Information” on page 49. ▶ This column is not displayed by default.
<p>Triage</p>	<p>Click the Triage button to go to the triage steps in Problem Isolation for a selected CI.</p> <p>Note: By default, the Problem Isolation Validation page opens. For details, see “Validation Page” on page 94</p>

Properties Pane

<p>Description</p>	<p>For details on the Properties pane, see “Problem Isolation Properties Page” on page 76.</p>
---------------------------	--

Layer Analysis Page

Description	<p>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 being investigated.</p> <p>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 left pane. The main display area includes one of the following panes:</p> <ul style="list-style-type: none"> ▶ Layer Deviation Analysis Pane (for details, see page 54) ▶ System Status Pane (for details, see page 57) ▶ Transactions Layer Breakdown Pane (for details, see page 63) <p>To access: Click the Layer Analysis option in the Problem Isolation flow bar on any Problem Isolation page.</p>
Included in Tasks	“Isolate a Problem – Workflow” on page 20
Useful Links	“Triage Steps - Standard User Interface Elements” on page 91

This section includes the following topics:

- ▶ “Left Pane” on page 54
- ▶ “Layer Deviation Analysis Pane” on page 54
- ▶ “System Status Pane” on page 57
- ▶ “Transactions Layer Breakdown Pane” on page 63

Left 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 on the message to display the Layer Deviation Analysis Pane in the main display area (for details, see page 54).
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 on the message to display the System Status Pane in the main display area (for details, see page 57).
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 on the message to display the Transactions Layer Breakdown Pane in the main display area (for details, see page 63).
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):

<Common report settings>	For details, see “Common Report Elements” in <i>Reports</i> .
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.

<p>Compare To</p>	<p>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.</p> <p>Default value: A period of 6 hours, starting from 27 hours prior to the time that the problem was opened, to 21 hours before the time that the problem was opened.</p> <p>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:</p> <ul style="list-style-type: none"> ▶ 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.
<p>Current</p>	<p>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.</p> <p>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.</p>

Content

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

GUI Element (A–Z)	Description
<Fuel gauge>	Each fuel gauge 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 fuel gauge. The fuel gauge 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 fuel gauge. The color shading in the fuel gauge 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 fuel gauge arrow is, the more problematic is the layer, especially when the arrow is in the red shaded area of the fuel gauge.

System Status Pane

Description	<p>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.</p> <p>From the System Status report, you can drill down to see a detailed list of the monitors for each category in the selected tier.</p>
-------------	---

The System Status pane displays the following reports:

- “System Status Report” on page 58
- “Category Status for a Tier Report” on page 60

System Status Report

Report Settings

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

<Common report settings>	For details, see “Common Report Elements” in <i>Reports</i> .
--------------------------	---

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
<p>Tiers <x-axis></p>	<p>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.</p> <p>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:</p> <ul style="list-style-type: none"> ▶ 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. <p>Click on a bar to display the Category Status for a Tier Report (for details, see page 60), showing the status of the suspect CIs included in each of the categories that comprise the tier.</p>

Category Status for a Tier Report

<p>Important Information</p>	<p>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.</p> <p>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:</p> <ul style="list-style-type: none"> ▶ 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):

<Common report settings>	For details, see “Common Report Elements” in <i>Reports</i> .
--------------------------	---

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	<p>Displays the number of discovered changes made to the suspect CI. Click the number of changes displayed to see the Changes report for the CI.</p> <p>For details on the Changes report, see “Change Report” in <i>Model Management</i>.</p>

GUI Element (A–Z)	Description
CI Name	<p>Displays the name of the suspect CI.</p> <p>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.</p>
CI Type	<p>Displays the CI type icon of the suspect CI.</p>
Connectivity	<p>Displays the weighted percentage of the failed on-demand monitors for the CI, in the Connectivity category of the tier.</p> <p>Each cell is color coded according to its weighted percentage, as described in the legend.</p> <p>Click the Connectivity category to see the List of On-demand Monitors for the category.</p> <p>Default value: The default color coding is:</p> <ul style="list-style-type: none"> ➤ Green. 0% ➤ Yellow. 1% - 30% ➤ Red. 31% - 100% <p>Tooltip: The weighted percentage of failed monitors, the number of failed monitors, and the total number of monitors run for the CI.</p>
Critical Services	<p>Displays the weighted percentage of the failed on-demand monitors for the CI, in the Critical Services category of the tier.</p> <p>Each cell is color coded according to its weighted percentage, as described in the legend.</p> <p>Click the Critical Services category to see the List of On-demand Monitors for the category.</p> <p>Default value: The default color coding is:</p> <ul style="list-style-type: none"> ➤ Green. 0% ➤ Yellow. 1% - 30% ➤ Red. 31% - 100% <p>Tooltip: The weighted percentage of failed monitors, the number of failed monitors, and the total number of monitors run for the CI.</p>

GUI Element (A-Z)	Description
Deployed Monitors	<p>Displays the number of failed monitors out of the total number of monitors deployed on the suspect CI in the selected tier.</p> <p>Click the number of monitors to see the List of Monitors.</p>
Health	<p>Displays the weighted percentage of the failed on-demand monitors for the CI, in the Health category of the tier.</p> <p>Each cell is color coded according to its weighted percentage, as described in the legend.</p> <p>Click the Health category to see the List of On-demand Monitors for the category.</p> <p>Default value: The default color coding is:</p> <ul style="list-style-type: none"> ➤ Green. 0% ➤ Yellow. 1% - 30% ➤ Red. 31% - 100% <p>Tooltip: The weighted percentage of failed monitors, the number of failed monitors, and the total number of monitors run for the CI.</p>
Miscellaneous	<p>Displays the weighted percentage of the failed on-demand monitors for the CI, in the Miscellaneous category of the tier.</p> <p>Each cell is color coded according to its weighted percentage, as described in the legend.</p> <p>Click the Miscellaneous category to see the List of On-demand Monitors for the category.</p> <p>Default value: The default color coding is:</p> <ul style="list-style-type: none"> ➤ Green. 0% ➤ Yellow. 1% - 30% ➤ Red. 31% - 100% <p>Tooltip: The weighted percentage of failed monitors, the number of failed monitors, and the total number of monitors run for the CI.</p>

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 <i>Using End User Management</i> .
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):

<Common report settings>	For details, see “Common Report Elements” in <i>Reports</i> .
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 <i>Using End User Management</i> .
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 <i>Using End User Management</i> .

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	<p>Displays the monitors for the suspect CI and its descendants.</p> <p>To access: Click the value displayed for problem monitors in the Current Status column on the Suspects page.</p>
--------------------	---

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	<p>The Dashboard status of the monitor that was run on the suspect CI.</p> <p>Tooltip: Status details.</p>
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 67.
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: <ul style="list-style-type: none"> ▶ 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 67.

Monitor Profile Configuration Page

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

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	<p>Displays the category to which the monitor belongs. Valid options are:</p> <ul style="list-style-type: none"> ▶ 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.
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	<p>The page for creating new monitor profiles for Problem Isolation on-demand monitors.</p> <p>The page comprises the Monitor Profile General Properties pane (for details, see page 67) and the SiteScope Template pane (for details, see page 68).</p> <p>To access: Click the New Monitor Profile button in the Monitor Profile Configuration page.</p>
Important Information	<p>You edit an existing monitor profile on the Edit Monitor Profile page.</p>

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	<p>The name you choose for the new monitor profile.</p> <p>Note: This is a compulsory field and the name must be unique.</p>
Monitor Category	<p>Select the category to which the monitor belongs.</p> <p>Valid options are:</p> <ul style="list-style-type: none"> ▶ Connectivity ▶ Critical Services ▶ Health ▶ Other <p>Default value: Other</p>

GUI Element (A–Z)	Description
Note	A free text field for any notes you want to associate with the monitor.
Weight	<p>The weight of the monitor to be used when calculating the success rate percentage of the monitor set.</p> <p>For details about monitor weights and success ratios, see “Weighting and On-demand Monitors Success Ratio” on page 14.</p> <p>Default Value: 1</p> <p>Note: The weight must be a positive integer between 0 and 100.</p>

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


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


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: <ul style="list-style-type: none"> ▶ 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.
Group by	<p>Select the filter by which to group the displayed monitors. Valid options are:</p> <ul style="list-style-type: none"> ▶ Monitor type ▶ Suspect CI ▶ Topology pattern <p>Default value:</p> <ul style="list-style-type: none"> ▶ 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. <p>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.</p>



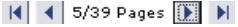
GUI Element (A-Z)	Description
<p>Monitor Type</p>	<p>Displays the on-demand monitors that run on the suspect CI. Each monitor is listed underneath the monitor type in a tree.</p> <p>Click a monitor to open the On-demand Monitor Parameters Dialog Box, where you can change the values of on-demand monitor parameters. For details on the On-demand Monitor Parameters dialog box, see “On-demand Monitor Parameters Dialog Box” on page 69.</p> <p>Tooltip: The CI type of the suspect CI on which the monitor runs, the topology pattern used by the monitor, and the monitor weight.</p> <p>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.</p>
<p>Run Monitors</p>	<p>Click the Run Monitors button to run the selected on-demand monitors.</p>

GUI Element (A-Z)	Description
Status	<p>Displays the status of the monitor.</p> <p>The valid statuses are:</p> <ul style="list-style-type: none"> ➤ 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. <p>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 68.</p> <p>Tooltip: The monitor run results.</p>
Suspect CI	<p>Displays the suspect CI and each monitor that runs on it.</p> <p>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 69.</p> <p>Tooltip: The suspect CI type, the topology pattern used by the monitor that runs on it, and the monitor weight.</p> <p>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.</p>

Problem Isolation Entry Page for HP ServiceCenter

<p>Description</p>	<p>Enables you to select and triage a CI from the HP Business Availability Center Universal CMDB when accessing Problem Isolation directly from HP ServiceCenter. When you select and triage a CI, a new isolation record is created.</p> <p>To access: See the HP ServiceCenter documentation.</p>
<p>Important Information</p>	<ul style="list-style-type: none"> ▶ 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
	<p>Click to reset the table columns' width to its 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.</p>
	<p>Click the Select Columns button to open the Select Columns dialog box and select the columns you want to be displayed on the table.</p>
	<p>Divides the table of data into pages. You move from page to page by clicking the relevant button:</p> <ul style="list-style-type: none"> ▶ 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	<p>Lists the CI Ids that start with the string in the CI Id filter.</p> <p>Note:</p> <ul style="list-style-type: none"> ▶ For details on working with the column filters, see “Important Information” on page 74. ▶ This column is not displayed by default.
CI Name	<p>Lists the CI names that start with the string in the CI Name filter.</p> <p>Note:</p> <ul style="list-style-type: none"> ▶ For details on working with the column filters, see “Important Information” on page 74. ▶ This column is displayed by default.
CI Type	<p>Lists the CI types that start with the string in the CI Type filter.</p> <p>Note:</p> <ul style="list-style-type: none"> ▶ For details on working with the column filters, see “Important Information” on page 74. ▶ This column is displayed by default.
Triage	<p>Click the Triage button to go to the triage steps in Problem Isolation for a selected CI.</p> <p>Note:</p> <ul style="list-style-type: none"> ▶ Click a row in the table to select a CI. ▶ By default, the Problem Isolation Impact page opens. For details, see “Impact Page” on page 36.

Problem Isolation Properties Page

<p>Description</p>	<p>Displays detailed information about the problematic CI currently selected in the Isolation History pane and enables you to update the information.</p> <p>To access:</p> <ul style="list-style-type: none"> ➤ 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
	<p>Refresh button. Click to refresh the incident or problem details displayed for the problematic CI.</p>
<p><Incident details></p>	<p>For isolation records that are associated with an HP ServiceCenter incident, lists the HP ServiceCenter ticket Id, title, status, severity and assigned operator. For details on HP ServiceCenter incidents, see the HP ServiceCenter documentation.</p> <p>Note:</p> <ul style="list-style-type: none"> ➤ This section of the pane is displayed only if HP ServiceCenter is integrated with HP Business Availability Center. ➤ You can set Incident details as the default display mode for unassociated isolation records. <p>For details on configuring HP ServiceCenter and HP Business Availability Center integration, see “Configure Problem Isolation and HP ServiceCenter Integration” on page 25.</p>

GUI Element (A–Z)	Description
<Problem details>	<p>For isolation records that are associated with an HP ServiceCenter problem, lists the HP ServiceCenter problem Id, title, status, and severity. For details on HP ServiceCenter problems, see the HP ServiceCenter documentation.</p> <p>Note:</p> <ul style="list-style-type: none"> ▶ This section of the pane is displayed only if HP ServiceCenter is integrated with HP Business Availability Center. ▶ You can set Problem details as the default display mode for unassociated isolation records. <p>For details on configuring HP ServiceCenter and HP Business Availability Center integration, see “Configure Problem Isolation and HP ServiceCenter Integration” on page 25.</p>
Associate	<p>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 ServiceCenter incident or problem. A login page for HP ServiceCenter opens where you enter your HP ServiceCenter login and password. For details on working with HP ServiceCenter, see the HP ServiceCenter documentation.</p> <p>Note: Click the Associate button directly to access HP ServiceCenter for the default action—associate an incident or associate a problem. For details on setting the default action, see “Configure Problem Isolation and HP ServiceCenter Integration” on page 25.</p>
CI	<p>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.</p>
CI name	<p>Displays the name of the problematic CI.</p>
CI Type	<p>Displays the CI type of the problematic CI.</p>

GUI Element (A–Z)	Description
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 root cause CI.
Detach	Click the Detach button to detach a problematic CI from an HP ServiceCenter 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	<p>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 ServiceCenter and associate it with the selected isolation record. A login page for HP ServiceCenter opens where you enter your HP ServiceCenter login and password. For details on working with HP ServiceCenter, see the HP ServiceCenter documentation.</p> <p>Note: Click the New button directly to access HP ServiceCenter for the default action—open a new incident or open a new problem. For details on setting the default action, see “Configure Problem Isolation and HP ServiceCenter Integration” on page 25.</p>
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	<p>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 ServiceCenter incident or problem.</p> <p>To access: Click the Snapshot Report button from any Problem Isolation triage step.</p>
Important Information	<p>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.</p>
Included in Tasks	<p>“Isolate a Problem – Workflow” on page 20</p>

This section includes the following topics:

- “Attach Problem Snapshot” on page 79
- “Summary” on page 80
- “Suspects Table” on page 81
- “On-demand Monitor Details” on page 81
- “Discovered Changes Details” on page 82

Attach Problem Snapshot

Description	<p>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 ServiceCenter incident or problem.</p> <p>Note: The Attach button is enabled only if HP Business Availability Center is integrated with HP ServiceCenter and an HP ServiceCenter incident or problem is already attached to the isolation record you are triaging.</p>
--------------------	---

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, see “Validation Page” on page 94.
Report generated by	The login name of the user who generated the report.
Report generated on	The date and time on which the report was generated.
User volume	<p>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, lists the following information:</p> <ul style="list-style-type: none"> ➤ 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. <p>Note: If more than one application is applicable, the values shown are the total values for all applicable applications.</p>

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 “Right Pane” on page 89. 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 67.
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.


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: Admin > Problem Isolation > On-demand Monitors
--------------------	--

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.
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

<p>Description</p>	<p>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.</p> <p>To access:</p> <ul style="list-style-type: none"> ➤ 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.
<p>Important Information</p>	<ul style="list-style-type: none"> ➤ When using the Suspect CI Monitor Configuration Wizard to edit a previously configured on-demand monitor: <ul style="list-style-type: none"> ➤ 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.
<p>Included in Tasks</p>	<p>“Deploy Problem Isolation – Workflow” on page 18</p>
<p>Wizard Map</p>	<p>The Suspect CI Monitor Configuration Wizard contains:</p> <p>Welcome page > Select Suspect CI Topology Page > Select Suspect CI Monitors Page > Configure Monitor Parameters Page > Summary</p>

Select Suspect CI Topology Page

Description	Page on which you configure the topology name and nodes, as well as the CI type, to be used by the monitors run on suspect CIs.
Wizard Map	<p>The Suspect CI Monitor Configuration Wizard contains:</p> <p>Welcome > Select Suspect CI Topology Page > Select Suspect CI Monitors Page > Configure Monitor Parameters Page > Summary</p> <p>Note: The Welcome and Summary pages are not included in the wizard when editing a previously configured on-demand monitor.</p>

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	Page on which you select the monitors to be run on a specific CI type, in a selected topology.
Important Information	<ul style="list-style-type: none"> ▶ 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	<p>The Suspect CI Monitor Configuration Wizard contains:</p> <p>Welcome > Select Suspect CI Topology Page > Select Suspect CI Monitors Page > Configure Monitor Parameters Page > Summary</p> <p>Note: The Welcome and Summary pages are not included in the wizard when editing a previously configured on-demand monitor.</p>

Configure Monitor Parameters Page

Description	Enables you to configure the parameters for the monitors run on suspect CIs.
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 67.
Wizard Map	<p>The Suspect CI Monitor Configuration Wizard contains:</p> <p>Welcome > Select Suspect CI Topology Page > Select Suspect CI Monitors Page > Configure Monitor Parameters Page > Summary</p> <p>Note: The Welcome and Summary pages are not included in the wizard when editing a previously configured on-demand monitor.</p>

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 20
Useful Links	“Triage Steps - Standard User Interface Elements” on page 91

This section includes the following topics:

- “Left Pane” on page 88
- “Right Pane” on page 89


Left 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 Right Pane.
Recommendation	Displays the recommended steps to take, to help solve the problem.

Right 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 suspect CIs.
CI Name	Displays the name of the suspect CI.
CI Type	Displays the CI type icon and name for the suspect CI.
Correlation Score	<p>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.</p> <p>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.</p> <p>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 30</p> <p>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.</p>

GUI Element (A–Z)	Description
<p>Deployed Monitors Current Status</p>	<p>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 on the value displayed to see the List of Monitors. For details on the List of Monitors, see “List of Monitors” on page 64.</p> <p>Tooltip: The number of problem monitors and the number of total monitors for the suspect CI.</p>
<p>Discovered Changes</p>	<p>Displays the number of changes made to the suspect CI and its descendant CIs. Click on the number of changes displayed to see the Changes report for the CI. For details on the Changes report, see “Change Report” in <i>Model Management</i>.</p> <p>Tooltip: The number of discovered changes and the time frame in which they were discovered.</p>
<p>On-demand Monitor Results</p>	<p>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 70.</p> <p>Tooltip: The number of failed on-demand monitors out of the total number of monitors run, and the calculated weighted score.</p>
<p>Weighted Score</p>	<p>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 “Weighting and On-demand Monitors Success Ratio” on page 14.</p> <p>Tooltip: The weight and score for each column of data for the suspect CI.</p>


Triage Steps - Standard User Interface Elements

Description	<p>The user interface for the triage steps used to isolate a problem has a standard layout and includes common elements in each step.</p> <p>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 48.</p>
Included in Tasks	“Isolate a Problem – Workflow” on page 20

This section includes the following topics:

- “Isolation Steps and Flow Bar” on page 91
- “Left Pane” on page 92
- “Right Pane” on page 92
- “Common User Interface Elements” on page 92

Isolation Steps and Flow Bar

Description	<p>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.</p> <p>Under the steps is a flow bar with an indicator  that shows you which isolation step is current.</p>
--------------------	---

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.

GUI Element	Description
<Breadcrumb>	<p>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 on a link in the path to return to that page.</p> <p>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.</p>
Snapshot Report	<p>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 79.</p>
On-demand Monitors	<p>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 70.</p>
Properties	<p>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 52.</p>

Validation Page

Description	<p>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.</p> <p>To access:</p> <ul style="list-style-type: none"> ➤ 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	<p>For important information, see “Notes and Limitations” on page 98.</p>
Included in Tasks	<p>“Isolate a Problem – Workflow” on page 20</p>
Useful Links	<p>“Triage Steps - Standard User Interface Elements” on page 91</p>

This section includes the following topics:

- “Left Pane” on page 95
- “Right Pane” on page 95
- “Notes and Limitations” on page 98

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 on 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	<p>The current status of the transaction, based on the thresholds configured for the transaction in End User Management Administration. The valid statuses are:</p> <ul style="list-style-type: none"> ➤  Idle. ➤ Pending. Selected and waiting to run ➤ Running. Currently running ➤  OK. Transaction ran successfully, with the measurement calculated for the KPI falling within the value range for the OK objective. ➤  Minor. Transaction ran successfully, with the measurement calculated for the KPI falling within the value range for the Minor objective. ➤  Critical. Transaction ran successfully, with the measurement calculated for the KPI falling within the value range for the Critical objective. ➤  Failed. Transaction did not run successfully. <p>Tooltip: A summary of the transaction's statuses during the relevant time period.</p>
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	<p>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:</p> <ul style="list-style-type: none"> ▶  OK. Transaction ran successfully, with the measurement calculated for the KPI falling within the value range for the OK objective. ▶  Minor. Transaction ran successfully, with the measurement calculated for the KPI falling within the value range for the Minor objective. ▶  Critical. Transaction ran successfully, with the measurement calculated for the KPI falling within the value range for the Critical objective. ▶  Failed. Transaction did not run successfully. <p>Tooltip: A summary of the transaction's statuses during the relevant time period.</p> <p>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.</p>
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	<p>Displays the trend of the change between the Open Status and the Current Status. The valid trend options are:</p> <ul style="list-style-type: none"> ➤  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. <p>Tooltip: The trend status.</p>

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 on 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 67.

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 69.

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 84.

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 84.

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 107
- ▶ Permissions on page 109

Tasks

- ▶ Configure Proactive Analysis – Workflow on page 109

Reference

- ▶ Proactive Analysis User Interface on page 110

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 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 looks for patterns and irregular behavior in the availability and response times of the transactions, and breaks down the day's data into a number of time segments. Similar sequential segments are combined. For example, three consecutive good segments (that is, without any problematic behavior), followed by two consecutive bad segments (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 availability problems, breaches in transaction thresholds, and significant changes in transaction response times without a breach in transaction thresholds. 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 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 that occurred in an anomaly's time range (by default, the transaction with the most severe anomaly, as calculated by the proactive analysis process, is displayed) and can see any discovered or planned changes, as well as incidents, that occurred in the same time range. The measurements returned by SiteScope monitors run on the CIs suspected of causing an anomaly, that are most correlated to the selected transaction, are also displayed and you can select the measurements you want to display together with the transaction data in the same graph. This enables you to see the correlation between the transaction data, the suspect CI measurements, changes (both discovered and planned), and incidents. For details on the Proactive Analysis page, see "Proactive Analysis Page" on page 114.

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 111.

Note: Before the proactive analysis process runs for the first time, you must re-aggregate Business Process Monitor data for six weeks back, and SiteScope data for one week back. Re-aggregating data for less than the specified periods results in less accurate proactive analysis data. For details on re-aggregating Business Process Monitor and SiteScope data, consult HP Software Support.

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 permissions, 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:

- “Re-aggregate Business Process Monitor and SiteScope Data” on page 110
- “Configure the Proactive Analysis Process” on page 110
- “Results” on page 110

1 Re-aggregate Business Process Monitor and SiteScope Data

Before the proactive analysis process runs for the first time, you must re-aggregate Business Process Monitor data for six weeks back, and SiteScope data for one week back. Re-aggregating data for less than the specified periods results in less accurate proactive analysis data. For details on re-aggregating Business Process Monitor and SiteScope data, consult HP Software Support.

2 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, see “Proactive Analysis Configuration Page” on page 111.

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, see “Proactive Analysis Page” on page 114.

Proactive Analysis User Interface



This section describes:

- Proactive Analysis Configuration Page on page 111
- Proactive Analysis Page on page 114

Proactive Analysis Configuration Page

Description	<p>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.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ Admin > Problem Isolation > Proactive Analysis ▶ Click the Configure Proactive Analysis button  in the Anomalies pane of the Proactive Analysis page.
Important Information	<ul style="list-style-type: none"> ▶ Before the proactive analysis process runs for the first time, you must re-aggregate Business Process Monitor data for six weeks back, and SiteScope data for one week back. Re-aggregating data for less than the specified periods results in less accurate proactive analysis data. For details on re-aggregating Business Process Monitor and SiteScope data, consult HP Software Support. ▶ 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 107

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>	<p>Displays the names and type of all the applications and business services available for proactive analysis. Click an application name to select it.</p> <p>Default value: CIs with the following CI types are displayed:</p> <ul style="list-style-type: none"> ▶ logical_application ▶ business_service_for_catalog ▶ sap_resource ▶ siebel_application ▶ websphere <p>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.</p>
<Right pane>	<p>Displays the names and type of all the applications already configured for proactive analysis. Click an application name to select it.</p>

GUI Element (A-Z)	Description
Run daily at	<p>Select the time (hours and minutes) that you want the proactive analysis process to run each day.</p> <p>Tip:</p> <ul style="list-style-type: none"> ▶ 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	<p>Enables you to view anomalies in the behavior of transactions for selected applications, as well as measurements that have a high correlation to the transaction behavior. Also shows incidents, planned changes, and discovered changes that may be related to the application.</p> <p>To access: Applications > Problem Isolation > Proactive Analysis</p>
Important Information	<ul style="list-style-type: none"> ▶ When transaction 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, and an hourly time breakdown is used, raw data is displayed. In all other instances, aggregated data is used. Aggregated data may not show the same results as raw data and may not reflect the actual data for a single anomaly. ▶ All references to HP ServiceCenter are also applicable to HP Service Manager.
Useful Links	<p>“Proactive Analysis Overview” on page 107</p>





This section includes the following topics:

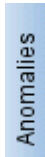





- ▶ “Anomalies Pane” on page 115
- ▶ “Proactive Analysis Graph Pane” on page 118
- ▶ “Correlation Measurements Pane” on page 124

Anomalies Pane

Description	<p>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.</p> <p>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.</p>
--------------------	---

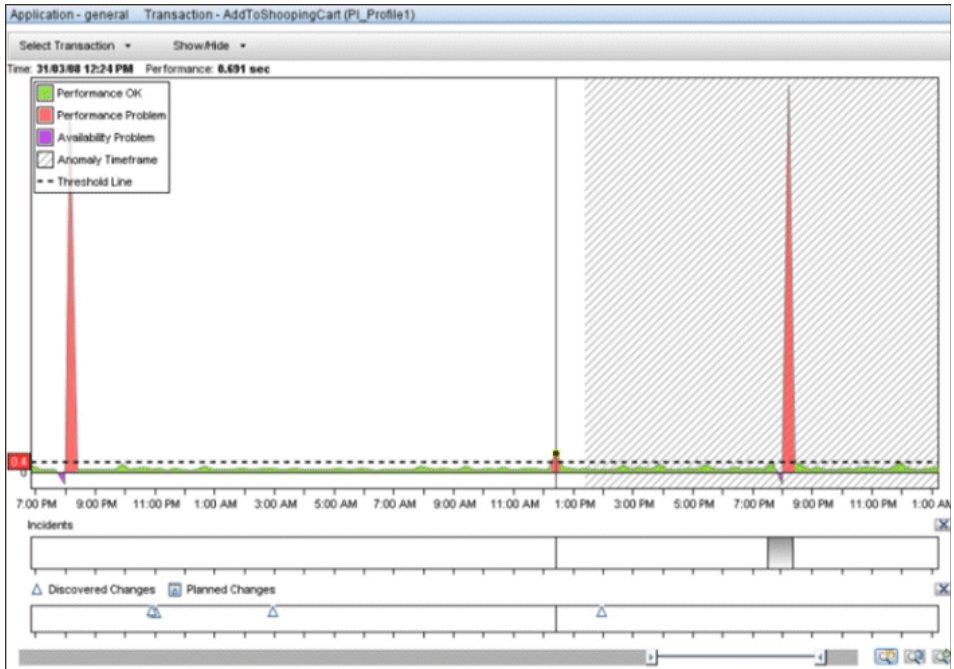
The following elements are included (unlabeled GUI elements are shown in angle brackets>):


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 111.

GUI Element (A-Z)	Description
	<p>Anomalies button. Place your cursor on this button to temporarily display the Anomalies pane when it is hidden.</p> <p>Note: This button is only displayed when the Anomalies pane is hidden.</p>
	<p>Availability Problems Anomaly icon. Indicates that an anomaly contains transactions with availability problems.</p>
	<p>Threshold Cross Anomaly icon. Indicates that an anomaly contains transactions that crossed their critical threshold.</p>
	<p>Increased Response Time Anomaly icon. Indicates that an anomaly contains transactions with a significant increase in their response time.</p>
	<p>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.</p>
	<p>Incidents icon. Indicates that there are HP ServiceCenter incidents during the anomaly time period.</p>
<p><Anomalies></p>	<p>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.</p> <p>Tooltip: The application name, anomaly date range, anomaly type icons and descriptions, and the number of incidents and changes.</p>
<p>Anomaly Type</p>	<p>Select the anomaly type by which to filter the displayed anomalies. Select None to display all anomaly types.</p>




GUI Element (A-Z)	Description
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.
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 ServiceCenter 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





Description	Enables you to view the response times of a transaction during a period of time identified as an anomaly for an application. You can also view incidents , planned changes, 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, enabling you to correlate the data visually.
Important Information	<p>You can change the time range or zoom of the graph by using the following methods:</p> <ul style="list-style-type: none"> ▶ 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 the transaction included in the graph. To the left of the line, a small, red square displays the number of seconds configured as the critical transaction time threshold.
	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.

GUI Element (A-Z)	Description
	<p>Reset Zoom button. Click to display the graph with the original time range used.</p>
	<p>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.</p> <p>Tooltip: The number of discovered changes for the given point of time.</p>
	<p>Planned Changes icon. Indicates that there are planned changes in HP ServiceCenter at a given point of time. Click the icon to display details of the planned changes in a new window.</p> <p>Tooltip: The number of planned changes for the given point of time.</p>
	<p>Time Scroll bar. Click on 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.</p> <p>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.</p> <p>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.</p> <p>Note: As the length of the time range changes, the time units displayed may change between hours, days, and weeks to accommodate the relevant data.</p>
	<p>Located above the Incidents and Changes graphs, click to hide the relevant graph. Use the Show/Hide option to show the graphs again.</p>

GUI Element (A-Z)	Description
<Changes>	<p>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 planned changes (RFCs)  in HP ServiceCenter. Click a change icon to display details of the changes in a new window.</p> <p>Tooltip: The number of changes for the applicable date and time.</p> <p>Note:</p> <ul style="list-style-type: none"> ▶ The Changes graph uses the same time range as the main proactive analysis graph. ▶ Planned and discovered changes data is aggregated hourly or daily, depending on the graph's time range. Raw data is not displayed. ▶ Changes might be displayed in the Changes graph, even though no changes are indicated for the anomaly in the Anomaly pane. Changes are displayed for the entire time range of the Changes graph, although the change icon is only displayed in the Anomaly 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.
<Colored blocked areas>	<p>Indicate the OK (green), performance problem (red) and availability problem (purple) statuses of the transaction included in the graph, during the graph's time range. The anomaly timeframe area is denoted by diagonal gray lines.</p>


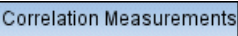
GUI Element (A-Z)	Description
<p><Date and response time indicator> (vertical black line)</p>	<p>A vertical black line appears on the graph when you place the cursor on the main area of the graph. This line indicates a specific date and time in the graph's time range, and a small black square on the line shows the data point in the graph for the relevant transaction response time. Move the cursor to the left or right to move the line to a different date and time in the graph. The date and time, as well as the transaction response time value indicated by the line are displayed at the top of the graph.</p>
<p><Legend></p>	<p>Describes the color coding used in the graph. The legend is displayed by default. You can use the Show/Hide option to toggle between displaying and hiding the legend.</p>
<p><Thin colored lines connecting data points></p>	<p>Display the values of the correlation measurements you select in the Correlation Measurements pane to include in the graph.</p>
<p><Time> (x-axis)</p>	<p>Displays the time division units applicable for the graphs's time range.</p>
<p>Incidents</p>	<p>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 ServiceCenter. 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.</p> <p>Tooltip: The number of incidents in HP ServiceCenter for the applicable date and time.</p> <p>Note:</p> <ul style="list-style-type: none"> ➤ 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. Raw data is not displayed.

GUI Element (A-Z)	Description
Performance	Located above the graph, displays the transaction response time indicated by the vertical black line.
Select Transaction	<p>Click Select Transaction to display a list of an application's transactions that showed anomalous behavior during the anomaly's time range (that is, had availability problems, crossed thresholds, or had an increase in response time). The transactions are sorted in descending order according to the extent of their anomaly and also show their location and anomalies. Click a transaction name in the list to display the Proactive Analysis graph for that transaction and to change the Correlation Measurement list to the measurements with the highest correlation to that transaction during the anomaly time period.</p> <p>Default value: The most anomalous transaction during the anomaly's time range.</p>
Show/Hide	Click Show/Hide to display a list of the additional graphs included in the Proactive Analysis Graph pane— Changes and Incidents . Click a graph name to select it for display, or if already selected, click the name to hide the graph. Selected graphs are denoted by a tick in front of the name. You also use the Show/Hide option to display or hide the graph's legend.
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 displayed in the main proactive analysis graph. You can select measurements to be included in the main proactive analysis graph.
Important Information	By default, the measurements are displayed in descending order, according to their correlation to the transaction 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.

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. Select the check box in the header row to include all the measurements 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.
Correlation (%)	Displays the correlation percentage of the measurement to the selected transaction.

GUI Element (A-Z)	Description
Correlation Measurements	Place your cursor on the Correlation Measurements 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.
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.

Index

C

Configure Monitor Parameters page 87
Correlation graph 30

E

Edit Monitor Profile page 34

I

Impact page 36
Initial Analysis page 40
isolate a problem 20
Isolation History page 48

L

Layer Analysis page 53

M

Monitor Profile Configuration page 66
monitors list 64

N

New Monitor Profile page 67

O

On-demand Monitor Details dialog box 68
On-demand Monitor Parameters dialog box 69
on-demand monitors 13
 list 65
 SQL scripts 27
 success ratio 14
On-demand Monitors Results pane 70

P

permissions
 Problem Isolation 18, 109
proactive analysis 107
 configure 109
 user interface 110
Proactive Analysis Configuration page 111
Proactive Analysis page 114
Problem Isolation
 configure proactive analysis 109
 configure ServiceCenter integration 25
 deploy 18
 deploy sis_for_pi_v7_0.zip file 23
 isolate a problem 20
 modify default on-demand monitor TQLs 26
 modify default suspect algorithms 26
 on-demand monitor SQL scripts 27
 on-demand monitors 13
 permissions 18, 109
 proactive analysis 107
 proactive analysis user interface 110
 reactive analysis 12
 reactive analysis user interface 29
 ServiceCenter integration 16
 standard user interface elements 91
 troubleshooting and limitations 100
Problem Isolation entry page from HP Service Center 74
Problem Isolation Properties page 76
Problem Snapshot report 79

R

reactive analysis 12
 user interface 29

Index

S

- Select Suspect CI Monitors page 86
- Select Suspect CI Topology page 85
- ServiceCenter
 - Problem Isolation integration 16
- sis_for_pi_v7_0.zip file
 - deploy 23
- SQL scripts
 - for Problem Isolation on-demand monitors 27
- success ratio
 - on-demand monitors 14
- Suspect CI Monitor Configuration page 82
- Suspect CI Monitor Configuration wizard 28, 84
- suspect CIs
 - weighting 14
- Suspects page 88

T

- troubleshooting and limitations
 - Problem Isolation 100

U

- user interface
 - proactive analysis 110
 - reactive analysis 29

V

- Validation page 94

W

- weighting
 - suspect CIs 14