

HP Business Availability Center

for the Windows and Solaris operating systems

Software Version: 7.0

Using Problem Isolation

Document Number: BACPRI7.0/01

Document Release Date: September 2007

Software Release Date: August 2007



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 - 2007 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://ovweb.external.hp.com/lpe/doc_serv/

Support

Mercury Product Support

You can obtain support information for products formerly produced by Mercury as follows:

- If you work with an HP Software Services Integrator (SVI) partner (**http://h20230.www2.hp.com/svi_partner_list.jsp**), contact your SVI agent.
- If you have an active HP Software support contract, visit the HP Software Support Web site and use the Self-Solve Knowledge Search to find answers to technical questions.
- For the latest information about support processes and tools available for products formerly produced by Mercury, we encourage you to visit the Mercury Customer Support Web site at: **<http://support.mercury.com>**.
- If you have additional questions, contact your HP Sales Representative.

HP Software 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: PROBLEM ISOLATION

Chapter 1: Problem Isolation	11
Introduction to Problem Isolation	12
The Problem Lifecycle	14
On-demand Monitors.....	15
Calculating the Business Impact of a Problem CI.....	16
Weighting and On-demand Monitors Success Ratio	17
Deploy Problem Isolation.....	19
Manage a Problem	21
Isolate a Problem	22
Problem Isolation Standard User Interface Elements	24
Deploying the sis_for_pi_v7_0.zip File.....	26
Prerequisites.....	27
Suspect CI Monitor Configuration Wizard.....	27
Changing the Default Number of Hosts on Which a Script is Revalidated	28
Changing the Default Transactions Status for Automatic Revalidation	29
Configuring the Link to HP ServiceCenter Software	29
Disabling Automatic Transaction Revalidation	30
Modifying the BPM Triage Report's Default Time Period.....	30
Modifying the Error Summary Report's Default Time Period.....	30
Modifying the Event Over Time Report's Default Time Period.....	31
Modifying the KPI Over Time Report's Default Time Period	31
Modifying a Default Suspect Algorithm.....	32
Modifying a Default On-demand Monitor TQL	32
Troubleshooting and Limitations	33

PART II: USER INTERFACE

Chapter 2: Problem Isolation User Interface 39

Correlation Graph 40

Edit Monitor Profile Page 43

Impact Page 45

Initial Analysis Page 47

Layer Analysis Page 53

List of Monitors 63

List of On-demand Monitors 64

Monitor Profile Configuration Page..... 65

New Monitor Profile Page 67

On-demand Monitor Details Dialog Box 69

On-demand Monitor Parameters Dialog Box 70

On-demand Monitors Results Pane 71

Problem List..... 75

Suspect CI Monitor Configuration Page 79

Suspect CI Monitor Configuration Wizard..... 81

Suspects Page 85

System CI Summary Report..... 89

Validation Page..... 90

Index 97

Welcome to This Guide

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

This chapter describes:	On page:
How This Guide Is Organized	7
Who Should Read This Guide	8
Getting More Information	8

How This Guide Is Organized

The guide contains the following parts:

Part I Problem Isolation

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

Part II User Interface

Describes the pages and dialog boxes that are part of the Problem Isolation user interface.

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

Problem Isolation

1

Problem Isolation

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

This chapter describes:	On page:
Concepts	
Introduction to Problem Isolation	12
The Problem Lifecycle	14
On-demand Monitors	15
Calculating the Business Impact of a Problem CI	16
Weighting and On-demand Monitors Success Ratio	17
Tasks	
Deploy Problem Isolation	19
Manage a Problem	21
Isolate a Problem	22
General Reference	
Problem Isolation Standard User Interface Elements	24
Deploying the sis_for_pi_v7_0.zip File	26
Prerequisites	27
Suspect CI Monitor Configuration Wizard	27

This chapter describes:	On page:
Customization	
Changing the Default Number of Hosts on Which a Script is Revalidated	28
Changing the Default Transactions Status for Automatic Revalidation	29
Configuring the Link to HP ServiceCenter Software	29
Disabling Automatic Transaction Revalidation	30
Modifying the BPM Triage Report's Default Time Period	30
Modifying the Error Summary Report's Default Time Period	30
Modifying the Event Over Time Report's Default Time Period	31
Modifying the KPI Over Time Report's Default Time Period	31
Modifying a Default Suspect Algorithm	32
Modifying a Default On-demand Monitor TQL	32
Troubleshooting and Limitations	33

Introduction to Problem Isolation

Problem Isolation enables you to isolate and manage 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. For details on opening a problem, see “Manage a Problem” on page 21.

The Problem Isolation module consists of two main areas:

- ▶ **Problem List.** Used for managing a problem within HP Business Availability Center. Once a new problem has been created, you use the Problem list to enter information about the problem, update the information throughout the problem's life, and close the problem once it has been corrected. For details on managing a problem, see "Manage a Problem" on page 21.
- ▶ **Problem Isolation.** Used to determine the scope and impact of the problem, and to enable locating the root cause of the problem. To isolate a problem, you can:
 - ▶ revalidate the problem to see if it is still actual, or if its status has changed.
 - ▶ determine the impact of the problem on SLAs.
 - ▶ 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.
 - ▶ 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.
 - ▶ list suspected CIs and view their correlation with the problem CI.

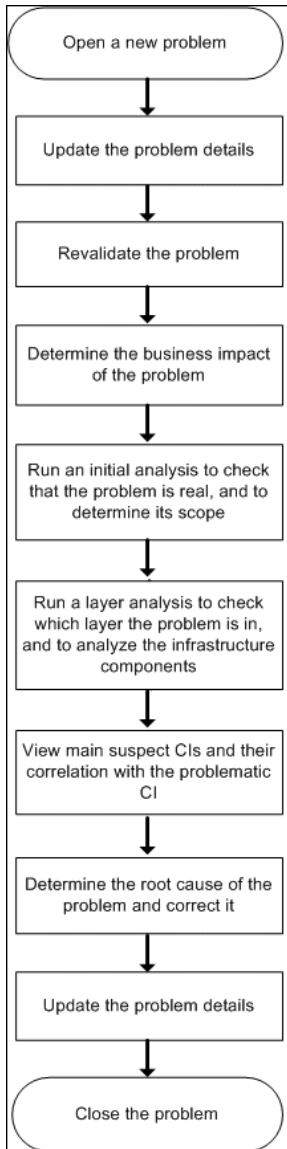
For details on Problem Isolation, see "Isolate a Problem" on page 22.

A problem's lifecycle incorporates elements from both the Problem list and Problem Isolation. For details of the problem lifecycle, see "The Problem Lifecycle" on page 14.

For a list of the prerequisites for working with the Problem Isolation module, see "Prerequisites" on page 27.

The Problem Lifecycle

The following diagram shows the lifecycle of a problem, which includes elements from both the Problem list and Problem Isolation.



Updating details of the problem can occur at any time in the cycle, as new information is discovered and conclusions are reached while isolating the problem.

The different steps carried out in isolating the problem can be performed as individual steps. They are not dependent on one another; however it is recommended to carry out all the steps in the order shown.

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 “Deploying the sis_for_pi_v7_0.zip File” on page 26.

For details on modifying standard correlation rules and TQLs, see “Modifying a Default Suspect Algorithm” on page 32 and “Modifying a Default On-demand Monitor TQL” on page 32.

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 85).

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 90), 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 81. Changes to existing monitor definitions for Suspect CIs in a topology are made using the “Suspect CI Monitor Configuration Page” on page 79.

Calculating the Business Impact of a Problem CI

Based on the number of SLAs containing the problematic CI, a numeric value is determined that is translated to the business impact of a problem. The following table lists the numeric value based on the number of affected SLAs, and the impact level to which the value is translated.

Number of SLAs	Value	Impact Level
N/A	1	Low
1 - 3	2	Medium
4 - 6	3	High
> 6	4	Strong

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 Main Suspects screen, is calculated according to the following formula:

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

plus

Changes weight, as configured in Problem Isolation infrastructure settings, * (log(1 + the number of changes made on the Suspect CI) / log(1 + the number of changes made to the first of the other Suspect CIs) + log(1 + the number of changes made to the next of the other Suspect CIs) + ... + log(1 + 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

Impacted monitors weight, as configured in Problem Isolation infrastructure settings, * (the number of impacted monitors for the CI that failed / the total number of impacted monitors for the CI)

plus

Dependencies monitors weight, as configured in Problem Isolation infrastructure settings, * (the number of dependent monitors for the CI that failed / the total number of dependent monitors for the CI)

plus

Dependencies changes weight, as configured in Problem Isolation infrastructure settings, * (the number of dependencies changes for the CI / the total number of dependencies changes for the suspect CIs)

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:

- ▶ Monitors weight
- ▶ Changes weight
- ▶ Diagnostic monitors weight
- ▶ Impacted monitors weight
- ▶ Dependencies monitors weight
- ▶ Dependencies changes 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 Main Suspects screen, 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 43 and “New Monitor Profile Page” on page 67.

Deploy Problem Isolation

The steps below describe the process used to deploy Problem Isolation.

Deploy the `sis_for_pi_v7_0.zip` File

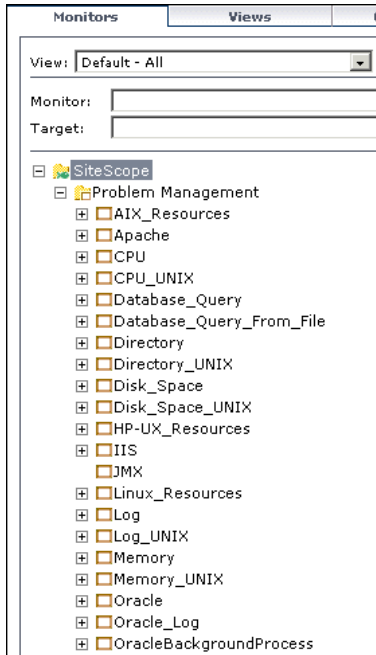
Deploy the `sis_for_pi_v7_0.zip` file included in Problem Isolation to install the following:

- ▶ **Problem Isolation monitors template.** This contains the SiteScope monitors used by Problem Isolation for running on-demand monitors on suspect CIs.
- ▶ **SQL scripts.** Used by the on-demand monitors.

For details, see “Deploying the `sis_for_pi_v7_0.zip` File” on page 26.

Example

After deploying the `sis_for_pi_v7_0.zip` file to the **SiteScope root directory** of a SiteScope machine, the monitor templates are automatically imported by SiteScope and the templates, monitors, and variables can be viewed and managed on the SiteScope machine.



Configure the Problem Isolation On-demand Monitors

Add or change monitor settings to adapt the on-demand monitors for your needs. For details on adding and changing monitors, see “Suspect CI Monitor Configuration Wizard” on page 27.

Manage a Problem

The steps below describe the process used to manage a problem.

Open the Problem

In Dashboard, right-click the problematic CI in View Explorer and select **Go to Problem Isolation**. From any step in Problem Isolation, click the **Actions** button and select **Create problem** from the menu. The **Problem Properties** pane opens where you enter the problem's details and click **Create**. For details on the Problem Properties pane, see "Problem List" on page 75.

Once a problem has been created, it appears in the Problem list.

A problem can only be opened on CIs of specific types, that are configured in the Problem Isolation Infrastructure settings. To modify the default list of CI types on which a problem can be opened, select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the **Allowed CI types for problem creation** entry in the **General Settings** table. Modify the comma separated list of CI types as applicable.

Update the Problem

Select **Applications > Problem Isolation** to open the Problem list and click the problem you want to update to select it. Update the relevant details in the **Problem Properties** pane and click **Update** to save the change. For details on the Problem list, see "Problem List" on page 75.

Close the Problem

Select **Applications > Problem Isolation** to open the Problem list and click the problem you want to close to select it. In the **Problem Properties** pane update the **Root Cause CI**, **Root Cause Layer**, and **Root Cause Description**, as well as any other relevant details, and change the problem status to **Closed**. Click **Update** to save the change. For details, see "Problem List" on page 75.

Isolate a Problem

The steps below describe the process used to isolate a problem and find its root cause. Each step is accessed by clicking the appropriate link in the Problem Isolation flow bar displayed at the top of each Problem Isolation page.

Note: Each of the isolation steps can be run independently of the others. However, it is recommended to carry out all the steps in the order in which they are listed.

You access the Problem Isolation pages by right-clicking a CI in Dashboard, and selecting **Go To Problem Isolation** in the menu, or by selecting **Applications > Problem Isolation** and clicking the **Triage** button for a problem in the Problem list. When accessing Problem Isolation from the Dashboard, the Validation page is displayed and when accessing Problem Isolation by clicking the Triage button in the Problem list, the Initial Analysis page is displayed.

Validate the Problem

Rerunning the transactions affected by the problem 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 problem 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 90.

Determine the Impact of the problem 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 affected by the problem. Knowing its impact helps you prioritize the problem.

For details on determining the impact of a problem, see “Impact Page” on page 45.

Run an Initial Analysis on the Problem

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 synthetic monitors (Business Process Monitors), and 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 47.

Run a Layer Analysis on the Problem

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.

View the Main Suspects and the Correlation Graph

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, changes, related topology status for dependencies and impacted CIs, and deeper diagnostic scripts).

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 Suspects, see “Suspects Page” on page 85.

Problem Isolation Standard User Interface Elements

The user interface for the steps used to isolate a problem has a standard layout and includes common elements in each step. For details on the steps used to isolate a problem, see “Isolate a Problem” on page 22.

Isolation Steps and Flow Bar

At the top of each page, the different isolation steps are listed in the recommended order for isolating a problem. Click on a step to access the relevant user interface page.



Under the steps is a flow bar with an indicator that shows you which isolation step is current.

Left Pane

The left pane contains the following data:




- ▶ **Highlights.** Contains the general status of the problem or system, that is relevant to the current Problem Isolation step.
- ▶ **Info.** Contains specific data relating to the current Problem Isolation step and provides links for displaying detailed data and reports in the main display area of the page.
- ▶ **Recommendations.** Based on the data collected and analyzed for the current Problem Isolation step, displays the recommended Problem Isolation steps with which to continue, to help solve the problem.

Right Pane

The right pane displays data and reports for the current Problem Isolation step, that are accessed by clicking on the Info messages in the left pane.

Common User Interface Elements

The following table describes the standard user interface elements that are included in the steps used to isolate a problem:

GUI Element	Description
	Click to display both the left and right panes.
	Click to maximize a pane so that it uses the entire display area and hides the second pane.
	Click to minimize a pane so that it is hidden by the other pane, that uses the entire display area.
<Breadcrumb>	<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 its status. 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>
Actions	<p>Click the Actions button to open the Actions menu, which includes the following options:</p> <ul style="list-style-type: none"> ▶ Create problem. Click to create a new problem. For details on creating a problem, see “Manage a Problem” on page 21. ▶ Open ticket. Click to access HP ServiceCenter software, where you can open a ticket for a problem. A link to HP ServiceCenter software must be configured in Infrastructure Settings.
On-demand Monitors	Click the On-demand Monitors button to open the On-demand Monitors Results pane, where you can view the status of, and run, the on-demand monitors for Suspect CIs.
Properties	Click the Properties button to open the Problem Properties pane, where you can view and update a problem's properties.

Deploying the sis_for_pi_v7_0.zip File

The `sis_for_pi_v7_0.zip` file that is included with HP Business Availability Center contains:

- ▶ the template container of the SiteScope monitor templates that are used by Problem Isolation on-demand monitors when gathering information about a problem's suspect CIs.
- ▶ the SQL scripts that are used by a number of on-demand monitors when gathering information about a problem's suspect CIs.

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

You deploy the `sis_for_pi_v7_0.zip` file on each of the SiteScope machines in your system used to run Problem Isolation on-demand monitors. Once deployed, SiteScope automatically adds the template container to its configuration, and imports the Problem Isolation monitor templates.

Note: Once the monitor templates have been imported, the templates, monitors, and variables can only be managed directly on the SiteScope machines, and not via 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.

To deploy the sis_for_pi_v7_0.zip file:

Extract the sis_for_pi_v7_0.zip file included in HP Business Availability Center, to the **SiteScope root directory** on the SiteScope machine. Make sure to use the folder names to keep the directory structure.

Prerequisites

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

- SiteScope 8.7 or later

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 81).

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 79.



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 82.
- ▶ **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 83.
- ▶ **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 83.
- ▶ **Summary.** Displays and saves the configured data. This page is not available when editing an existing Suspect CI monitor configuration.

Changing the Default Number of Hosts on Which a Script is Revalidated

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.

Changing the Default Transactions Status for Automatic Revalidation

By default, only problematic transactions (that is, transactions that had 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 dropdown list as required.

Configuring the Link to HP ServiceCenter Software

You can configure a link to HP ServiceCenter software and access it from Problem Isolation to open a ticket on a problem. You access HP ServiceCenter software from Problem Isolation by:

- ▶ clicking the **Open Ticket** button for a problem in the Problem list.
- ▶ clicking the **Actions** button in any Problem Isolation step and selecting **Open Ticket** from the menu.

To configure a link to HP ServiceCenter software:

To configure a link to HP ServiceCenter software, select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the **HP ServiceCenter software URL** entry in the **General** table. Enter the URL for HP ServiceCenter software in the following format:

<http://<HP ServiceCenter software server name or IP address>:<port number for accessing the HP ServiceCenter software server >/sc/index.do?ctx=docEngine&file=probsummary&query=false>

Disabling Automatic Transaction Revalidation

By default, when isolating a problem from Dashboard, the transactions for the selected problem are automatically revalidated. 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**.

Modifying the BPM Triage Report's Default Time Period

To modify the default time period used by the BPM Triage report, select **Admin > Platform > Setup and Maintenance > Infrastructure Settings**, choose **Applications**, select **Problem Isolation**, and locate the following entries in the **Initial Analysis** table:

- ▶ **Problem Scope Report Time Frame Hours Back.** Modify the number of hours prior to the problem open time to use as the starting time for the BPM Triage report.
- ▶ **Problem Scope Time Frame Hours Length.** Modify the duration, in hours, of the BPM Triage report time frame.

Modifying the Error Summary Report's Default Time Period

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 following entries in the **Initial Analysis** table:

- ▶ **Error Summary Report Time Frame Hours Back.** Modify the number of hours prior to the problem open time to use as the starting time for the Error Summary report.
- ▶ **Error Summary Report Time Frame Hours Length.** Modify the duration, in hours, of the Error Summary report time frame.

Modifying the Event Over Time Report's Default Time Period

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 following entries in the **Initial Analysis** table:

- **Error Over Time Report Time Frame Hours Back.** Modify the number of hours prior to the problem open time to use as the starting time for the Error Over Time report.
- **Error Over Time Report Time Frame Hours Length.** Modify the duration, in hours, of the Error Over Time report time frame.

Modifying the KPI Over Time Report's Default Time Period

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 following entries in the **Initial Analysis** table:

- **KPI Over Time Report Time Frame Days Back.** Modify the number of days prior to the problem open time to use as the starting day for the KPI Over Time report.
- **KPI Over Time Frame Days Length.** Modify the duration of the KPI Over Time report time frame.

Modifying a Default Suspect Algorithm

If you want to modify one of the default suspect algorithms (that is, a suspect correlation rule) included in the standard Problem Isolation package, you should make a copy of the rule and modify the copy. This ensures that your changes will not be 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** You can now modify the new rule as required.

Modifying a Default On-demand Monitor TQL

If you want to modify one of the default on-demand monitor TQLs included in the standard Problem Isolation package, you should make a copy of the TQL and modify the copy. This ensures that your changes will not be overwritten if a new Problem Isolation package is deployed.

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 You can now modify the new TQL as required.

Troubleshooting and Limitations

This chapter includes troubleshooting and limitations for Problem Isolation.

- ▶ 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 will not be 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 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 70.
- ▶ The Correlation graph currently displays Business Process Monitor KPI measurements only. Real User Monitor KPI measurements are not displayed.
- ▶ The Problem Isolation Validation step is unable to revalidate transactions on synthetic users (Business Process Monitors) that use basic authentication.
- ▶ 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.
- ▶ 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.

- 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 *IT World Model Management*. For details on configuring on-demand monitors, see “Suspect CI Monitor Configuration Wizard” on page 81.

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

- 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 *IT World Model Management*.

Part II

User Interface

2

Problem Isolation User Interface

This chapter includes the pages and dialog boxes that are part of the Problem Isolation user interface, listed alphabetically.

This chapter describes:	On page:
Correlation Graph	40
Edit Monitor Profile Page	43
Impact Page	45
Initial Analysis Page	47
Layer Analysis Page	53
List of Monitors	63
List of On-demand Monitors	64
Monitor Profile Configuration Page	65
New Monitor Profile Page	67
On-demand Monitor Details Dialog Box	69
On-demand Monitor Parameters Dialog Box	70
On-demand Monitors Results Pane	71
Problem List	75
Suspect CI Monitor Configuration Page	79
Suspect CI Monitor Configuration Wizard	81
Suspects Page	85

This chapter describes:	On page:
System CI Summary Report	89
Validation Page	90

Correlation Graph

Description	<p>Displays the correlation between a problem CI's transactions and a selected Suspect CI's measurements. Also shows changes made to the selected suspect CI.</p> <p>To access: Click the Show Correlation Graph button on the Suspects page.</p>
Included in Tasks	"Isolate a Problem" on page 22
Important Information	If you select a time range greater than 48 hours, data for the last two hours is not included in the graph.

Graph Settings

The area includes the following elements (listed alphabetically):

<Common report settings>	For details, see “Understanding Common Report Elements” in <i>Reference Information</i> .
EUM Monitor	<p>Select the problem CI’s Business Process step, or transaction monitor child CI to include in the Correlation graph. If the CI on which the problem was opened does not have any such child CIs, the problem CI itself is included.</p> <p>Default value: All of the problem CI’s Business Process steps and transaction monitors are included in the list, and the first one is selected.</p> <p>Customization: To modify the Business Process steps and transaction monitors displayed in the list, so that only bad ones are displayed, select Admin > Platform > Setup and Maintenance > Infrastructure Settings, choose Applications, select Problem Isolation, and locate the Show only bad transactions in correlation graph filter entry in the Correlation Graph table. Modify the value to true.</p>
KPI	<p>The KPI of the CI on which the problem was opened, that is included in the Correlation graph.</p> <p>Default value: The problem CI’s KPI on which the problem was opened.</p>
Measurement Filter	<p>Click to open a list (sorted alphabetically) of all the measurements for the selected Suspect CI. Select the checkboxes of the measurements you want to include in the graph.</p> <p>Default value: The first six measurements in the list.</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 Number of selected measurements in filter entry in the Correlation Graph table. Modify the value to the required number of measurements.</p>

Graph Content

The Correlation graph includes the following elements (listed alphabetically):

GUI Element	Description
<Bars>	Show changes made to the selected Suspect CI, over the time period for which the Correlation graph is displayed. Tooltip: The relevant time period from the first to the last change, the contained CI names and the number of changes for each one.
<Legend>	Describes the color coding used in the graph.
<Thick line connecting data points>	Shows the status of the selected transaction for the problem CI, over the time period for which the Correlation graph is displayed. Tooltip: The transaction name, the availability or performance status value, and the aggregated data measurement in seconds for performance, or percentage for availability.
<Thin lines connecting data points>	Show the status of the selected measurements for the selected Suspect CI, over the time period for which the Correlation graph is displayed. Tooltip: The measurement name, the relevant time, the measurement value, the monitored CI name, and the name of the Suspect CI.
Scaled Value <y-axis>	The KPI measurements, scaled as percentage units, with the highest measurement represented as 100%.
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 43) and the SiteScope Template pane (for details, see page 44).</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.
Included in Tasks	“Deploy Problem Isolation” on page 19
Useful Links	“Naming Conventions” in <i>Reference Information</i>

Monitor Profile General Properties Pane

The Monitor Profile General Properties pane includes the following elements (listed alphabetically):

GUI Element	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. Valid options are:</p> <ul style="list-style-type: none"> ➤ Connectivity ➤ Critical Services ➤ Health ➤ Other <p>Default value: Other</p>

GUI Element	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 SiteScope Template pane includes the following elements (listed alphabetically):

GUI Element	Description
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.
Parameter Name	Displays the parameters available for the monitor in the selected SiteScope template.
Parameter Default Value	Enter a default value to be used for the monitor parameter.

Impact Page

Description	Displays a problem's impact on business and also shows the SLAs 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" on page 22
Useful Links	"Problem Isolation Standard User Interface Elements" on page 24

The impact page includes the following panes:

- "Left Pane" on page 45
- "Right Pane" on page 46

Left Pane

The left pane includes the following elements (listed alphabetically):

GUI Element	Description
Highlight	Displays the general business impact of the problem. For details on how the impact level is calculated, see "Calculating the Business Impact of a Problem CI" on page 16.
Info - SLA Impact	Displays the number of SLAs impacted by the problem 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.
Recommendation	Compares the impact of the problem to that of other open problems and recommends what steps to take.

Right Pane

The right pane includes the following elements (listed alphabetically):

GUI Element	Description
<Legend>	Describes the different SLA statuses shown.
SLA Description	Displays the description, customer, and provider of the impacted SLA. Tooltip: Full SLA description.
SLA Name	Displays the name of the impacted SLA. Tooltip: Full SLA name.
SLA Status	The status shows a 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. Tooltip: Hold the cursor over the speedometer, or status icon, to display the status and the relevant time period.

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 synthetic monitors, and if your system is configured for snapshot on error, displays the relevant snapshots. ▶ 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"> ▶ Synthetic User (BPM) Error Summary Pane (for details, see page 49). ▶ Synthetic User (BPM) Event Over Time Pane (for details, see page 50). ▶ Problem Scope Pane (for details, see page 52). ▶ KPI Over Time Report Pane (for details see page 52). <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 problem in the Problem list.
<p>Included in Tasks</p>	<p>“Isolate a Problem” on page 22</p>
<p>Useful Links</p>	<p>“Problem Isolation Standard User Interface Elements” on page 24</p>

Left Pane

The left pane includes the following elements (listed alphabetically):

GUI Element	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 - End User Errors	If the Problem 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 Synthetic User (BPM) Error Summary Pane in the main display area (for details, see page 49).
Info- Event Over Time	Click on the message to display the Synthetic User (BPM) Event Over Time Pane in the main display area, where you can view a graph of the errors and events that occurred on synthetic users (BPM) over a period of time (for details, see page 50).
Info - Problem Over Time	If the Problem CI is monitored by end-user monitors, and KPI data over time exists for the Problem CI, a message indicating the number of related KPIs that have a problematic status is displayed. Click on the message to display the KPI Over Time Report Pane in the main display area (for details, see page 52).
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 52).
Recommendation	Displays the recommended steps to take, to help solve the problem.

Synthetic User (BPM) Error Summary Pane

Description	<p>The Synthetic User (BPM) Error Summary pane displays one of the following:</p> <ul style="list-style-type: none"> ➤ Synthetic User (BPM) Error Summary Report (for details, see page 49). The default view when the pane is first accessed. ➤ Error List (for details, see page 50). Accessed from the Synthetic User (BPM) Error Summary report.
Important Information	<p>For details on modifying the default time period used by the report, see “Modifying the Error Summary Report’s Default Time Period” on page 30.</p>

Synthetic User (BPM) Error Summary Report

Report Settings

<Common report settings>	<p>For details, see “Understanding Common Report Elements” in <i>Reference Information</i>.</p>
--------------------------	---

Report Content

Description	<p>The Synthetic User (BPM) 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 50.</p>



Error List

Report Settings

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

Report Content

The Error list includes the following elements (listed alphabetically):

GUI Element	Description
	Click to displaying a snapshot of the page on which the error occurred. Note: This button is only enabled if a snapshot of the page exists.
	Click to open a zip file of a page’s snapshot. Note: This button is only enabled if a zip file of the page’s snapshot exists.
Time	Displays the time that the error occurred.

Synthetic User (BPM) Event Over Time Pane

Description	The Synthetic User (BPM) Event Over Time pane displays one of the following: <ul style="list-style-type: none"> ▶ Synthetic User (BPM) Error Summary Report (for details, see page 49). The default view when the pane is first accessed. ▶ Error List (for details, see page 50). Accessed from the Synthetic User (BPM) Event Over Time report.
Important Information	For details on modifying the default time period used by the report, see “Modifying the Event Over Time Report’s Default Time Period” on page 31.

Report Settings

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

Report Content

The Synthetic User (BPM) Event Over Time report includes the following elements (listed alphabetically):

GUI Element	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 50.</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 synthetic users.
Time <x-axis>	The time division units for the time range specified when generating the report.

Problem Scope Pane

Description	The Problem Scope pane displays the Transaction by Location section of the Business Process Monitor Triage report. For details on the Triage report, see “Triage Raw Data Report” in <i>Using End User Management</i> .
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 Problem CI. ▶ For details on modifying the default time period used by the report, see “Modifying the BPM Triage Report’s Default Time Period” on page 30.

KPI Over Time Report Pane

Description	The KPI Over Time Report pane displays the KPI Over Time report for the Problem 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	For details on modifying the default time period used by the report, see “Modifying the KPI Over Time Report’s Default Time Period” on page 31.

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 56) ▶ Transactions Layer Breakdown Pane (for details, see page 62) <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” on page 22
Useful Links	“Problem Isolation Standard User Interface Elements” on page 24

The Layer Analysis page includes the following panes:

- ▶ “Left Pane” on page 54
- ▶ “Layer Deviation Analysis Pane” on page 54
- ▶ “System Status Pane” on page 56
- ▶ “Transactions Layer Breakdown Pane” on page 62

Left Pane

The left pane includes the following elements (listed alphabetically):

GUI Element	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 56).
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 62).
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 Problem CI.

Settings

The area includes the following elements (listed alphabetically):

<Common report settings>	For details, see “Understanding Common Report Elements” in <i>Reference Information</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 Problem CI are displayed.
Compare To	<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.
Current	<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 Layer Deviation Analysis pane includes the following elements (listed alphabetically):

GUI Element	Description
<Fuel gauge>	<p>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.</p>

System Status Pane

<p>Description</p>	<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 57
- “Category Status for a Tier Report” on page 59

System Status Report

Report Settings

The area includes the following elements (listed alphabetically):

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

Report Content

The System Status report includes the following elements (listed alphabetically):

GUI Element	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	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 59), showing the status of the Suspect CIs included in each of the categories that comprise the tier.</p>

Category Status for a Tier Report

Important Information	<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 area includes the following elements (listed alphabetically):

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

Report Content

The Category Status for a Tier report includes the following elements (listed alphabetically):

GUI Element	Description
<Legend>	Describes the color coding of the statuses included in the report.
CI Type	Displays the CI type icon of the Suspect CI.
CI Name	Displays the name of the Suspect CI. Tooltip: The full CI name, the weighted percentage of failed monitors for the CI, and the number of failed monitors out of the total number of monitors run for the CI in each category in the tier.

GUI Element	Description
<p>Connectivity</p>	<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>
<p>Critical Services</p>	<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	Description
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>

GUI Element	Description
Deployed Monitors	Displays the number of failed monitors out of the total number of monitors deployed on the Suspect CI in the selected tier. Click the number of monitors to see the List of Monitors.
Changes	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. For details on the Changes report, see “Change Report User Interface” in <i>IT World Model Management</i> .

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 Problem CI.

Report Settings

The area includes the following elements (listed alphabetically):

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

Report Content

The Transaction Layer Breakdown pane includes the following elements (listed alphabetically):

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

List of Monitors

Description	Displays the monitors for the Suspect CI and its descendants. To access: Click the value displayed for problem monitors in the Current Status column on the Suspects page.
Included in Tasks	“Isolate a Problem” on page 22

The List of Monitors includes the following elements (listed alphabetically):

GUI Element	Description
CI Name	The name of the Suspect CI.
CI Type	The type of the Suspect CI.
Monitor Name	The name of the monitor that was run on the Suspect CI.
Monitor Status	The Dashboard status of the monitor that was run on the Suspect CI. Tooltip: Status details.
Monitor Type	The type of the monitor that was run on the Suspect CI.

List of On-demand Monitors

Description	Displays the on-demand monitors that were run on the suspect CI. To access: Click a category in the Category Status for a Tier report, which is part of the System Status report.
Included in Tasks	“Isolate a Problem” on page 22


The List of On-demand Monitors includes the following elements (listed alphabetically):

GUI Element	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	Displays existing monitor profiles for Problem Isolation on-demand monitors. Enables you to edit existing monitor profiles and configure new ones. To access: Admin > Problem Isolation > Monitor Profiles
Included in Tasks	“Deploy Problem Isolation” on page 19

The Monitor Profile Configuration page includes the following elements (listed alphabetically):

GUI Element	Description
	Click to access the Edit Monitor Profile Page, where you edit an existing monitor profile configuration.
Category	Displays the category to which the monitor belongs. Valid options are: <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	You edit an existing monitor profile on the Edit Monitor Profile page.
Included in Tasks	“Deploy Problem Isolation” on page 19
Useful Links	“Naming Conventions” in <i>Reference Information</i>

Monitor Profile General Properties Pane

The Monitor Profile General Properties pane includes the following elements (listed alphabetically):

GUI Element	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. Valid options are:</p> <ul style="list-style-type: none"> ▶ Connectivity ▶ Critical Services ▶ Health ▶ Other <p>Default value: Other</p>

GUI Element	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 17.</p> <p>Default Value: 1</p> <p>Note: The weight must be a positive integer between 0 and 100.</p>

SiteScope Template Pane

The SiteScope Template pane includes the following elements (listed alphabetically):

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

On-demand Monitor Details Dialog Box

Description	Dialog box to view the details of an on-demand monitor run. To access: Click the status of a monitor from the list in the On-demand Monitors Results pane.
Included in Tasks	“Isolate a Problem” on page 22


The On-demand Monitor Details dialog box includes the following elements (listed alphabetically):

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

On-demand Monitor Parameters Dialog Box

Description	Dialog box to change the parameters of on-demand monitors, before running them. To access: Click a monitor from the list in the On-demand Monitors Results pane.
Included in Tasks	“Isolate a Problem” on page 22


The On-demand Monitor Parameters dialog box includes the following elements (listed alphabetically):

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





On-demand Monitors Results Pane

Description	Lists the on-demand monitors that are run on Suspect CIs and shows their status. Also enables you to run the monitors. To access: Click the On-demand Monitors button on any Problem Isolation page.
Included in Tasks	“Isolate a Problem” on page 22

The On-demand Monitors Results pane includes the following elements (listed alphabetically):

GUI Element	Description
	Click to refresh the displayed list of monitors.
Abort	Click the Abort button to cancel all pending monitors. Monitors that are currently running will not be 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	Select the filter by which to group the displayed monitors. Valid options are: <ul style="list-style-type: none"> ➤ Monitor type ➤ Suspect CI ➤ Topology pattern Default value: Monitor type

GUI Element	Description
Monitor Type	<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 70.</p> <p>Tooltip: The CI type of the Suspect CI on which the monitor runs, the topology pattern used by the monitor, the variable values obtained from the topology pattern for use 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>
Run Monitors	Click the Run Monitors button to run the selected on-demand monitors.

GUI Element	Description
<p>Status</p>	<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 ➤  Idle. ➤  OK. The monitor ran successfully. ➤  Bad. The monitor ran, but was not successful. ➤  Failed. The monitor did not successfully complete its run. <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 69.</p> <p>Tooltip: The monitor run results.</p>
<p>Suspect CI</p>	<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 70.</p> <p>Tooltip: The Suspect CI type, the topology pattern used by the monitor that runs on it, the variable values obtained from the topology pattern for use by the monitor, 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 List

Description	The page on which you manage, update, and close problems. Click on a problem in the Problem list to make it current. To access: Applications > Problem Isolation
Included in Tasks	“Manage a Problem” on page 21

The Problem list includes the following panes:

- “Problems Pane” on page 75
- “Problem Properties Pane” on page 77

Problems Pane

Description	The Problems pane comprises two areas. The top area includes filters for selecting the problems included in the Problem list, which is displayed in the main, bottom area.
--------------------	--

Filters Area

The Filters area includes the following elements (listed alphabetically):

GUI Element	Description
<Common report settings>	For details, see “Understanding Common Report Elements” in <i>Reference Information</i> .
Open Date	Filter for selecting the records displayed in the Problem list by the date and time the problem was opened. Select a pre-defined option from View , or click the from and to links to open a dialog box in which you can set the start and end time and date. Default value: Current date to one week back

GUI Element	Description
Opened By	Filter for selecting the records displayed in the Problem list by the login name of the user who opened the problem.
Problem Status	Filter for selecting the records displayed in the Problem list by problem status. Default value: Active

Problem List

The Problem list includes the following elements (listed alphabetically):

GUI Element	Description
Business Entity Name	The full name, including the path, of the CI on which the problem was opened. If the name is longer than the available space, three dots (...) are added at the beginning of the name.
Business Priority	The assigned business priority. Available options are: <ul style="list-style-type: none"> ▶ High ▶ Medium ▶ Low
Current Entity	The name of the problem CI's KPI on which the problem was opened.
Elapsed Time	The amount of time elapsed since the problem was opened.
Generate	Click the Generate button to create and display the problem list using the filters you set.
Open Ticket	Click to open HP ServiceCenter software, where you can open a ticket for the problem. A link to HP ServiceCenter software must be configured in Infrastructure Settings. For details on configuring a link to HP ServiceCenter software, see "Configuring the Link to HP ServiceCenter Software" on page 29.

GUI Element	Description
Opened By	Filter for selecting the records displayed in the Problem List by the login name of the user who opened the problem.
PID	Automatically assigned, unique problem ID.
Problem Opened Date	Filter for selecting the records displayed in the Problem List by the date and time the problem was opened. Select a pre-defined option from View , or click the from and to links to open a dialog box in which you can set the start and end time and date. Default value: Current date to one week back
Problem Status	Filter for selecting the records displayed in the Problem List by problem status. Default value: Active
Problem Status	Assigned problem status. Available options are: <ul style="list-style-type: none"> ▶ Active. For new problems. ▶ Known Error. For problems that have been successfully identified and for which a workaround has been developed. ▶ Closed. For problems that have been resolved and for which a record of the solution has been recorded.
Triage	Click to go to the Initial Analysis page for the specific problem.

Problem Properties Pane

Description	Contains detailed information about the problem currently selected in the list of problems in the Problems pane. Also used for updating problem information.
--------------------	--

The Problem Properties pane includes the following elements (listed alphabetically):


GUI Element	Description
Acknowledgement Details	Sets the acknowledgement status and details of the CI in Dashboard. For details on acknowledging CIs, see “Acknowledge Performance Problems” in <i>Using Dashboard</i> .
Business Impact	Sets the business impact of the problem. Default value: Medium
Business Priority	Sets the business priority of the problem. Default value: Medium
Business Urgency	Sets the business urgency of the problem. Default value: Normal
CI Type	Displays the CI type for the CI on which the problem was opened.
Create	Click the Create button to save the properties of a new problem. Note: This button is only visible when creating a new problem.
Elapsed Time	Displays the length of time elapsed since the problem was opened.
Opened By	Displays the login name of the user who opened the problem.
Opened Time	Displays the time that the problem was opened.
Problem Category	Sets the category of the problem.

GUI Element	Description
Problem Status	Sets the status of the problem Default value: Current value, or Active for a new problem.
Update	Click the Update button to update the values of the editable properties with the current status. Note: This button is only visible when updating the details of an existing problem.


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
Included in Tasks	“Deploy Problem Isolation” on page 19

The Suspect CI Monitor Configuration page includes the following elements (listed alphabetically):

GUI Element	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” on page 19</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 New Suspect CI Topology Configuration page includes the following elements (listed alphabetically):

GUI Element	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 will not be 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 Configure Monitor Parameters page includes the following elements (listed alphabetically):

GUI Element	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” on page 22
Useful Links	“Problem Isolation Standard User Interface Elements” on page 24

The Suspects page includes the following panes:

- “Left Pane” on page 85
- “Right Pane” on page 86

Left Pane

The left pane includes the following elements (listed alphabetically):

GUI Element	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


Settings

The area includes the following elements (listed alphabetically):

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

Content

The area includes the following elements (listed alphabetically):

GUI Element	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 for the Suspect CI. Tooltip: The name of the CI type.
Current Status	Displays the status icon for the Suspect CI, based on the status of the worst monitor in the group of monitors run on the CI. Also displays the number of problem monitors (out of the total number of monitors) for the CI and its descendants. Click on the number of problem monitors displayed to see the List of Monitors. Tooltip: The number of problem monitors and the number of total monitors for the Suspect CI.
Dependent CI Status	Displays the worst status of the dependent CIs of the suspect CI, as well as the number of such CIs that are problematic out of the total number of dependent CIs. Click on the number of dependent CIs to display the System CI Summary report. Tooltip: A list of the dependent CIs and the number of failed monitors out of the total number of monitors run for each one.
Discovered Changes	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 User Interface” in <i>IT World Model Management</i> . Tooltip: The number of discovered changes and the time frame in which they were discovered.

GUI Element	Description
<p>Discovered Dependent CI Changes</p>	<p>Displays the number of changes made to dependent CIs of the suspect CI, and their descendant CIs. Click the number of changes displayed to display the System CI Summary report.</p> <p>Tooltip: A list of the dependent CIs and the number of changes for each one.</p>
<p>Impacted CI Status</p>	<p>Displays the worst status of the CIs of which the suspect CI is a dependent, as well as the number of such CIs that are problematic out of the total number of impacted CIs. Click on the number of impacted CIs to display the System CI Summary report</p> <p>Tooltip: A list of the impacted CIs and the number of failed monitors out of the total number of monitors run for each one.</p>
<p>On-demand Monitor Results</p>	<p>Displays the success ratio of the on-demand monitors run on the Suspect CI. Click on 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.</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>Show Correlation Graph</p>	<p>Click the Show Correlation Graph button to open the Correlation graph.</p> <p>Note: You must select a Suspect CI to be included in the Correlation graph.</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.</p> <p>Tooltip: The weight and score for each column of data for the suspect CI.</p>

System CI Summary Report

Description	<p>Displays the impacted or dependent CIs of a Suspect CI, depending from where you access the report, and shows information about them.</p> <p>To access:</p> <ul style="list-style-type: none"> ▶ Click the value displayed for the problematic CIs in the Impacted CI Status column in the Suspects page. The report shows the impacted CIs of the Suspect CI (that is, the CIs of which the Suspect CI is a dependent). ▶ Click the value displayed for the problematic CIs in the Dependent CI Status column in the Suspects page. The report shows the dependent CIs of the Suspect CI. ▶ Click the value displayed for the changes in the Dependent CI Changes column in the Suspects page. The report shows the dependent CIs of the Suspect CI.
Included in Tasks	“Isolate a Problem” on page 22

The System CI Summary report includes the following elements (listed alphabetically):

GUI Element	Description
<Legend>	Describes the CI status icons used in the report.
Discovered Changes	Displays the number of discovered changes for the CI. Note: This column is not included in the report when it displays the impacted CIs of the Suspect CI (that is, when it is accessed by clicking the number of problematic CIs in the Impacted CI Status column in the Suspects Page).
CI Name	Displays the CI name.
Deployed Monitors	Displays the number of monitors that were run on the CI out of the total number of monitors available for the CI.
Current Status	Displays the current status of the CI.
Suspect Type	Displays the CI type icon for the Suspect CI. Tooltip: The name of the CI type.

Validation Page

Description	<p>Revalidates the transactions affected by the Problem 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	<ul style="list-style-type: none">▶ 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 the Dashboard. For details on disabling automatic revalidation, see “Disabling Automatic Transaction Revalidation” on page 30.▶ By default, only problematic transactions (that is, transactions with a status of failed, minor, or critical when the problem was opened) are automatically revalidated. For details on changing the transaction status for automatic revalidation, see “Changing the Default Transactions Status for Automatic Revalidation” on page 29.▶ 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. For details on changing the number of hosts on which a script is revalidated, see “Modifying the KPI Over Time Report’s Default Time Period” on page 31.▶ 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.
------------------------------	---

Included in Tasks	“Isolate a Problem” on page 22
Useful Links	“Problem Isolation Standard User Interface Elements” on page 24

The Validation page includes the following panes:

- “Left Pane” on page 92
- “Right Pane” on page 92

Left Pane







The left pane includes the following elements (listed alphabetically):





GUI Element	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 right pane includes the following elements (listed alphabetically):

GUI Element	Description
	Click to refresh the list of transactions displayed.
<Legend>	Describes the icons used to denote the open and current statuses.
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	Description
<p>Open Status</p>	<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>Customization: To modify the time period on which transaction status is calculated, 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 number of hours prior to the problem open time that you want to use.</p> <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>
<p>Run Transaction</p>	<p>Click the Run Transaction button to start manual revalidation of selected transactions.</p>
<p>Script Name</p>	<p>The name of the script in which the transaction is included.</p>

GUI Element	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>

Index

B

business impact 16

C

changing the default number of hosts for revalidation
 problem isolation 28
changing the default transaction status for automatic revalidation
 problem isolation 29
configure monitor parameters page 83
correlation graph
 problem isolation 40

D

deploy problem isolation 19
deploying the sis_for_pi_v7_0.zip file
 problem isolation 26
disabling automatic revalidation of transactions
 problem isolation 30

E

edit monitor profile page 43
edit suspect CI monitor configuration wizard 81
error summary report
 changing the default time period in
 problem isolation 30
event over time report
 changing the default time period in
 problem isolation 31

H

HP ServiceCenter software
 linking to problem isolation 29

I

impact page 45
initial analysis page 47
introduction to problem isolation 12

K

KPI over time report
 changing the default time period in
 problem isolation 31

L

layer analysis page 53
list of monitors 63
list of on-demand monitors 64

M

monitor profile configuration page 65

N

new monitor profile page 67
new suspect CI monitor configuration wizard 27, 81

O

on-demand monitor details dialog box 69
on-demand monitor parameters dialog box 70

Index

- on-demand monitor TQL
 - modifying defaults in problem isolation 32
- on-demand monitors 15
- on-demand monitors results pane 71
- on-demand monitors success ratio
 - problem isolation 17

P

- prerequisites
 - problem isolation 27
- problem isolation
 - changing the default number of hosts for revalidation 28
 - changing the default time period of the BPM triage report 30
 - changing the default time period of the error summary report 30
 - changing the default time period of the event over time report 31
 - changing the default time period of the KPI over time report 31
 - changing the default transaction status for automatic revalidation 29
 - configuring a link to HP ServiceCenter software 29
 - deploying the sis_for_pi_v7_0.zip file 26
 - disabling automatic revalidation of transactions 30
 - introduction 12
 - modifying a default on-demand monitor TQL 32
 - modifying a default suspect algorithm 32
 - new suspect CI monitor configuration wizard 27
 - prerequisites 27
 - problem lifecycle 14
 - standard user interface elements 24
 - troubleshooting and limitations 33
 - user interface 39
- problem isolation concepts
 - business impact 16

- introduction 12
- on-demand monitors 15
- on-demand monitors success ratio 17
- problem lifecycle 14
- suspect CI weighting 17
- problem isolation tasks
 - deployment 19
 - isolate a problem 22
 - manage a problem 21
- problem lifecycle 14
- problem list 75

S

- select suspect CI monitors page 83
- select suspect CI topology page 82
- sis_for_pi_v7_0.zip file
 - deploying for problem isolation 26
- standard user interface elements
 - problem isolation 24
- suspect algorithm
 - modifying defaults in problem isolation 32
- suspect CI monitor configuration page 79
- suspect CI monitor configuration wizard 81
- suspect CI weighting
 - problem isolation 17
- suspects page 85
- system CI summary report 89

T

- trriage report
 - changing the default time period in problem isolation 30
- troubleshooting and limitations
 - problem isolation 33

U

- user interface
 - problem isolation 39

V

- validation page 90