

HP OpenView Self-Healing Services

User's Guide

Software Version: 2.60

for the following operating systems:

HP-UX 11.x

Solaris 7, 8, 9, and 10

Microsoft Windows 2000 Professional SP-4, 2000 Advanced Server, 2003 Server, XP Professional



Manufacturing Part Number : None

Document Release Date: February 2007

Software Release Date: February 2007

© Copyright 2003-2007 Hewlett-Packard Development Company, L.P.

Legal Notices

Warranty.

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

The information contained herein is subject to change without notice.

Restricted Rights Legend.

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

Copyright Notices.

©Copyright 2003-2007 Hewlett-Packard Development Company, L.P.

No part of this document may be copied, reproduced, or translated to another language without the prior written consent of Hewlett-Packard. The information contained in this material is subject to change without notice.

Trademark Notices.

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32- and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

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

UNIX® is a registered trademark of the Open Group.

Itanium® is a registered trademark of Intel Corporation or its subsidiaries in the United States and other countries.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

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

Additional Notices

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

1. Introduction to Self-Healing Services

In This Chapter	18
About Self-Healing Services	19
An Overview of Software Fault Management	20
What Is Self-Healing?	21
When is Self-Healing Useful?	21
How Does Self-Healing Services Help?	22
What is HP OpenView Self-Healing Services?	23
Self-Healing Services Roles	25
Self-Healing Process	29
Data Collection	31
Analysis	31
Report Life Cycle	31

2. The Self-Healing Services Client User Interface

In This Chapter	34
Overview	35
Start or Stop the Self-Healing Services Client	36
Start the Self-Healing Services User Interface	37
Local Managed Client Page	39
Configuration Center Page	44

3. Customizing Your Self-Healing Environment

In This Chapter	50
Specifying Global Settings at the Configuration Center	51
Change Your User Name or Password	51
Customize the Default Rule Settings	55
Configure the Notification Settings	57
Configure the E-mail Server Settings	64
Change Your Contact Information	66
Add, Edit, or Remove Managed Clients	68
Add, Edit, or Remove a Communication Gateway	73
Add a Gateway	74
Change the Port Number for a Gateway	75
Remove a Gateway	76
Customizing Settings for Each Managed Client	77
Customize the Specific Fault Rules	77
Customize the Triggers	81
Add or Modify a Trigger	85
Advanced Functions	87
Deactivate a Configuration Center	88
Deactivate a Communication Gateway	91
View or Modify the Configuration Center Settings	92

4. Managing Incidents

In This Chapter	96
-----------------	----

Contents

View Incidents and Collected Data	97
View Data Collected for a Particular Incident	102
Establish Data Filter Settings	104
View an Incident Summary Report.	108
About the Incident Summary Report.	109
Submit Incidents on Hold	112
Change Your Filter Settings	113
Submit a System Assessment	116
Manually Submit an Incident	118
View or Modify Incident Deletion Settings.	122

5. Incident Analysis Reports

In This Chapter	126
Access the Self-Healing Services Support Web Site.	127
Use the Incident Manager	129
Find an Incident Analysis Report	132
The Incident Analysis Report	137
Incident Summary	138
Detailed Incident Analysis Report.	140
Product Configuration Analysis	140
Patch Analysis	142
Document Analysis	146
Discussion Forum Analysis.	147
Case Management and Report Feedback Utilities	147
Open a Support Case	148
Submit Feedback to HP	154
Change the System Handle/SAID Associated with an Incident	159
View Your Support Contract Information.	162
Metric Reports	167
View your metric reports	168
Create a metric report	169
Copy a metric report	169
Delete a Metric Report	170
Download Client Software.	171
Your Self-Healing Services Sign-In Information	173
About HP Passport.	174

6. Understanding Service Notifications

In This Chapter	180
Welcome to Self-Healing Services Notification.	181
Report Available Notification	182
Entitlement Action Required Notification	183
Additional Data Requested Notification.	187
Additional Data Received Notification	188
Metric Report Available Notification	189

7. Troubleshooting Information

Understanding Potential Problem Locations	192
Self-Healing Services Process	192
Diagnosing a Problem Using E-Mail Messages	194
Diagnosing a Problem Using Error Messages	196
Diagnosing a Problem Using Other Indicators	200
Collecting Information for HP Support.	204

A. Scripts

Available Scripts	206
-------------------------	-----

B. Log Files

Available Log Files	210
---------------------------	-----

C. Data Collected

Data Collected by Self-Healing Services.	214
System Information Collected	214

Support

You can visit the HP OpenView support web site at:

<http://www.hp.com/managementsoftware/support>

HP OpenView 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
- Download software patches
- Submit and track progress on support cases
- 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 log in. Many also require a support contract.

To find more information about access levels, go to:

http://www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

<http://www.managementsoftware.hp.com/passport-registration.html>

In This Guide

This guide describes HP OpenView Self-Healing Services. It includes an overview of the architecture and operation of Self-Healing Services, as well as detailed instructions for customizing and using this product in your environment.

Audience

The audience for this guide is IT administrators. To understand and use the information in this guide, the reader must have the following background:

- Understands and has a working knowledge of UNIX[®] commands
- Understands and has a solid working knowledge of Windows[®] operating systems
- Understands networking concepts and language
- Understands the function and operation of one or more of the HP OpenView applications supported by Self-Healing Services.
- Understands the HP OpenView support process and has an HP support contract system handle or service agreement identifier (SAID)
- Is familiar with HP Instant Support Enterprise Edition (ISEE)
- Understands network security issues

Conventions

The following typographical conventions are used in this guide.

Font	What the Font Represents	Example
<i>Italic</i>	Book or manual titles, and manpage names	See the <i>HP OpenView Self-Healing Services Installation guide</i> for more information.
	Provides emphasis	You <i>must</i> follow these steps.
	Specifies a variable that you must supply when entering a command	Run the command: swinstall <fileName>
	Parameters to a method	The <i>assigned_criteria</i> parameter returns an ACSE response.
Bold	New terms	The distinguishing attribute of this class...
Computer	Text and items on the computer screen	The system replies: Press Enter
	Command names	Use the <code>grep</code> command ...
	Method names	The <code>get_all_replies()</code> method does the following...
	File and directory names	Edit file <code>/opt/hp/config/datamon.xml</code>
	Process names	Check to see if <code>cron</code> is running.
	Window/dialog box names	In the <code>Test and Track</code> dialog...
	XML tag references	Use the <code><DBTable></code> tag to...
Computer Bold	Text that you must type	At the prompt, type: ls -l
Keycap	Keyboard keys	Press Return .
Button	Buttons on the user interface.	Click Delete .
Menu Items	A menu name followed by an arrow (→) means that you select the menu and then the item.	Select Locate→Objects→by Comment

Self-Healing Services Terms

The following terms are used throughout the Self-Healing Services documentation. The definitions shown here apply *only* in the context of Self-Healing Services and do not apply to other HP OpenView software applications.

System Role	Software Hosted	Function
configuration center	Self-Healing Services client	<p>A configuration center provides the interface that you use to specify the configuration settings for the Self-Healing Services client software. These configuration settings are then automatically retrieved from the configuration center by the individual managed clients and communication gateways assigned to it.</p> <p>Multiple managed clients and communication gateways can be assigned to a single configuration center.</p>
communication gateway	Self-Healing Services client and Instant Support Enterprise Edition (ISEE) client	<p>A communication gateway receives collected data from one or more managed clients and sends that data to HP through a secure ISEE connection.</p> <p>This system must have internet access (or internet access by web proxy).</p> <p>A communication gateway is assigned to one and only one configuration center. Multiple managed clients can be associated with a single communication gateway.</p>
managed client	One or more HP OpenView software applications supported by Self-Healing Services—such as Network Node Manager (NNM), OpenView Operations (OVO), or Service Desk—and a Self-Healing Services client	<p>A managed client detects faults in supported applications (and the Self-Healing Services client), collects data, provides fault notification, and generates incident summary reports.</p> <p>A managed client is assigned to one and only one configuration center. A managed client can be associated with more than one communication gateway.</p>

NOTE

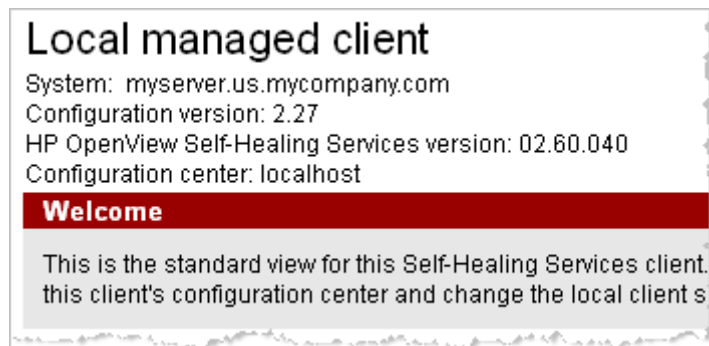
Individual systems can play multiple roles in the Self-Healing Services environment. Because communication gateways and configuration centers host the Self-Healing Services client, for example, they also serve as managed clients. If a configuration center hosts the ISEE client, it can also serve as a communication gateway. A single system can, in fact, play all three roles.

Installation Directories

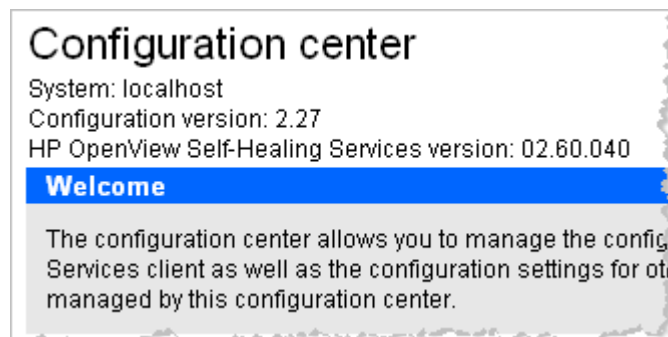
Variable Used	Description and Default Locations
<code><installDir></code>	Application directory chosen during installation. Windows default: C:\Program Files\HP OpenView UNIX default: /opt/OV
<code><dataDir></code>	Data directory chosen during installation Windows default: C:\Program Files\HP OpenView\data UNIX default: /var/opt/OV

What's New in Version 2.60

- The Self-Healing Services version 2.60 client uses the Jetty 6.0.1 web container instead of Tomcat. This results in several advantages over earlier clients:
 - Only a Java runtime engine (JRE) is required for version 2.60. Earlier versions required the much larger Java development kit (JDK).
 - Installation complexity is reduced.
 - The version 2.60 client uses less memory.
 - The probability of port conflicts with other applications is reduced.
 - Other unwanted interactions with HP OpenView applications are also reduced.
- Integration with HP OpenView products is also improved and expanded, and problems associated with earlier versions have been corrected.
- Each of the two user interface views for the Self-Healing Services client, the Local Managed Client view and the Configuration Center view, now has its own accent color. The Local Managed client pages use red accents:



The Configuration Center pages use blue accents:



This makes it easier to determine which view you are using at any given time.

1 Introduction to Self-Healing Services

This chapter presents an overview of HP OpenView Self-Healing Services. It begins with an introduction to software fault management and concludes with a description of the capabilities, structure, and operation of Self-Healing Services.

In This Chapter

This chapter provides an introduction to HP OpenView Self-Healing Services. It contains the following topics:

- “About Self-Healing Services” on page 19
- “An Overview of Software Fault Management” on page 20
- “What Is Self-Healing?” on page 21
- “What is HP OpenView Self-Healing Services?” on page 23
- “Self-Healing Services Roles” on page 25
- “Self-Healing Process” on page 29

About Self-Healing Services

HP OpenView Self-Healing Services provides the following functions for HP OpenView applications that offer full Self-Healing Services support:

- Rapid, automated management software fault detection
- Data collection at the time fault occurs
- Automated problem analysis and recommendations
- Automated patch analysis
- Efficient support case initiation

Self-Healing Services also allows you to *manually* submit a software fault to HP for applications that offer either full or basic Self-Healing Services support. In this case, Self-Healing Services provides automated problem analysis and recommendations, automated patch analysis, and efficient support case initiation as well.

See the Self-Healing Services web site for a list of applications that offer full or basic Self-Healing Services support:

http://support.openview.hp.com/self_healing.jsp

You must properly install and configure the Self-Healing Services client on your management server or agent according to the instructions provided in the *HP OpenView Self-Healing Services Installation Guide* before you can customize or use Self-Healing Services.

IMPORTANT

Do not install Self-Healing Services on a remote console. It is only supported on management servers and agents.

NOTE

A web browser must be installed on any machine from which you will access your Self-Healing Services client. The minimum requirements are Microsoft® Internet Explorer 6.0 (or later) or Netscape 7.0 (or later).

The web browser does not need to be installed on all systems that host the Self-Healing Services client. It can be installed anywhere there is connectivity to the Self-Healing Services managed environment.

Windows 2000 systems **MUST** have Internet Explorer 6.0 (or later) installed.

An Overview of Software Fault Management

The life cycle of a software fault often generates lively debate about how the break/fix process should be handled. How it is handled today often reflects the technological history of a given organization. Some organizations have a rich collection of tools to capture, analyze, and fix problems that occur in the production environment. Others simply keep track of the fact that a problem occurred and restart the production system in question, hoping that the problem will not recur. More sophisticated organizations have implemented a software management framework, such as HP OpenView Operations (OVO) and Network Node Manager (NNM), to mechanically watch the infrastructure, services, and applications that make up the modern data center.

Management Framework

The correct and consistent operation of products such as OVO and NNM has, in fact, become critical to ensuring IT success for many organizations. Such management frameworks have become so ingrained in the operating model that a framework failure constitutes a critical service failure. These kinds of failures are extremely difficult to capture and analyze, and pinpointing the root causes can be frustrating and expensive. It has therefore become necessary to manage the management software.

Fault Detection & Problem Analysis

In the traditional model, software faults are detected by people. Those people then contact the software manufacturer, describing the fault and the series of events that led up to the fault. The support engineer then asks the customer to collect a significant number of artifacts (files, messages, etc.). Next, the support engineer searches a database of known problems and issues in an effort to determine if the issue is known and whether a solution exists for that issue. If the issue is known, the results are given back to the customer, often with a directive to “try this and let me know if it works.”

The process of investigating a software fault consists of three distinct phases: data collection, problem analysis, and reporting. In the traditional model, this process is inherently iterative. The data collection and analysis phases, for example, are often repeated until the problem can be reproduced and adequately characterized by the support engineer. The process is often protracted, as delay is introduced each time information is exchanged between the customer and the support engineer. The process can also be error-prone, as it relies on data that is collected manually.

Automating the Process

Self-healing is the next step in the evolutionary cycle of management. In the self-healing model, software faults are detected by both independent monitors and self-management modules in the management software itself. The detection of a fault causes the traditional fault life cycle to be initiated, but with a twist. In the self-healing model, the process of fault detection, data collection, problem analysis, and reporting is not conducted by people; it is conducted by computers.

What Is Self-Healing?

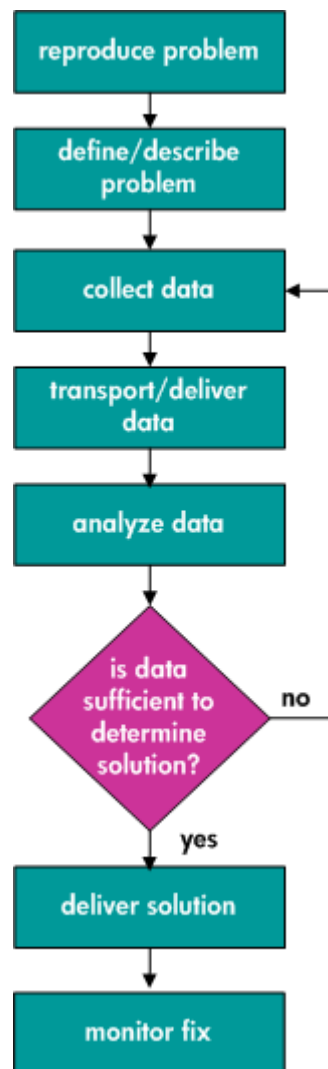
Self-healing is a process by which software and services can recognize when a failure occurs and automatically take immediate action to begin diagnosing the underlying problem. Self-healing reduces the time it takes to resolve break/fix technical issues associated with management software and proactively reduces unscheduled downtime.

When is Self-Healing Useful?

One of the most challenging aspects of network administration is troubleshooting problems with complex software applications. This often requires a call to the software provider's response center. A typical problem resolution interaction with the response center is shown in Figure 1-1.

Figure 1-1

Traditional Problem Resolution Process



This process can be inherently time-consuming and frustrating for the network administrator, as well as the support engineer, for numerous reasons:

1. Data collection does not usually begin in earnest until the support call is made.
2. Multiple data collection iterations are often required before a solution can be successfully determined.
3. The wrong data is often gathered only to be discarded later.
4. Data is no longer valid because too much time has elapsed since the failure.
5. If an escalation is required, more delay is introduced, and one or more additional data collection iterations is almost always also required.

To avoid this potential frustration, most network administrators attempt to solve problems themselves before contacting the response center. To do this, they often search available knowledge bases manually for clues to the problem's root cause and its solution.

The success of this manual process, however, relies on their ability to provide the correct keywords, in the correct combination, to the knowledge base search engine. Depending on an administrator's experience with a particular application, this can be an inefficient and sometimes fruitless process.

How Does Self-Healing Services Help?

Self-Healing Services liberates you from the frustration of the typical break/fix problem resolution process. By automating the fault detection and investigation process, Self-Healing Services increases the effectiveness and efficiency of the fault resolution process with no cost to you. These services reduce the time required to resolve technical issues associated with HP management software and work proactively to minimize unscheduled downtime.

Self-Healing Services saves you time by freeing you from having to:

- Manually search through the HP Support Knowledge Base and IT Resource Center forum messages to obtain the information you need to solve a problem yourself.
- Manually collect troubleshooting data and system information and submit it by e-mail to HP support so they can troubleshoot a problem.
- Reproduce a management software fault to collect troubleshooting data.

Self-Healing Services increases your efficiency when you are attempting to solve a problem yourself by providing you with:

- Rapid, automated detection of management software faults.
- Automated data collection of system information and data for troubleshooting at the time a fault occurs, reducing the potential for collecting inaccurate data.
- Automated transport of collected data to HP for analysis and entry into the HP Response Center database through a secure network connection called HP Instant Support Enterprise Edition (ISEE).
- Automated recording of fault metrics.
- A custom Incident Analysis Report published on a private and secure HP OpenView Self-Healing Services Support web page for each fault submitted to HP (see “The Incident Analysis Report” on page 137).

Self-Healing Services increases your efficiency when solving a problem with the assistance of an HP support engineer by:

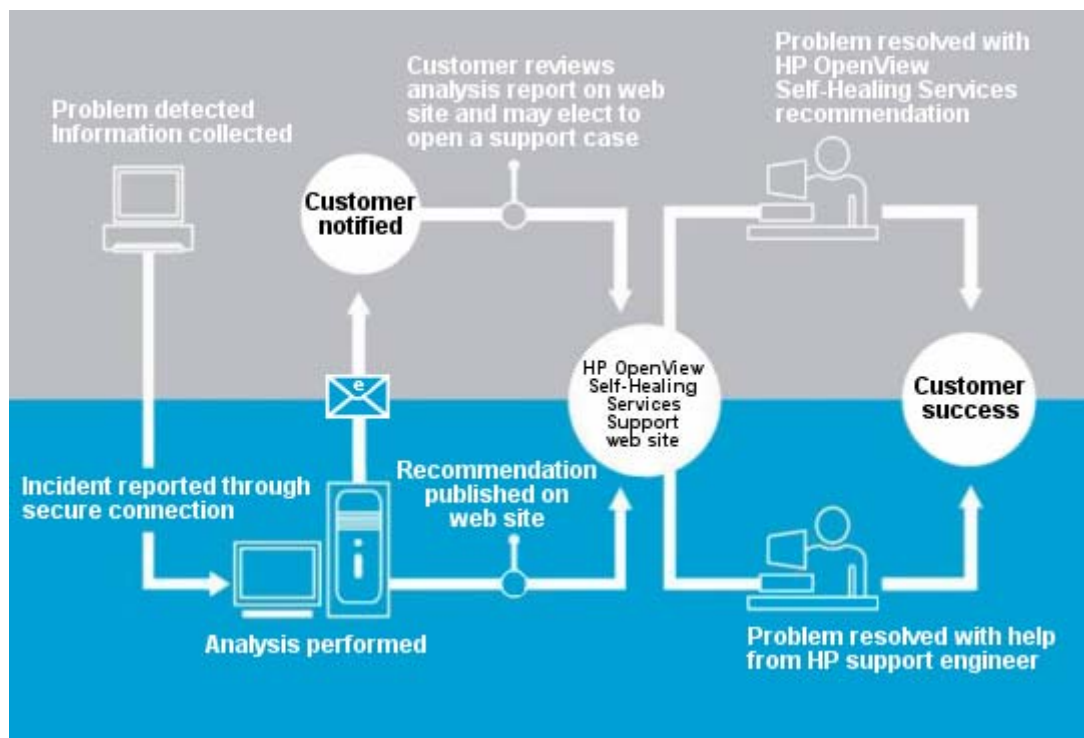
- Providing a support case submission link located at the end of each incident analysis report that electronically opens a support case when you click it.
- Providing your HP support engineer with the collected data and system information for the software fault before the support case is opened.
- Allowing you to submit additional data needed by your HP support engineer through an ISEE connection using the Self-Healing Services user interface.

What is HP OpenView Self-Healing Services?

HP OpenView Self-Healing Services is a service that significantly decreases the time and effort involved in fixing management software faults within the HP OpenView product suite by automating fault detection and much of the troubleshooting process. In effect, Self-Healing Services allows HP to manage its own management software. This leading-edge technology makes it possible for system administrators to spend less time maintaining their OpenView software and more time managing their business.

Self-Healing Services carries out four primary steps: fault detection, data collection, incident analysis, and reporting. It performs these steps automatically without intervention on your part. In most cases, your first contact with Self-Healing Services happens when you receive a notification e-mail message informing you that a problem has been detected, and an Incident Analysis Report is ready for your review. You can also trigger the Self-Healing Services process manually using the Self-Healing Services user interface.

Figure 1-2 HP OpenView Self-Healing Services



You can customize Self-Healing Services to meet the needs of your environment. You can specify which faults are submitted to HP and how often they are submitted. You can also specify how you prefer to receive fault and service notifications. To protect your security and privacy, you can instruct Self-Healing Services to remove specific data items from your incident packages before they are submitted to HP.

Self-Healing Services provides you with two types of audit output: an incident summary and individual incident reports. An incident summary enables you to quickly determine which of your Self-Healing Services nodes have submitted faults to HP or have faults on hold. Incident reports enable you to quickly determine where faults are occurring, what types of faults are occurring, and the self-healing status of each fault (received, failed, hold, ignored, submitted, or suppressed).

Self-Healing Services also provides you with an incident viewer that allows you to view the data that has been collected for each individual fault.

Self-Healing Services Roles

A Self-Healing Services managed environment includes three roles:

- Managed client
- Configuration center
- Communication gateway (optional)

Each role maps to a specific function in the environment, as shown in Figure 1-6.

A **managed client** detects faults in supported applications (and the Self-Healing Services client itself), collects data, provides fault notification, and generates incident summary reports. A managed client can only be associated with one configuration center at any given time. A managed client can, however, be associated with more than one communication gateway.

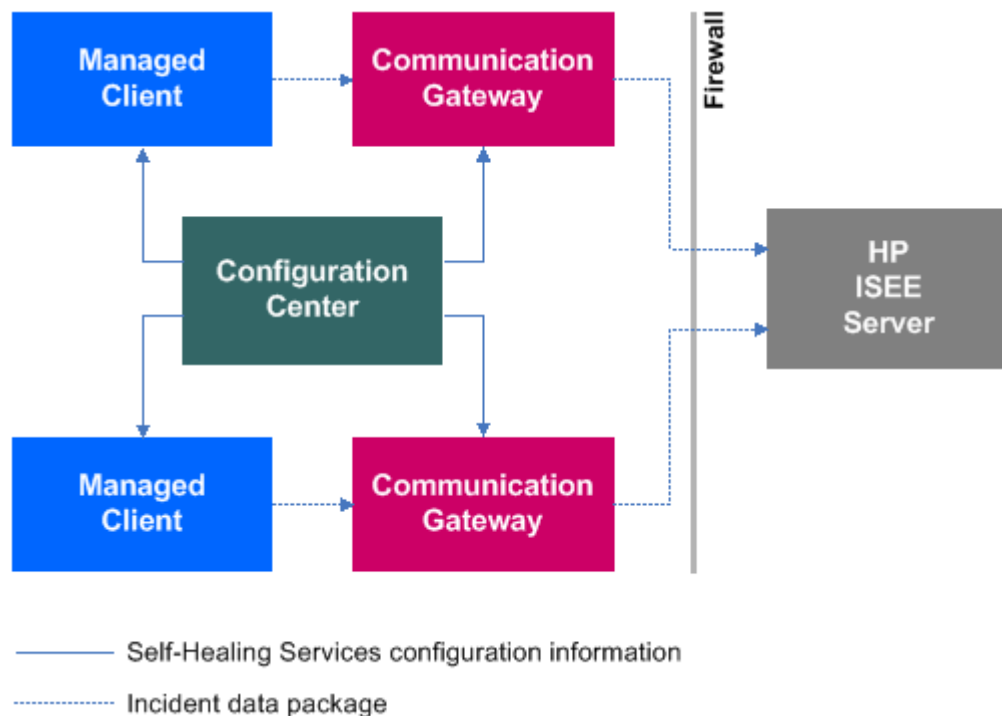
A **configuration center** provides the interface that you use to specify the configuration settings for the Self-Healing Services client software. These configuration settings are then automatically retrieved by the individual managed clients and communication gateways assigned to this configuration center. Multiple managed clients and communication gateways can be assigned to one configuration center.

The optional **communication gateway** receives data collected from one or more managed clients and sends that data to HP through a secure Instant Support Enterprise Edition (ISEE) connection. The system hosting the communication gateway must have Internet access, either directly or by web proxy. Multiple managed clients can be associated with a single communication gateway. A communication gateway can only be assigned to one configuration center at any given time. However, a Self-Healing Services managed environment can have multiple communication gateways, all assigned to a single configuration center. In fact, this is recommended for fail-over purposes. It can also have no communication gateway—in this disconnected mode, however, incidents cannot be submitted to HP for analysis.

A Self-Healing Services managed environment consists of a single configuration center with at least one managed client assigned to it. It may or may not have a communication gateway. A managed client or communication gateway can only be assigned to one configuration center.

The following diagram above is an example of a valid Self-Healing Services managed environment with one configuration center, two communication gateways, and two managed clients. The managed clients download configuration information from the configuration center at specific intervals and whenever they are restarted. Because it has a communication gateway, this environment is operating in fully connected mode.

Figure 1-3 Example of a Distributed Self-Healing Services Managed Environment

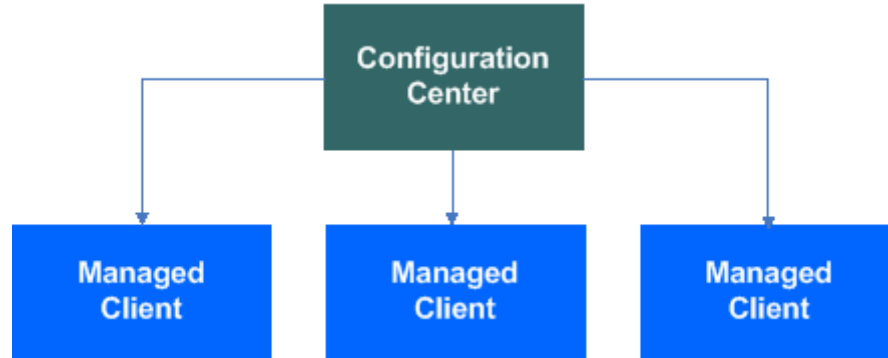


NOTE

You can have more than one configuration center in your network environment. In this case, you would be operating multiple Self-Healing Services managed environments. Each individual managed client and communication gateway, however, can only be assigned to one configuration center. In other words, a managed client or communication gateway can only belong to one Self-Healing Services managed environment at a time.

The following diagram is an example of a valid Self-Healing Services managed environment without a communication gateway. This environment is operating in disconnected mode. The managed clients download configuration information from the configuration center at specific intervals and whenever they are restarted.

Figure 1-4 Distributed Environment in Disconnected Mode



The next diagram shows three Self-Healing Services managed clients that are not connected to either a configuration center or a communication gateway. These managed clients are operating in silent mode. They can detect faults, collect data, and notify you by e-mail when a fault occurs, but they cannot submit incidents to HP for analysis. Managed clients operating in silent mode cannot retrieve configuration information from a configuration center. If you want to receive fault notifications from clients that are operating in silent mode, you must configure the e-mail server settings for those clients.

Figure 1-5 Silent Mode



Individual systems within the Self-Healing Services managed environment often play multiple roles. Because the Self-Healing Services client software is installed on them, for example, communication gateways and configuration centers also act as managed clients. Communication gateways and configuration centers perform their specific functions as well as the functions of a managed client.

Any machine that has the Self-Healing Services client installed on it becomes a managed client. The only choices you must make are whether it is also to become a configuration center, a communication gateway, or both. The following combinations are possible:

- Configuration center, communication gateway, and managed client
- Configuration center and managed client
- Communication gateway and managed client
- Managed client only

For a system to be used as a communication gateway, it must host the ISEE client and have Internet access (or Internet access by web proxy).

IMPORTANT

A Self-Healing Services managed client must be installed on a machine that serves as either a management server (in NNM or Service Desk, for example) or an agent (in OVO, for example) in order to detect faults. The Self-Healing Services client will not detect faults if it is installed on a remote console.

For a list of applications currently supported by Self-Healing Services, refer to the following web page:

http://support.openview.hp.com/self_healing_downloads.jsp

Self-Healing Process

A managed client monitors supported software applications installed on it. When a managed client detects a fault, it consults its rule configuration settings to determine if it should ignore, suppress, hold, or submit the fault for analysis (see Table 3-2 on page 77 for descriptions of these rules). If the rule configuration settings say to hold or submit the fault, the managed client immediately collects data and system information (see “Data Collection” on page 31 for details), and creates an incident package. If the rule configurations say to submit the fault, the managed client consults its filter policy settings to determine whether data should be removed from the incident package before it is submitted to HP; it then removes the specified data and sends the incident package to an available communication gateway.

The communication gateway receives the incident package and sends it to HP for analysis through a secure connection called ISEE—a multi-level, layered security structure that uses encryption, authentication, industry-standard security protocols, and best practices integrated at the physical, network, application, and operational levels to protect your systems and data. Transactions from your enterprise network to HP are restricted and tightly controlled through this single secure access point.

NOTE

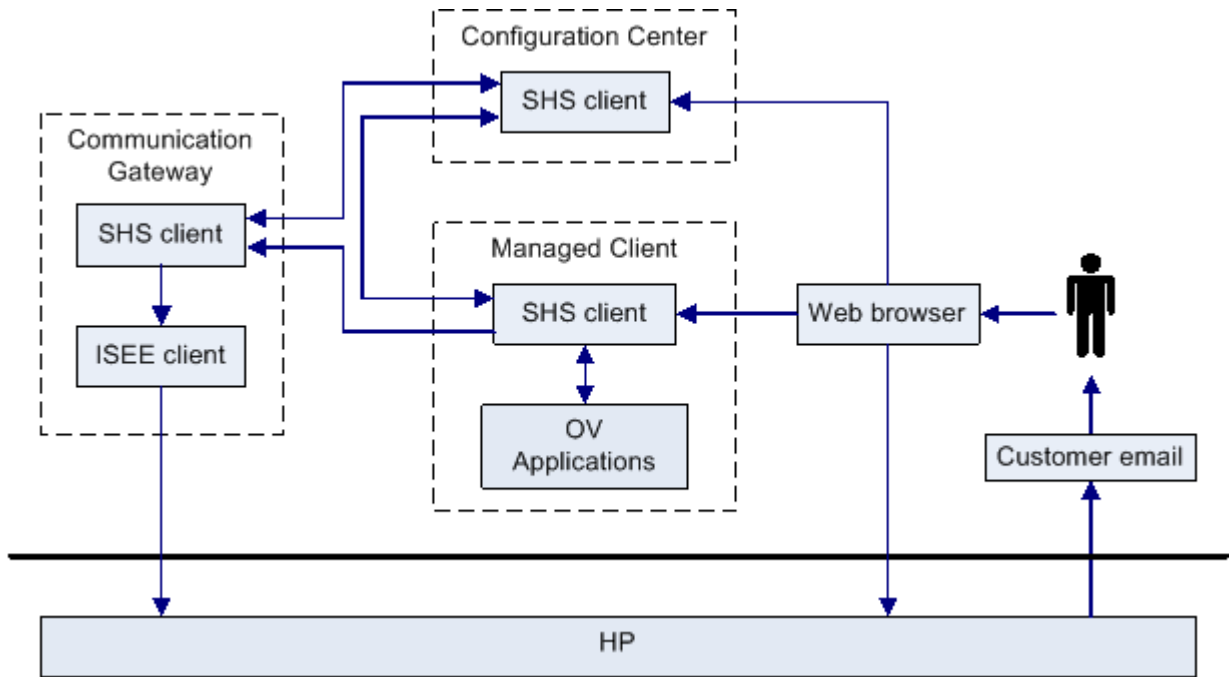
For additional information about ISEE, see the following web site:

http://www.hp.com/hps/hardware/hw_enterprise.html

When the incident package arrives at HP, the following five things happen:

1. The Self-Healing Services entitlement system determines whether the system handle/service agreement identifier (SAID) submitted with the incident package is valid.
2. If the system handle/SAID is *invalid*, Self-Healing Services sends you a service notification by e-mail with instructions about how to correct the entitlement issue. This notification includes a link to an HP OpenView Self-Healing Services Support web page where you can associate a valid system handle/SAID with this incident or investigate the status of your support agreement with HP (see “Entitlement Action Required Notification” on page 183).
3. If the system handle/SAID is *valid*, Self-Healing Services copies the incident package to an HP Response Center server for support engineer access. If you choose to open a support case, your HP support engineer will be able to immediately access this copy of the incident package.
4. Self-Healing Services analyzes the incident package (see “Analysis” on page 31) and generates a comprehensive incident analysis report. It then stores your incident analysis report on a private and protected web page on the HP OpenView Self-Healing Services Support web site.
5. Self-Healing Services sends you a service notification by e-mail containing a link that you can use to access the report (see “Report Available Notification” on page 182).

Figure 1-6 Self-Healing Services Conceptual Architecture



Data Collection

Data is collected for all faults that are not suppressed or ignored. The type and amount of data is controlled by the context of the fault and the specific application that experiences the problem. Whenever a fault is detected by the software, it passes information known as “context” to the Self-Healing Services client. This context information allows the data collector to target specific data relative to the fault. This also prevents the collection of large amounts of irrelevant data, as it focuses the collection on the problem being handled.

All collections include the base operating environment information: operating system, version numbers, and so forth. They also include a list of the applications and application patches installed on the machine. This allows for detection of missing patches, conflicting patches, and conflicting applications. If the fault originated in an HP OpenView software application that is fully integrated with Self-Healing Services, additional targeted collections are performed. These targeted collections include key data that is specific to the application. For additional information about what information is collected, see Appendix C, “Data Collected,” on page 213.

Analysis

Once your system handle or service agreement identifier (SAID) is validated, the analysis engine checks your application software patch level and determines what software patches (if any) are required to bring your system up-to-date. The analysis engine also searches the HP knowledge base and IT Resource Center (ITRC) Forums for troubleshooting and solution documents that match the problem.

If the software fault occurred on an HP OpenView Operations (OVO) management server or agent, the analysis engine performs a product configuration analysis and determines if the parameter configuration values meet the minimum required values.

Report Life Cycle

Self-Healing Services incorporates an incident analysis report life cycle process that enables you to manage your list of incident analysis reports. You can delete an incident analysis report by “closing” the incident associated with the report (see Figure 5-6 on page 138). If the closed incident is not re-opened within 90 days, the incident analysis report associated with the incident is deleted and can no longer be viewed.

Incidents associated with incident analysis reports that you have not accessed for 30 days will also be demoted to the “closed” state automatically. However, you can always access the incident analysis reports associated with closed incidents and re-open them if the need arises. If a closed incident is not re-opened within 90 days, its associated incident analysis report is deleted and can no longer be viewed.

2 The Self-Healing Services Client User Interface

This chapter describes the Self-Healing Services client user interface and how to access it from a web browser.

In This Chapter

This chapter contains the following topics:

- “Overview” on page 35
- “Start or Stop the Self-Healing Services Client” on page 36
- “Start the Self-Healing Services User Interface” on page 37
- “Local Managed Client Page” on page 39
- “Configuration Center Page” on page 44

Overview

The Self-Healing Services client includes a graphical user interface (UI) that allows you to customize its functions, view incident summary reports, and examine individual incident packages. The UI is implemented as a set of web pages and is accessible to you through your web browser. You can access the UI from any system that can successfully ping the system hosting the Self-Healing Services managed client.

The Self-Healing Services client UI has two main portal pages:

- The Local Managed Client page (provides the managed client view)
- The Configuration Center page (provides the configuration center view)

If you access a managed client or communication gateway using the UI, only the Local Managed Client page is visible. If you access a configuration center, both portal pages are visible.

You perform most of your Self-Healing Services customization by accessing the configuration center using the Self-Healing Services client UI and specifying the global configuration settings there. These configuration settings are then automatically retrieved from the configuration center by the communication gateways and managed clients assigned to it.

The two exceptions are specific fault rule configuration and filter settings. Fault rule configuration and filter settings are specific to each managed client. You can customize these settings by accessing the UI functions available from the Local Managed Client page.

Related Topics

- “Start or Stop the Self-Healing Services Client” on page 36
- “Start the Self-Healing Services User Interface” on page 37
- “Local Managed Client Page” on page 39
- “Configuration Center Page” on page 44

Start or Stop the Self-Healing Services Client

You can start or stop the Self-Healing Services client at any time as follows.

For HP-UX or Solaris operating systems:

- To start Self-Healing Services, type this command:
`<installDir>/bin/shsctrl -start`
- To stop Self-Healing Services, type this command:
`<installDir>/bin/shsctrl -stop`
- To stop and restart Self-Healing Services, type this command:
`<installDir>/bin/shsctrl -restart`
- To determine whether Self-Healing Services is running, type this command:
`<installDir>/bin/shsctrl -status`
- To view the list of possible options for the `shsctrl` script, type:
`<installDir>/bin/shsctrl -h.`

In this case, `<installDir>` is the directory where Self-Healing Services is installed on HP-UX and Solaris operating systems. By default, this is `/opt/OV`.

For Windows operating systems:

- To start Self-Healing Services, type this command:
`cscript <installDir>/bin/shsctrl.vbs -start`
- To stop Self-Healing Services, type this command:
`cscript <installDir>/bin/shsctrl.vbs -stop`
- To stop and restart Self-Healing Services, type this command:
`cscript <installDir>/bin/shsctrl.vbs -restart`
- To determine whether Self-Healing Services is running, type this command:
`cscript <installDir>/bin/shsctrl.vbs -status`
- To view the list of possible options for the `shsctrl.vbs` script, type:
`cscript <installDir>/bin/shsctrl.vbs -h.`

In this case, `<installDir>` is the directory where Self-Healing Services is installed on Windows operating systems. By default, this is `C:\Program Files\HP OpenView`.

TIP

If you start Self-Healing Services by using the `shsctrl` script, wait a moment before proceeding to allow all Self-Healing Services component processes to initialize.

Start the Self-Healing Services User Interface

After Self-Healing Services is running (see “Start or Stop the Self-Healing Services Client” on page 36), you can access its user interface (UI). In your web browser, specify the following URL:

https://<hostName>:<portNumber>/SAM

where <hostName> is the host name of the system where this Self-Healing Services client resides, and <portNumber> is the port number that the client uses for https communication. The default port number is 5814.

TIP Make sure to use https. If you use http, the UI will not open.

The web browser does not need to be on the Self-Healing Services system that you are accessing. It can be installed anywhere there is connectivity to the Self-Healing Services managed environment.

Figure 2-1 Sign-In Page

The screenshot shows the sign-in page for HP OpenView Self-Healing Services. At the top, it says 'HP OpenView Self-Healing Services' and 'Version 02.60.040'. Below this is a red horizontal bar with the text 'Sign-in information'. Underneath the bar are two input fields: 'User name' and 'Password'. To the right of the 'Password' field is a link that says 'Forgot user name and/or password?'. At the bottom right of the page is a button labeled 'Sign-In »'.

Type **admin** for both your initial user name and password. Then, click **Sign-In**. The Local Managed Client page opens, as shown in Figure 2-2 on page 39.

NOTE Your initial user name and password are established when you install the Self-Healing Services client. You can change your user name and password after you set up your configuration center.

IMPORTANT If you are signed in to the UI, and the UI is idle longer than the time-out interval, your user session times out, and you must sign in again.

Always click the **Sign-out** link to sign out of the Self-Healing Services client UI before you close the web browser window. If you do not, you will have to wait for the existing UI session to time out before you can sign in again.

The Self-Healing Services client UI allows only one user at a time for a particular host (managed client or configuration center). If a UI session is already active for that host, you will be unable to sign in. You must either sign out of the UI, or the idle time-out interval must expire before you can sign in to the UI for that host again.

The default time-out setting is 10 minutes. Anytime after you set up the configuration center, you can change the idle time-out setting on the User Name and Password page.

Local Managed Client Page

The Local Managed Client page contains links to the functions that apply to a particular managed client. This page is available when you access a managed client using the Self-Healing Services client user interface (see “Start the Self-Healing Services User Interface” on page 37).

Figure 2-2 Managed Client View

The screenshot displays the 'Local managed client' page in the HP OpenView Self-Healing Services web site. The page is divided into a left navigation menu and a main content area.

Left Navigation Menu:

- » Local managed client
 - » Contact information
 - » User name & password
 - » Notification settings
 - » E-mail server settings
 - » System assessment
 - » Communication gateways
 - » Configuration center
 - » Rule settings
 - » Trigger settings
 - » Manual incident submission
 - » Incident summary report
 - » Incident viewer
 - » Incident deletion
 - » Filter settings
- » Local managed client
- » Self-Healing Services setup
 - » Help
 - » Sign-out

Main Portal Area:

» HP OpenView Home
» Self-Healing Services web site

Local managed client
 You are currently not connected to HP. [More Info](#)
 System: myserver.us.mycompany.com
 Configuration version: 2.0
 HP OpenView Self-Healing Services version: 02.60.040
 Configuration center: Not Connected

Welcome

This is the standard view for this Self-Healing Services client. You can view this client's configuration center and change the local client settings.

<p>» Contact information</p> <p>View your primary contact information including name, telephone, e-mail address, system handle/SAID, and other information.</p>	<p>» User name & password</p> <p>View your user name and password settings.</p>
<p>» Notification settings</p> <p>View your application fault and HP service notification settings.</p>	<p>» E-mail server settings</p> <p>View your e-mail server settings.</p>
<p>» System assessment</p> <p>Generate an inventory report of your OpenView software (and associated system information) that is monitored by Self-Healing Services.</p>	<p>» Communication gateways</p> <p>View communication gateway settings.</p>
<p>» Manual incident submission</p>	<p>» Incident viewer</p>

Setup Information → (points to the HP logo and system details)

Left Navigation Menu → (points to the left sidebar menu)

Main Portal Area (indicated by a bracket at the bottom)

The Local Managed Client page includes 3 primary parts:

- The main portal area
- The left navigation menu
- The setup information

TIP

Click the **i** button to view additional information about a particular item.

Click the **Help** link in the left navigation menu to display online help.

Main Portal Area

The main portal is the portion of the Local Managed Client page that lies to the right of the left navigation menu and below the setup information. The main portal contains links to and brief descriptions of each of the functions you can perform when you access a managed client.

In Table 2-1, links to pages that are read-only are marked with an asterisk (*). The information displayed on these pages is specified and maintained on the configuration center associated with this managed client. These settings apply to all managed clients associated with this configuration center.

Table 2-1

Local Managed Client Functions

Link	Purpose
Contact information*	The information on this page includes the primary e-mail address where fault and service notifications are sent. It also includes your system handle or support agreement identifier (SAID), which must be validated before your incidents can be analyzed.
User name & password*	The information on this page includes the user name that you use to sign in to the Self-Healing Services user interface (UI) as well as the e-mail address to which your user name and password are sent if you click the Forgot user name and/or password link on the Sign-In page. It also includes the idle timeout setting for the Self-Healing Services UI.
Notification settings*	The information on this page includes the settings that determine how Self-Healing Services fault notifications are displayed in the OVO message browser and the NNM incident browser. It also includes the list of e-mail addresses to which fault and service notifications are sent.
E-mail server settings*	The information on this page shows you the e-mail server settings that are used for offline operation.

Table 2-1 Local Managed Client Functions (Continued)

Link	Purpose
System assessment	This page enables you to request a system assessment for this managed client. A system assessment is a report about the HP OpenView software installed on this managed client and all of the other managed clients, if any, assigned to the same configuration center. It offers a software inventory of the configuration center topology and updates all of the baseline information for the managed client from which it is submitted.
Communication gateways*	This page lists the communication gateways connected to this managed client and the status (up or down) of each. You can add managed clients to or delete them from the list by using the configuration center.
Manual incident submission	This page enables you to submit an incident to HP manually. This is useful if you want to test your setup, or if a particular fault is not automatically detected by Self-Healing Services
Incident summary report*	This page contains a summary of the number and types of incidents processed by Self-Healing Services on this managed client during a particular period of time.
Incident viewer	This page enables you to search for and list incidents that have occurred on this managed client. You can view all the incidents for this client, or you can view a subset that matches specific search criteria. You can view the contents of the incident package for each incident in the list as well.
Filter settings	This page lists the data items that are removed from incident packages before those packages are submitted to HP for analysis. Filter settings are established and maintained for each managed client. You can establish different filter settings for each managed client in your Self-Healing Services managed environment.

Table 2-1 Local Managed Client Functions (Continued)

Link	Purpose
Rule settings	This page enables you to establish the incident processing rule settings for this managed client. The first time a particular fault is encountered, Self-Healing Services creates a new rule by copying the settings of the default rule. Thereafter, the rule specific to this fault is applied. After a specific fault rule is created, the rule's settings can be changed, allowing the behavior for each fault to be customized. Specific fault rules are maintained on each managed client; default rules are maintained on the configuration center.
Trigger settings	This page enables you to configure a managed client to trigger fault events based on error messages that appear in HP OpenView product log files or based on error/crash files created under specific HP OpenView product directories. On Windows systems, you can also create triggers based on the Windows event log.
Self-Healing Services setup	This page enables you to run the Self-Healing Services setup function. By using this function, you can either create a new configuration center or associate this client with an existing configuration center. If the system hosting this client has HP Instant Support Enterprise Edition (ISEE) installed and running, you can also create a communication gateway
Configuration center	<p>If this managed client is connected to a remote configuration center, this page enables you to remove the association between the managed client and the configuration center. This is useful, for example, if you decide to host the configuration center on a different system.</p> <p>If this managed client is also a configuration center, this link opens the Configuration Center view of the Self-Healing Services UI.</p>

Left Navigation Menu

The left navigation menu contains links to all the functions listed on the main menu. It also contains links to the following items:

- The online help system for the Self-Healing Services UI.
- The Sign-Out page.
- The Analysis Reports page on the secure HP server.
- The software Downloads page for Self-Healing Services.

Setup Information

The setup information tells you five things:

- Whether or not this client is connected to HP through a communication gateway.

If the following message appears, this client is operating in disconnected mode:

You are currently not connected to HP.

If no message appears, this client is connected to a communication gateway.

Immediately after installation, every client is in disconnected mode because it is not yet connected to a communication gateway. When you run the Self-Healing Services setup function, you can either make this client a communication gateway—in which case the ISEE client must be installed, configured, and running on this system—or you can connect this client to a remote communication center. You can also choose to continue operating this client in disconnected mode.

- The host name of the system where this managed client resides.

This host name matches the host name you specified in the URL when you started the Self-Healing Services UI (see page 37).

- The current configuration version.

The configuration version for every client is initially 2.0. Each time the configuration settings are modified on the configuration center, the number to the right of the decimal point is incremented by 1. The first time the configuration settings change, the configuration version becomes 2.1; the twelfth time, it becomes 2.12. This happens on the configuration center.

Every update cycle (default is 24 hours), each managed client checks its own configuration version number against that of the configuration center. If the configuration version of the managed client is less than that of the configuration center, the managed client retrieves updated settings from the configuration center.

When you reset the configuration center from the Local Managed Client page, the configuration version for that managed client becomes 2.0 again.

- The version number for the client software.

In this example, the software version number is 02.60.040.

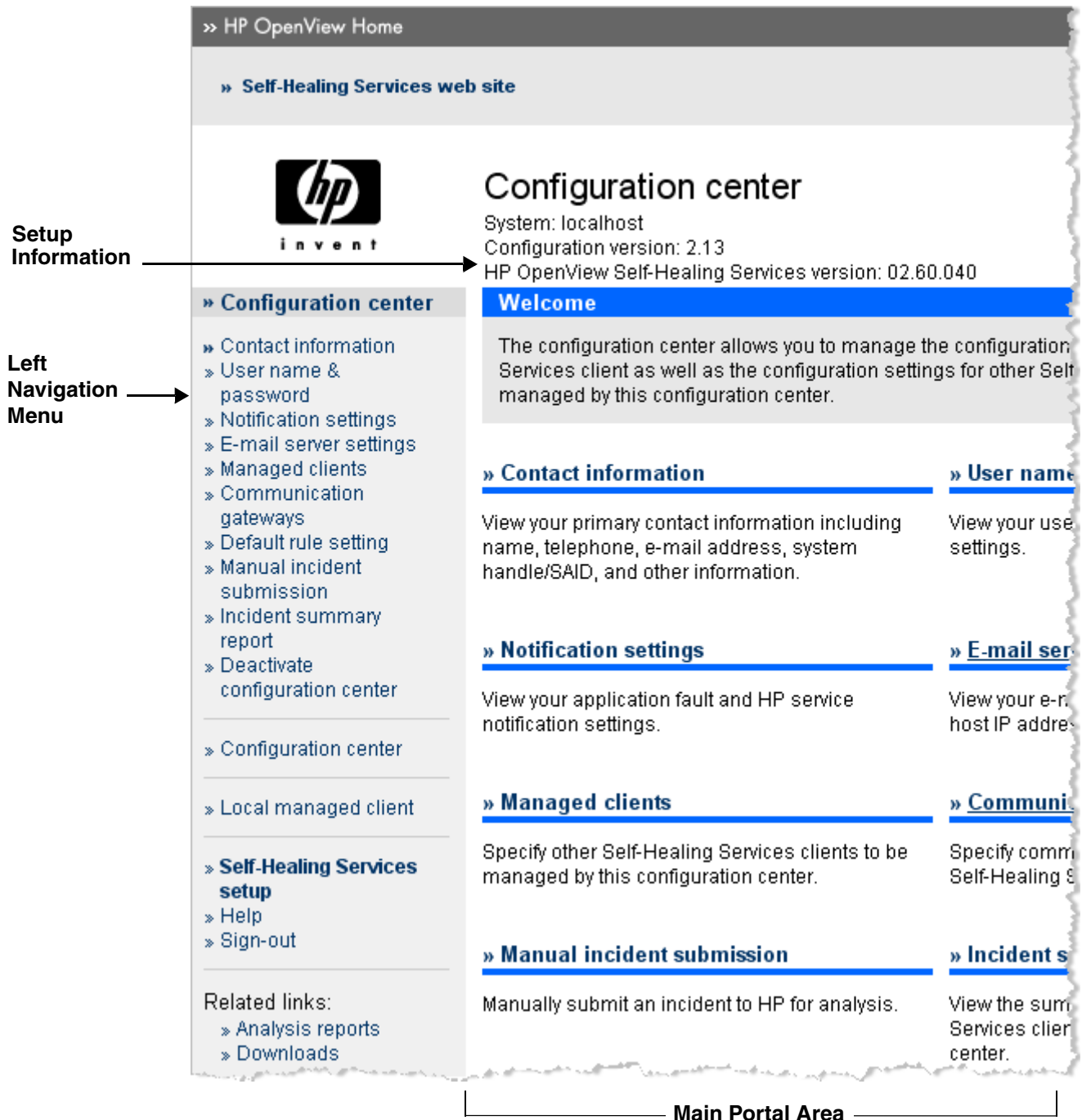
- The name of the configuration center, if any, that this managed client is connected to.

Immediately after installation, the client is not connected to a configuration center. When you run the setup function, you can either make this client a configuration center, or you can connect it to an existing configuration center. You can also choose to continue operating this client in silent mode (for additional information about silent mode, see “Self-Healing Services Roles” on page 25).

Configuration Center Page

The Configuration Center page contains links to the configuration functions that apply to all clients in the Self-Healing Services managed environment. This page is available when you access a configuration center using the Self-Healing Services client user interface (see “Start the Self-Healing Services User Interface” on page 37).

Figure 2-3 Configuration Center View



The Configuration Center main portal page includes 3 primary parts:

- The main portal area
- The left navigation menu
- The setup information

TIP

Click the **i** buttons in the Self-Healing Services UI to display additional information.

Click the **Help** link in the left navigation menu to display online help.

Always click the **Sign-out** link to log out of the Self-Healing Services client user interface before you close the web browser window. If you do not, you will have to wait for the existing session to time out before you can log on again. The time-out interval is configurable (see “Change Your User Name or Password” on page 51).

Main Portal Area

The main portal is the portion of the Configuration Center page that lies to the right of the left navigation menu and below the setup information. The main portal contains links to and brief descriptions of each of the functions you can perform when you access a configuration center.

Table 2-2 Configuration Center Functions

Link	Purpose
Contact information	This page enables you to specify your primary contact information for this Self-Healing Services managed environment. This includes the primary e-mail address where fault and service notifications will be sent. It also includes your system handle or support agreement identifier (SAID), which must be validated before your incidents can be analyzed.
User name & password	This page enables you to specify the user name and password that you use to sign in to the Self-Healing Services user interface (UI) on this system. It also enables you to specify an e-mail address to which your user name and password are sent if you click the Forgot user name and/or password link on the Sign-In page. This page is also where you establish the idle timeout setting for the Self-Healing Services UI.
Notification settings	This page enables you to specify how you want to display Self-Healing Services fault notifications in the OVO message browser or the NNM incident browser. It also enables you to specify additional e-mail addresses for fault and service notifications.
E-mail server settings	This page enables you to specify e-mail server settings for offline operation.

Table 2-2 Configuration Center Functions (Continued)

Link	Purpose
Managed clients	This page lists the managed clients connected to this configuration center. You can add managed clients to or delete them from the list by using this page.
Communication gateways	This page lists the communication gateways connected to this configuration center and the status (up or down) of each. You can add managed clients to or delete them from the list by using this page.
Manual incident submission	This page enables you to submit an incident to HP manually. This is useful if you want to test your setup, or if a particular fault is not automatically detected by Self-Healing Services
Incident summary report	This page contains a summary of the number and types of incidents processed by Self-Healing Services on all managed clients associated with this configuration center during a particular period of time.
Default rule setting	This pages enables you to establish the default incident processing rule setting: Submit, Suppress, Hold, or Ignore. The first time a particular fault is encountered, the default rule is applied.
Self-Healing Services setup	This page enables you to run the setup function, which allows you to specify the Self-Healing Services role that a particular client will play.
Deactivate configuration center	This page enables you to turn off the configuration center function for this client. This is useful if you decide to host the configuration center on another system.

Left Navigation Menu

The left navigation menu contains links to all the functions listed in the main portal area. It also contains links to the following items:

- The Local Managed Client hosted on the same system as this configuration center.
- The Self-Healing Services Setup function.
- The online help system for the Self-Healing Services UI.
- The Sign-Out page.
- The Analysis Reports page on the secure HP server.
- The software and documentation Downloads page for Self-Healing Services.

Setup Information

The setup information for a configuration center tells you four things:

- Whether or not this client is connected to HP through a communication gateway.

If the following message appears, this client is operating in disconnected mode:

You are currently not connected to HP.

If no message appears, this client is connected to a communication gateway.

Immediately after installation, every client is in disconnected mode because it is not yet connected to a communication gateway. When you run the Self-Healing Services setup function, you can either make this client a communication gateway—in which case the ISEE client must be installed, configured, and running on this system—or you can connect this client to a remote communication center. You can also choose to continue operating this client in disconnect mode.

- The host name of the system where this configuration center resides.

This host name matches the host name you specified in the URL when you started the Self-Healing Services UI (see “Start the Self-Healing Services User Interface” on page 37).

- The current configuration version.

The configuration version for every client is initially 2.0. Each time the configuration settings are modified on the configuration center, the number to the right of the decimal point is incremented by 1. The first time the configuration settings change, the configuration version becomes 2.1; the twelfth time, it becomes 2.12. This happens only on the configuration center.

Every update cycle (default is 24 hours), each managed client checks its own configuration version number against that of the configuration center. If the configuration version of the managed client is less than that of the configuration center, the managed client retrieves updated settings from the configuration center.

When you reset the configuration center from the Local Managed Client page, the configuration version for that managed client becomes 2.0 again.

- The version number for the client software.

In this example, the software version number is 02.60.040.

3

Customizing Your Self-Healing Environment

This chapter explains how to use the Self-Healing Services client user interface to customize the behavior of HP OpenView Self-Healing Services for your environment.

In This Chapter

This chapter contains the following topics:

- “Specifying Global Settings at the Configuration Center” on page 51
 - “Change Your User Name or Password” on page 51
 - “Customize the Default Rule Settings” on page 55
 - “Configure the Notification Settings” on page 57
 - “Configure the E-mail Server Settings” on page 64
 - “Change Your Contact Information” on page 66
 - “Add, Edit, or Remove Managed Clients” on page 68
 - “Add, Edit, or Remove a Communication Gateway” on page 73
- “Customizing Settings for Each Managed Client” on page 77
 - “Customize the Specific Fault Rules” on page 77
 - “Customize the Triggers” on page 81
- “Advanced Functions” on page 87
 - “Deactivate a Configuration Center” on page 88
 - “Deactivate a Communication Gateway” on page 91
 - “View or Modify the Configuration Center Settings” on page 92

NOTE

To improve the clarity of the screen images in this chapter, the left navigation menus are not shown.

Specifying Global Settings at the Configuration Center

Most of the configuration and customization that you will do for your Self-Healing Services managed environment happens at the configuration center. The purpose of the configuration center, in fact, is to be the repository for all global configuration settings. These settings are periodically retrieved by the managed clients assigned to the configuration center. Specific fault rules, filter settings, and triggers are customized for each managed client; you can customize these items by using the Local Managed Client page.

NOTE

A managed client retrieves configuration settings from its configuration center once every update cycle (24 hours by default) and whenever that managed client is restarted. See “Start or Stop the Self-Healing Services Client” on page 36 for additional information.

When you run the Self-Healing Services setup function immediately after installation, you establish most of the configuration settings for your environment. See the *HP OpenView Self-Healing Services Installation Guide* for more information about the setup function. The information in this guide pertains to changes that you make after the initial setup is completed.

Change Your User Name or Password

You can change any or all of the following settings on the User Name & Password page:

- User name
- Password
- E-mail address for forgotten sign-in information
- Idle timeout setting

When you install Self-Healing Services, your initial user name and password are both set to `admin`. Be sure to change your initial user name and password to make your Self-Healing Services installation more secure.

The e-mail address shown in the **Current e-mail address** box is where Self-Healing Services sends your user name and password if you click the **Forgot user name and/or password** link on the Sign-In Information page. If the **Current e-mail address** box is blank, and you do not specify an e-mail address, this information is sent to the e-mail address specified on the Contact Information page for this configuration center.

The idle time-out setting specifies the time, in minutes, after which the system should automatically sign out an inactive user. This is also the time that you must wait to sign in to the Self-Healing Services UI again if you close its browser window without first signing out. Changes to this setting do not take effect until Self-Healing Services is restarted.

The required field indicator (*) applies only within a particular setting. For example, if you want to change your password but not your user name, you do not need to specify anything in the **New user name** box even though it is marked as a required field.

Figure 3-1 Configuration Center—User Name & Password

User name & password

Instructions

This form allows you to change your user name, password, and confirmation e-mail address. If you forget your user name or password, Self-Healing Services can send that information to the confirmation e-mail address that you specify. You can also change the idle timeout from this form. This is the amount of time, in minutes, after which the system will automatically sign-out an idle session. Click the "Cancel" button if you do not want to save your changes. Click the "Save" button to update your information.

* = required fields (Note: Each section on this screen has its own required fields, which are only required by that section. You can leave the required fields blank in sections you are not changing.)

E-mail address information

Enter the e-mail address to which you want your user name and password sent if you forget this information.

Current e-mail address jsmith@mycompany.com

New e-mail address

User name information

Current user name admin

New user name*

Password information

Current password*

New password*

Re-type new password*

Idle timeout

Enter the time, in minutes, after which the system should automatically sign-out an inactive user (the new value will not take effect until the system is restarted).

Current idle timeout 10 minutes

New idle timeout minutes

To access the User Name & Password page:

1. Start and sign in to the Self-Healing Services user interface (UI) for the configuration center.

To change any of the settings on the User Name & Password page, you must access the configuration center. This page is read-only for managed clients.

2. In the left navigation menu, click **User name & password**.

To change your user name, password, e-mail address or idle timeout setting:

1. To change your e-mail address for sign-in information, type a different e-mail address in the **New e-mail address** box.
2. To change your user name, type the new user name in the **New user name** box.
3. To change your password, follow these steps:

- a. In the **Current password** box, type your existing password.
- b. In the **New password** box, type your new password.
- c. In the **Re-type new password** box, type your new password again.

4. If you want to change the idle timeout setting, type the new timeout duration (in minutes) in the **New idle timeout** box.

If you specify a new idle timeout period, the change will not take effect for the configuration center until you restart Self-Healing Services. It will not take effect for the managed clients assigned to the configuration center until they update their configuration information.

5. Click **Save**. Your changes are saved and can then be shared with the managed clients assigned to the configuration center that you are working with.

If you want to return to the main Configuration Center page without saving your changes, click **Cancel**.

TIP

You can change your user name, password, e-mail address, or idle timeout setting independently. Simply leave the text fields empty for the fields that you do not want to change.

Each of the sections on this page has its own required fields, which are required only when changing the settings in that section.

Customize the Default Rule Settings

Self-Healing Services detects software faults on the managed client systems where it is installed. When it detects a fault, Self-Healing Services consults the fault rules for that particular fault to determine whether to submit, suppress, hold, or ignore the fault. It then performs the action specified in the rule.

Table 3-1

Setting:	Action:
Submit	Self-Healing Services collects context-specific troubleshooting and system data at the time that the fault occurs and places the data in an incident package. The incident package is then immediately processed based on the filtration settings for that managed client and sent to the communication gateway. The gateway submits the incident to HP via ISEE.
Suppress	Self-Healing Services determines whether the same fault was already submitted to HP within the selected suppression time period. If it was, the fault is ignored (see Ignore). If it was not, the fault is submitted (see Submit). Only one instance of the fault is submitted for each increment of the suppression time period. The default suppression time period is 8 hours.
Hold	Self-Healing Services collects context-specific troubleshooting and system data at the time the fault occurs and places the data in an incident package. The incident package is then held until you explicitly release it to be submitted to HP (see Submit).
Ignore	No action is taken.

There are two types of rules: specific fault rules and the default rule. The first time a particular fault is encountered on a managed client, Self-Healing Services creates a new rule for that fault by copying the settings of the default rule. Thereafter, the rule specific to this fault is applied. After a specific fault rule is created, the rule's settings can be changed, allowing the behavior for each fault to be customized. Specific fault rules are maintained on each managed client; default rules are maintained on the configuration center. Specific fault rules are derived in one of two ways:

- They are created when a specific type of fault is detected at least once on a managed client.
- They are provided with Self-Healing Services (only for managed clients).

You can customize the fault rules on each of your managed clients to meet the needs of your environment. To do this, use the Local Managed Client page in the Self-Healing Services user interface. Each managed client has its own set of specific fault rules.

NOTE

The default rule settings for a configuration center are automatically retrieved by the managed clients assigned to it. The managed client default rule settings are overwritten by the configuration center default rule settings.

Figure 3-2 Configuration Center—Default Rule Setting

Default rule setting

Default rule

Action: Hold

Suppression Time: 0 Hours 0 Minutes

Cancel » Save »

To access the Default Rule Setting page:

1. Start and sign in to the Self-Healing Services user interface (UI) for the configuration center.
2. In the left navigation menu, click **Default rule setting**.

To configure the default rule settings:

1. In the left navigation menu, click **Rule configuration**.
2. From the **Action** list, choose the default rule action that you want to use: **Hold**, **Suppress**, **Submit**, or **Ignore** (see rule settings).

TIP

If you set the default rule action to **Hold**, you can manually remove (filter out) specific data from every incident package before it is submitted to HP. This ensures that sensitive data, not already removed from each incident package by your filter settings, is not submitted to HP.

3. If you chose **Suppress** as the default action, specify the suppression time in hours and minutes. The minimum suppression time is 1 minute; the maximum is 23 hours and 59 minutes.
4. Click **Save**.

Configure the Notification Settings

There are two types of notifications that Self-Healing Services provides: fault notifications and service notifications.

A **fault notification** occurs when a fault is either submitted to HP or placed on hold. The locally installed Self-Healing Services client will e-mail fault notifications to you and anyone else that you specify. However, you must first configure both your notification settings, as described below, and your e-mail server settings (see “Configure the E-mail Server Settings” on page 64) on the configuration center.

In addition to e-mail, you can receive fault notifications from Self-Healing Services through your HP OpenView Operations (OVO) or Network Node Manager (NNM) browser.

NOTE

Self-Healing Services does not support OVO message browser notification on Windows operating system. This feature is only available on HP-UX and Solaris operating systems.

A **service notification** occurs when one of the following things happens:

- You perform a connectivity test.
- An incident is submitted to HP through Self-Healing Services.
- A fault is submitted to HP with an invalid system handle/SAID.
- You upload additional data for an open support case and submit it to HP through Self-Healing Services.

The Self-Healing Services server at HP will e-mail service notifications to you by default when one of these events occurs. If you want anyone else to also receive copies of your service notifications, you must add their e-mail addresses to the list of recipients. See “Understanding Service Notifications” on page 179 for additional information.

Figure 3-3 **Fault Notification Example**

```
From: HP OpenView Software Support  
[mailto:openview-self-healing@hp.com]  
Sent: Saturday, December 02, 2006 12:22 PM  
To: Smith, John  
Subject: Report Available: "Test 1" - HP OpenView Self-Healing  
Services  
  
This message has been automatically generated. Please do not reply  
to this message.  
  
Your recently submitted HP OpenView Self-Healing Services incident  
has been analyzed, a report has been generated and it is available  
on the HP OpenView Support web site. Please view your HP OpenView  
Incident Analysis Report at the following web address (HP Passport  
sign-in & active support contract required):  
  
-  
http://support.openview.hp.com/software/analysis/report?incident=000000000000-00000000-0000000000-000000000000  
  
After you sign-in with an HP Passport account, you may need to  
provide the HP OpenView Support system handle / service agreement  
identifier (SAID) which was used to submit the incident. You can  
find this system handle / SAID in the HP OpenView Self-Healing  
Services client contact information located on the system from  
which this incident was submitted.  
  
This report will provide you with customized information and  
assistance to help you solve your software difficulties and keep  
your systems running smoothly. In the event that you require  
personal assistance, you will also be able to create a support  
case for this incident from the incident analysis report.  
  
Incident Summary:  
  
Date/Time:            Dec 2, 2006 7:15:09 PM GMT  
System name:         myserver.us.mycompany.com  
Product:             Self-Healing Services  
Incident ID:         000000000000-00000000-0000000000-000000000000  
Short description: Test 1  
  
Problem Detail:  
  
This will test the submission path and notification flow.  
  
Thank you,  
HP OpenView Self-Healing Services Team
```

Figure 3-4 Service Notification Example

```
From: HP OpenView Software Support
[mailto:openview-selfhealing@hp.com]
Sent: Sunday, December 03, 2006 08:35 AM
To: Smith, John
Subject: Additional Data Requested for Support Case - HP Open View
Self-Healing Services

This message has been automatically generated. Please do not reply
to this message.

HP Software Support is requested additional data from you with
regard to the support case (SampleCaseID) that you submitted for
incident 000000000000-00000000-0000000000-000000000000. Please
view the additional data request and the instructions on how to
submit any data files at the web address below (HP Passport sign-
in & active support contract required):

- http://support.openview.hp.com/software/analysis/report?inc
ident=000000000000-00000000-0000000000-000000000000

Support Case Summary:

Date/Time:          December 3, 2006 12:02:55 AM GMT
Support Case ID:    SampleCaseID
Title:              Sample Support Case

Incident Summary:

Date/Time:          December 2, 2006 5:01:46 PM GMT
System name:        myserver.us.mycompany.com
Product:            network node manager
Incident ID:        000000000000-00000000-0000000000-
000000000000
Short description:  File does not exist

Problem Detail:

File does not exist.

Thank you,
HP OpenView Self-Healing Services Team
```

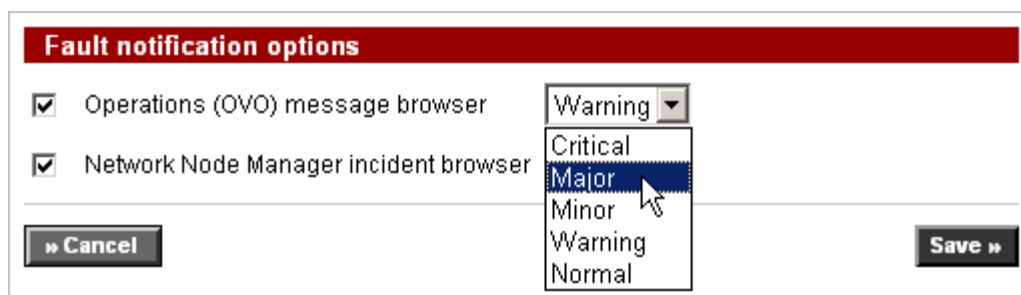

To configure OVO or NNM to receive fault notifications:

1. In the **Fault notification options** section, select one or both of the following fault notification options:

- Operations (OVO) message browser (not available on Windows systems)
- Network Node Manager incident browser

By default, if OVO or NNM is installed on this system, browser notification is turned on. To turn it off, clear the check box.

2. For each browser that you selected in step 1, choose the fault severity that you want Self-Healing Services to assign to the fault notification: Critical, Major, Minor, Warning, or Normal.



3. Click **Save**.

NOTE

Self-Healing Services does *not* verify which HP OpenView applications are installed on your system. If you select the OVO message browser check box or the NNM incident browser check box, make sure the respective application is installed and running on this system. If you select the OVO message browser check box, also be sure that OVO is configured to send messages to the OVO management server.

To add an e-mail address to the notifications list:

1. Click **Add E-mail Address**.

Add notification e-mail address

Add e-mail address for notification

* = required fields

E-mail address*

My e-mail client accepts UTF-8 [More info](#)

Country/Region*

Notification type Fault notification Service notification

Cancel » **Save »**

2. In the **E-mail address** box, type the e-mail address to which you want Self-Healing Services to send notifications.
3. Select the country to which this e-mail will be delivered.
4. If your e-mail client does not accept UTF-8 encoding, clear the **My email client accepts UTF-8** box.

Most mail readers do support UTF-8 encoding. If this box is not selected, e-mail will be sent using US-ASCII encoding, which only supports United States (US) based characters.

5. *Optional:* Select **Fault Notification** if you want the Self-Healing Services client to notify this individual by e-mail when an incident package is submitted to HP or placed on hold.
6. *Optional:* Select **Service Notification** if you want the Self-Healing Services server to send service notifications from HP to this individual.
7. Click **Save**. The **Notification settings** page is displayed again, and the list now includes the e-mail address that you just added.

Repeat these steps to add another e-mail address.

To change the notification type settings for one or more e-mail addresses in the list:

1. On the Notification Settings page, select **Fault Notification**, **Service Notification**, or both for each e-mail address in the list:

Fault notification & HP service notification e-mail addresses

Fault notification e-mails are sent from the Self-Healing Services client when a fault is detected and an incident package is submitted to HP or placed on hold. HP service notification e-mails are sent from HP when an incident analysis report is available and when other key Self-Healing Services events occur.

Delete	E-mail address	Country/Region	Fault notification	HP service notification
*	jsmith@mycompany.com *	United States	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	jeanmarc@mycompany.com	France	<input type="checkbox"/>	<input checked="" type="checkbox"/>

* Primary contact cannot be deleted.

Delete Checked E-mails » **Save Checked Notifications »**

2. Click **Save Checked Notifications**.

To edit the settings for an individual e-mail address in the list:

1. On the Notification Settings page, in the **E-mail address** column, click the link for the e-mail address that you want to work with.
2. Change the settings as needed.
3. Click **Save**.

NOTE

To edit the primary contact, which is the first e-mail address listed on this page, click the **Contact information** link in the left navigation menu, and edit the information on the Contact Information page.

To delete an e-mail address from the notification list:

1. On the Notification Settings page, in the **Delete** column, select box corresponding to the e-mail address (or addresses) that you want to delete.
2. Click **Delete Checked E-mails**.

Configure the E-mail Server Settings

NOTE

The E-mail Server Settings page is read-only when you are accessing a managed client using the Self-Healing Services user interface. To change your e-mail server settings, you must access the configuration center.

If your Self-Healing Services managed environment is not connected to HP through a communication gateway, you must configure your e-mail server settings so that you can receive fault notifications. You cannot complete the setup process for a configuration center until you either establish a communication gateway or specify your e-mail server settings.

To access the E-mail Server Settings page:

1. Start and sign in to the Self-Healing Services user interface (UI) for the configuration center.
2. In the left navigation menu, click **E-mail server settings**.

To configure your e-mail server settings:

1. In the **IP Address** box, type the IP address of the SMTP mail server that will be used to send notifications from Self-Healing Services to the recipients you specify on the **Notification settings** page.
2. Choose one of the following two options:
 - In the **From E-mail Address** box, type the e-mail address that fault notifications will appear to come from.
For example, if the **From e-mail address** is `janesmith@xyz.com`, your fault notifications will appear to come from `janesmith@xyz.com`.
 - In the **E-Mail Domain** box, type the domain that fault notifications will appear to come from.
For example, if the **E-mail domain** is `xyz.com`, your fault notifications will appear to come from `HP_Self_Healing_Agent@xyz.com`.

NOTE

If you provide both a **From e-mail address** and an **E-mail domain**, the **From e-mail address** is used.

3. *Optional:* In the **SMTP Port** box, specify the SMTP port on which the SMTP mail server is listening; the default is port 25.
4. *Optional:* In the **Retry Frequency** box, type the number of times that Self-Healing Services will attempt to connect to the SMTP mail server; the default is 3 attempts.
5. *Optional:* In the **Socket Timeout** box, specify the length of time in minutes after which a time-out will occur on the socket connection to the SMTP mail server; the default is 5 minutes.
6. *Optional:* In the **Sleep Time** box, specify the length of time in minutes that Self-Healing Services sleeps between retries; the default is 3 minutes.
7. *Optional:* In the **Server Admin IP Address**, specify the administration IP address for the SMTP server; this information is normally not required.

8. Click **Save**. Your changes are saved and automatically downloaded to the communication gateways and managed clients assigned to this configuration center.

Figure 3-6

Configuration Center—E-mail Server Settings

E-mail server settings

E-mail server settings

If you want to receive fault notification e-mails sent from your Self-Healing Services clients, enter your e-mail server settings below. This is recommended when your Self-Healing Services clients are not connected to HP through a communication gateway. Click 'Save' to save your information. Click 'Cancel' to disregard the settings you entered.

* = required fields
** = one of these fields is required

IP address*	<input type="text" value="99"/> . <input type="text" value="99"/> . <input type="text" value="99"/> . <input type="text" value="99"/>
From E-mail address**	<input type="text" value="disconnected@mycompany.com"/>
E-mail domain**	<input type="text"/>
SMTP port*	<input type="text" value="25"/>
Retry frequency*	<input type="text" value="3"/>
Socket timeout*	<input type="text" value="5"/>
Sleep time*	<input type="text" value="3"/>
Server admin IP address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>

Change Your Contact Information

NOTE

The Contact Information page is read-only for managed clients and communication gateways. You can only change your contact information on a configuration center.

You can, however, perform a connectivity test from the Contact Information page on a managed client or a communication gateway. Click Send Connectivity Test to perform this test.

When you create a configuration center using the Self-Healing Services setup function, you must provide your contact information. You can change or add to your contact information for that configuration center at any time thereafter. After you update your contact information on a configuration center, the information is shared with all managed clients and communication gateways associated with that configuration center.

To enter your contact information, type or paste the information in the boxes provided. Boxes marked with an asterisk (*) are required.

Figure 3-7 Contact Information Page

Contact information

Primary contact information

Enter your primary contact information below. Click 'Save' to save your information. Click 'Cancel' to disregard the information you entered.

* = required fields

Prefix	<input type="text"/>
First name*	<input type="text" value="John"/>
Last name*	<input type="text" value="Smith"/>
Suffix	<input type="text"/>
To e-mail address*	<input type="text" value="jsmith@mycompany.com"/>
	<input checked="" type="checkbox"/> My e-mail client accepts UTF-8 More info
Telephone*	<input type="text" value="1-800-555-1234"/>
Company/Organization*	<input type="text" value="My Widget Company"/>
Country/Region*	<input type="text" value="United States"/>
System Handle/SAID*	<input type="text" value="MYCOMPANY2007"/> More info

System handle/SAID is case sensitive.

To change your contact information:

1. In the configuration center view, click the **Contact information** link in the left navigation menu. The **Contact Information** page opens (see Figure 3-7 on page 67).
2. Change your contact information as needed. Items marked with an asterisk (*) are required.
3. If your e-mail client does not accept UTF-8 encoding, clear the **My e-mail client accepts UTF-8** check box. Most mail readers do support UTF-8 encoding. If this check box is not selected, e-mail will be sent from HP using US-ASCII encoding, which only supports United States (US) based characters.
4. In the **System Handle/SAID** box, type your system handle or service agreement identifier (SAID).

IMPORTANT

Your system handle/SAID is case-sensitive. If you change this field, Be sure to type your customer-specific HP OpenView application system handle/SAID exactly as it appears in your support contract with HP.

If you type it incorrectly, all your faults that get submitted to HP will fail the entitlement check, and you will have to manually re-associate each incident submitted with a valid system handle/SAID to resolve the entitlement check failure. See “Entitlement Action Required Notification” on page 183 for details.

5. Choose one of the following options:

- To save your changes without performing a connectivity test, click **Save**.
- To save your changes and then perform a connectivity test for the configuration center, click **Save and Send Connectivity Test**.

If the connectivity test is successful, you will receive a service notification welcoming you to Self-Healing services (see Figure 6-1 on page 181). If a connectivity test fails due to an entitlement issue, you will receive a service notification from Self-Healing Services indicating that the system handle/SAID is invalid. See “Entitlement Action Required Notification” on page 183 for further information and instructions. If you do not receive either notification, see “Diagnosing a Problem Using E-Mail Messages” on page 194.

When you save your changes at the configuration center, they are automatically downloaded to the communication gateways and managed clients assigned to it.

NOTE

To perform a connectivity test for a communication gateway or managed client, follow these steps:

1. Open the Self-Healing Services UI for that client.
2. Click the **Contact information** link. The Contact Information page opens.
3. Click **Send Connectivity Test**.

Add, Edit, or Remove Managed Clients

You can add, edit, or remove managed clients assigned to a configuration center at any time using the Managed Clients page. This page lists the managed clients assigned to a configuration center (see Figure 3-8 on page 69). Because the configuration center also serves as a managed client, the configuration center appears in the list of managed clients. Because communication gateways also serve as managed clients, the communication gateways assigned to the configuration center also appear in the list. The following information is displayed for each client in the list:

- The port number for the Self-Healing Services client.
- The date on which its configuration information was last updated.
- The current configuration version.
- The number of faults it has on hold.

The configuration version for a configuration center is incremented each time you change its configuration. The configuration version for gateway and managed clients indicates the latest configuration version each node has downloaded from the configuration center.

Managed clients are automatically added to the list when you configure them during the Self-Healing Services setup process. You do not need to manually add any managed clients to the list if they were configured during setup.

Figure 3-8 Managed Clients Page

Managed clients

Displaying managed Self-Healing Services client(s) (1-2 of 2)

Click the host name value to view or edit the properties of a specific managed client.
 Click the 'Add Managed Client' button to add another client by host name and port.
 Click the 'Incidents on hold' value to view a list of incidents for a specific client.

Delete	<u>Host name</u>	Port	<u>Updated date</u>	Configuration version	<u>Incidents On Hold</u>
*	myserver.us.mycompany.com *	5814	Dec 04, 2006	2.21	0
<input type="checkbox"/>	sales.uk.mycompany.com	5814	Dec 04, 2006	2.21	3
<input type="checkbox"/>	support.asia.mycompany.com	5814	Dec 04, 2006	2.21	6

* The local client cannot be edited.

** Indicates a gateway client. This can be edited only from the communication gateway client page.

Delete Checked Client »

Add Managed Client »

TIP By default, the clients in the table are listed alphabetically by host name. You can sort the managed client table by **Host name**, **Updated date**, or the number of **Incidents on hold** by clicking the link at the top of the appropriate column.

To add a managed client to the list:

1. In the configuration center view, click **Managed clients** in the left navigation menu. The **Managed clients** page opens (see Figure 3-8 on page 69).
2. Click **Add managed client**. The **Add Self-Healing Services client** page opens (see Figure 3-9).
3. In the **Host name** box, type the host name or IP address of the managed client that you want to assign to this configuration center.
4. In the **Port** box, type **5814** for the port number—unless you will be changing the Self-Healing Services client default port number as described in the *HP OpenView Self-Healing Services Installation Guide*. In that case, use that port number instead.
5. Click **Save**.

The **Managed clients** page is displayed again (see Figure 3-8). The list now includes the managed client you just added.

NOTE

The maximum number of managed clients that can be supported by a single configuration center is 100.

A managed client can only be assigned to one configuration center. If you attempt to add a managed client that is already assigned to a configuration center, you get an error. Similarly, if you attempt to add a client that is, itself, a configuration center, you get an error.

Figure 3-9 Add Self-Healing Services Client Page

Add Self-Healing Services Client

Self-Healing Services client settings

* = required fields

Host name*

Port*

To remove a managed client from the list:

1. In the configuration center view, click **Managed clients** in the left navigation menu. The **Managed clients** page opens (see Figure 3-8 on page 69).
2. In the **Delete** column, click the check box for each node that you want to remove from the list.
3. Click **Delete Checked Client**.

Figure 3-11 Managed Clients Page with Clients Marked for Deletion

Managed clients

Displaying managed Self-Healing Services client(s) (1-2 of 2)

Click the host name value to view or edit the properties of a specific managed client.
 Click the 'Add Managed Client' button to add another client by host name and port.
 Click the 'Incidents on hold' value to view a list of incidents for a specific client.

Delete	Host name	Port	Updated date	Configuration version	Incidents On Hold
*	myserver.us.mycompany.com *	5814	Dec 04, 2006	2.21	0
<input checked="" type="checkbox"/>	sales.uk.mycompany.com	5814	Dec 04, 2006	2.21	3
<input checked="" type="checkbox"/>	support.asia.mycompany.com	5814	Dec 04, 2006	2.21	6

* The local client cannot be edited.

** Indicates a gateway client. This can be edited only from the communication gateway client page.

Delete Checked Client »

Add Managed Client »

When a managed client is removed from the list, it can still detect faults and collect data. If this managed client was configured to serve as a communication gateway prior to being removed from the list, it can continue to submit incident packages to HP for analysis. If it was not configured to serve as a communication gateway, it will be unable to submit incidents. It can no longer receive configuration setting updates from the configuration center to which it was assigned, nor can it provide the configuration center with incident summary information.

NOTE

If this managed client was configured to serve as a communication gateway prior to being removed from the list, other managed clients in the network will not learn of the removal immediately. Any managed clients that previously used this gateway to submit incidents will continue to do so until they get their next configuration update from the configuration center.

Add, Edit, or Remove a Communication Gateway

You can add, edit, or remove a communication gateway assigned to a configuration center at any time using the Communication Gateways page. This page lists the communication gateways assigned to a particular configuration center (see Figure 3-12 on page 73). If the configuration center also serves as a communication gateway, it appears in the list as well. The following information is displayed for each node in the list:

- The port number for the Self-Healing Services client.
- The date on which its configuration information was last updated.
- The current configuration version.
- Whether the node is able to send incident packages to HP (Status = Up or Down).

The configuration version for a configuration center is incremented each time you change its configuration. The configuration version for gateway and managed clients indicates the latest configuration version each node has downloaded from the configuration center.

Figure 3-12 Communication Gateways Page

Communication gateways

Displaying communication gateways (2-2 of 2)

Click the host name value to view or edit the properties of a specific communication gateway. Click the 'Add Communication Gateway' button to add another gateway by host name and port. Click a value under 'Flush' to delete the incident packages that are in the process of being submitted to HP.

Delete	Host name	Port	Updated date	Configuration version	Status
*	myserver.us.mycompany.com *	5814	Dec 04, 2006	2.22	up
<input type="checkbox"/>	sales.uk.mycompany.com	5814	Dec 04, 2006	2.22	up

* The local client cannot be edited.

Delete Communication Gateways »

Add Communication Gateway »

You can sort the communication gateway table by **Host name** or **Updated date** by clicking the link at the top of the appropriate column.

Add a Gateway

It is recommended that you assign more than one communication gateway to a configuration center for failover protection. Before you can add a new gateway to the list, the following things must be true:

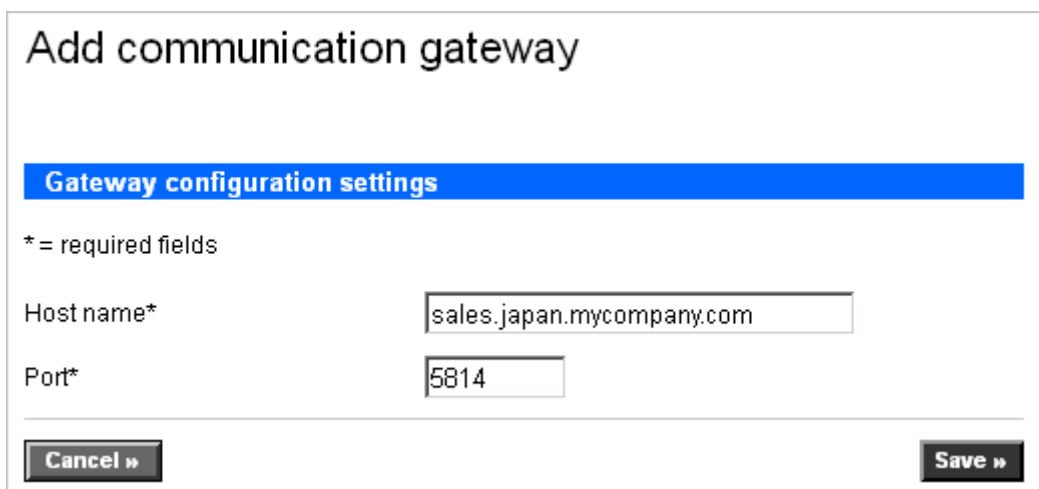
- The Self-Healing Services client is installed on that system.
- The ISEE client is installed on that system.
- You have run the Self-Healing Services setup function on that system and designated it to be a local communication gateway.

To add a communication gateway:

1. In the configuration center view, click the **Communication gateways** link in the left navigation menu. The Communication Gateways page opens (see Figure 3-12 on page 73).
2. Click **Add communication gateway**. The Add Communication Gateway page opens (see Figure 3-13).
3. In the **Host name** box, type the host name or IP address of the communication gateway that you want to assign to this configuration center.
4. In the **Port** box, type 5814 for the port number—unless you changed the Self-Healing Services client default port number as described in the *HP OpenView Self-Healing Services Installation Guide*. In that case, use the new port number instead.
5. Click **Save**.

The Communication Gateways page opens again (see Figure 3-12 on page 73). The list now includes the communication gateway you just added.

Figure 3-13 Add Communication Gateway Page



Add communication gateway

Gateway configuration settings

* = required fields

Host name*

Port*

NOTE

A communication gateway must only be assigned to one configuration center for Self-Healing Services to function correctly. The maximum number of communication gateways that can be supported by a single configuration center is 100.

Change the Port Number for a Gateway

If you change the Self-Healing Services port for a client serving as a communication gateway, you must tell the configuration center about the new port number. You can do this by using the Edit Communicate Gateway page.

To change the port number for a communication gateway already assigned to this configuration center:

1. In the configuration center view, click the **Communication gateways** link in the left navigation menu. The Edit Communication Gateway page opens.
2. Click the **Host name** link for the node with which you want to work. The Edit Communication Gateway page opens (see Figure 3-14 for an example).
3. In the **Port** box, type the new port number.
4. Click **Save**.

Figure 3-14 Edit Communication Gateway Page

Edit communication gateway

Edit communication gateway

* = required fields

Host name* sales.uk.mycompany.com

Port* 5814

« Cancel Save »

Remove a Gateway

You can remove a communication gateway from the list of gateways associated with a configuration center. When you remove a gateway from the list, it becomes unavailable to the configuration center and any other managed clients connected to that configuration center. The gateway still functions as a local gateway on the system where it is resident, however.

To remove a communication gateway:

1. In the configuration center view, click the **Communication gateways** link in the left navigation menu. The Communication Gateways page opens (see Figure 3-12 on page 73).
2. In the **Delete** column, click the check box for each node that you want to remove from the list.
3. Click **Delete Communication Gateways**.

The communication gateway removed will finish submitting to HP any incident packages it has received from the managed clients. It will no longer receive any new incident packages from the managed clients associated with the configuration center.

Customizing Settings for Each Managed Client

In addition to the global settings that you specify at the configuration center, you can establish customized local settings for each managed client in your Self-Healing Services managed environment.

Customize the Specific Fault Rules

The Self-Healing Services client detects software faults on each system where it is installed. When it detects a fault on a managed client, it consults that managed client's fault rule for that particular fault to determine whether to submit, suppress, hold, or ignore the fault. It then performs the specified action.

The default rule settings are used the first time a particular fault occurs on a managed client. From that point forward, the fault-specific rule is used whenever that particular fault occurs. The default rule settings are configured at the configuration center. Fault-specific rules are configured on each managed client.

Table 3-2

Rule Settings

Setting	Action
Submit	The Self-Healing Services client collects context-specific troubleshooting and system data at the time the fault occurs and places the data in an incident package. The incident package is then immediately processed based on the filtration rules for that managed client and sent to the communication gateway. The communication gateway submits it to HP via the ISEE client.
Suppress	The Self-Healing Services client determines if the same fault was already submitted to HP within the selected suppression time period. If it was, the fault is ignored (<i>see Ignore</i>). If it was not, the fault is submitted (<i>see Submit</i>). Only one instance of the fault will be submitted for each increment of the suppression time period. The default suppression time period is 8 hours.
Hold	The Self-Healing Services client collects context-specific troubleshooting and system data at the time the fault occurs and places the data in an incident package. The incident package is then held until you explicitly release it for submittal to HP, as described in "Submit Incidents on Hold" on page 112 (<i>see Submit</i>).
Ignore	No action is taken.

You can customize your fault rules to meet the needs of your environment. Each managed client has its own set of specific fault rules.

NOTE

A configuration center's default rule settings are automatically downloaded to the managed clients assigned to it. The default rule settings on the managed client are overwritten by the default rule settings on the configuration center each time the configuration is updated. The fault-specific rules, however, are not overwritten.

To customize the default rule settings for a configuration center:

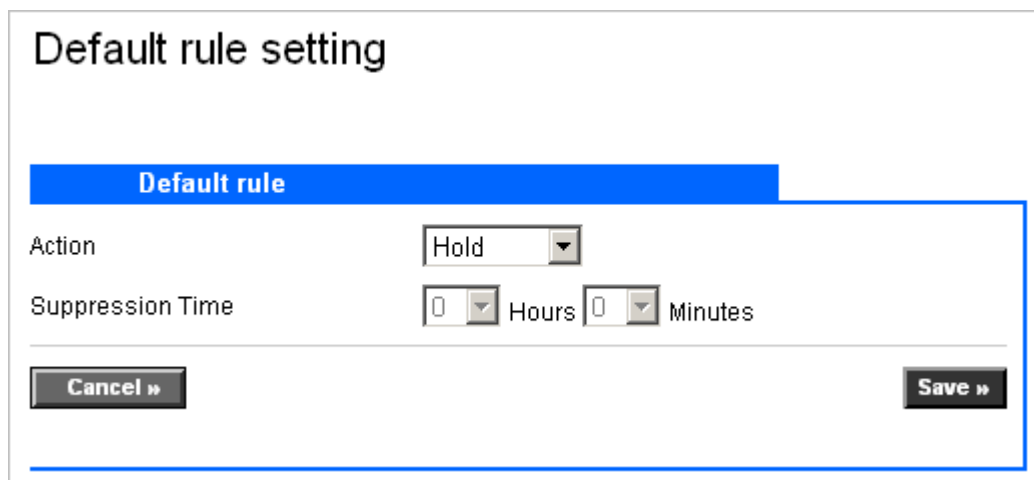
1. In the configuration center view, click **Default rule setting** in the left navigation menu.
2. From the **Action** list, select the default action that you want to use (see Table 3-2 on page 77 for action descriptions). If you select **Suppress**, specify the suppression time in hours and minutes

NOTE

Setting the default rule settings to **Hold** allows you to manually remove (filter out) specific data from every incident package generated before it is submitted to HP. This ensures that sensitive data that has not already been removed from each incident package based on your filtration policy is not submitted to HP.

3. Click **Save**.

Figure 3-15 Default Rule Setting Page for a Configuration Center



To customize the fault-specific rules for a managed client:

1. In the managed client view, click **Rule settings**.
2. The Rule Settings page is displayed (see Figure 3-16 for an example). This page has two tabs:
 - The **Default rule** tab shows the default rule settings. The default rule is automatically applied to faults the first time they are detected on this node.
3. Click the **Specific fault rule** tab.

NOTE

The default rules are configured on the configuration center. You can change the default rule settings on a managed client, but they will be overwritten whenever the configuration information is updated.

- The **Specific fault rule** tab shows the rule settings for specific types of faults that either were provided with the Self-Healing Services client or were detected at least once on this managed client. You can change the fault rule settings for a particular fault.

4. To change the fault rule settings for a single fault, follow these steps:
 - a. Click the **Rule description** link for that fault. The Edit Rule Settings page opens (see Figure 3-17).
 - b. Choose the **Action** that you want to use (see Table 3-2 on page 77). If you choose **Suppress**, specify the suppression time in hours and minutes.
 - c. *Optional:* If you want to change the rule description to be more meaningful for your environment, select the text in the **Rule Description** box, and type a new rule description.

NOTE

Rule descriptions can be anything you like. They are not referenced by the Self-Healing Services client to identify specific faults. The client identifies specific faults using the trigger IDs it assigns them (see Figure 3-16). Rule descriptions are strictly for your benefit.

- d. Click **Save**. Your changes are now visible on the Specific Fault Rule tab.
5. To change the fault rule settings for multiple faults, follow these steps:
 - a. In the **Select** column, select the check box for each fault whose rule settings you want to change.
 - b. In the **Change selected rules from above** section at the bottom of the Rule Configuration page, choose the **Action** that you want to use (see Table 3-2 on page 77). If you choose **Suppress**, specify the suppression time in hours and minutes.
 - c. Click **Save**. Your changes are now visible on the Specific Fault Rule tab.

TIP

You can sort the Specific Fault Rules table by Rule Description, Trigger ID (see “Customize the Triggers” on page 81), Content ID, Action, or Product/Application. To do so, click the link at the top of the appropriate column.

Figure 3-16 Rule Settings Page – Specific Fault Rule Tab

» Default rule
Specific fault rule

Click the rule description to edit an individual rule. To edit multiple rules at the same time, check the box for each rule that you want to change, scroll to the bottom of the page, and specify the rule settings.

<input type="checkbox"/>	Rule description	Trigger ID	Content ID	Action	Product or application
<input type="checkbox"/>	NNM: ovdbservice fails with "failure to connect... embedded database not started".	NNM-DB-ERROR-001		suppress	NNM

Change selected rules from above

Action Suppress ▾

Suppression time 8 ▾ Hours 0 ▾ Minutes

Cancel »
Save »

Figure 3-17 Edit Rule Settings Page

Edit rule settings

Rule settings

* = required field

Product or application NNM

Trigger ID: NNM-DB-ERROR-001

Action Suppress ▾

Suppression time is only needed if you select "Suppress" as an action.

Suppression time 0 ▾ Hours 0 ▾ Minutes

Rule description:* NNM: ovdbservice fails with

« Cancel
Save »

Customize the Triggers

A trigger is an error pattern that can be detected in a monitored resource. The following resources can be monitored by Self-Healing Services:

- HP OpenView application log files
- Specific directories where HP OpenView applications can create error or crash files
- Windows processes (event log)

You can use the trigger configuration process to create or update custom trigger rules for HP OpenView product faults. When the trigger conditions for a given rule are met, the Self-Healing Services client triggers a fault event and the subsequent collection of fault data.

It is the monitored resource to which a trigger is assigned that determines the role that trigger plays. If the monitored resource is a log file, the trigger patterns will be matched within the log file. If the monitored resource is a directory, the creation of files is what the trigger patterns will consider. If the monitored resource is Windows processes, the trigger patterns will be matched within the Windows event log.

You can create any trigger that you like and have it examine any monitored resource that you like. However, it makes sense that a trigger meant to look at a directory would contain a pattern like “*.java” (indicating all Java files), and a trigger examining a log file or the Windows event log would look like “Invalid entry: ‘.*’ is not a number”.

While the Self-Healing Service UI will not prevent the assignment of an inappropriate trigger pattern to a particular monitored resource, it won't actually ever trigger on that pattern.

The HP OpenView products that support trigger configuration for Self-Healing Services are listed in the Product/Application drop-down list on the Product Trigger Information page (see Figure 3-18 on page 83). Each product or application in the list has one or more resources—a log file, for example—that its triggers monitor. You can add or modify triggers for existing monitored resources. You cannot, however, add or modify monitored resources. You cannot delete an existing trigger. You can, however, choose to make it either active or inactive. If a trigger is inactive, no pattern matching is performed for that trigger.

A trigger consists of four required parameters and up to four additional optional parameters. These parameters are described in Table 3-3 on page 84. When you create a new trigger rule, you must provide values for each of the four required parameters.

To customize the triggers for a supported application or product:

1. In the local managed client view, click **Trigger settings** in the left navigation menu.
2. From the **Product or application** list, select the application that you want to work with.
3. From the **Monitored resource** list, select the resource that you want to work with.
4. Click **Refresh** to refresh the Resource Path and the set of triggers for the monitored resource selected. The Resource Path is the path of the log file or directory associated with this monitored resource.

The following information is displayed for each trigger:

Activate Flag	Whether this trigger is active for monitoring
Trigger Description	A short description of the trigger's purpose
Trigger ID	The unique identifier assigned to the trigger
Context	The context passed to the collector when this trigger fires

5. Perform one or more of the following actions:

- To edit or update the properties of an existing trigger, click the trigger description link.
- To add a new trigger, click **Click here to add a new trigger** (see “Add or Modify a Trigger” on page 85).
- Select the **Activate** box for all triggers that you want to use, clear the **Activate** box for all triggers that you do not want to use, and then click **Update trigger activations**.
- To sort the rules by Name, Message-ID or Context name, click the corresponding column header.

Figure 3-18 Trigger Settings Page

Trigger settings

Select product

Product or application

Monitored resource

Resource path

Cancel »
Refresh »

Trigger rules search results

Make changes to the trigger activation state, and then click "Update trigger activations" to update the triggers. An inactive trigger does not generate any incidents. Click the trigger description to view or edit the trigger properties.

» [Click here to add a new trigger.](#)

Activate	Trigger description	Trigger ID	Context
<input checked="" type="checkbox"/>	PD: Embedded database startup error	150-4	pd
<input checked="" type="checkbox"/>	PD: Database create error	150-5	pd
<input checked="" type="checkbox"/>	PD: Database startup error	150-2	pd
<input checked="" type="checkbox"/>	PD: External database error	150-3	pd
<input checked="" type="checkbox"/>	PD: Invalid NNM Advanced Edition	150-6	pd
<input checked="" type="checkbox"/>	PD: JDBC driver error	150-1	pd

Update trigger activations »

Table 3-3 Trigger Parameters

Name	Description
Trigger ID	A unique identifier within the set of triggers for this monitored resource. When you are updating an existing trigger, this field is read-only. When you are creating a new trigger, you must provide a Trigger ID that is unique among all the triggers for this monitored resource.
Trigger description	A short description of the trigger's purpose.
Context name	<p>The context information associated with the detected fault. The context name is passed to the data collector so that the data collector collects fault-specific data.</p> <p>Each HP OpenView product defines a set of contexts for Self-Healing data collection. Self-Healing Services attempts to retrieve the list of contexts that are supported by the Self-Healing data collector for that product. If Self-Healing Services successfully retrieves the list, it creates a drop-down list of those contexts. Otherwise, an input text field is provided where you can type in the context name.</p> <p>For descriptions of the context names for a specific HP OpenView product, see the following XML file:</p> <pre data-bbox="643 1035 1235 1060"><installDir>/conf/dc/<productName>.xml</pre> <p>where <i><installDir></i> is the directory where the Self-Healing Services client is installed, and <i><productName></i> is the abbreviated name of the HP OpenView application.</p> <p>For example, for information about contexts for Network Node Manager (NNM) installed on a UNIX operating system platform, see the file:</p> <pre data-bbox="643 1304 1089 1329">/opt/hpsupport/conf/dc/nnm.xml</pre> <p>On a Windows operating system platform, the default location of the file is as follows:</p> <pre data-bbox="643 1430 1357 1455">C:/Program Files/Hewlett Packard/conf/dc/nnm.xml</pre>

Table 3-3 Trigger Parameters (Continued)

Name	Description
Pattern	<p>A pattern that will be used for detecting faults in the application. The pattern must be a valid regular expression. The regular expression will be matched in the following ways:</p> <ul style="list-style-type: none"> • For a log file or the Windows event log resource, this regular expression will be matched against log messages written to the log file. The pattern must match a substring of the log message. • For a directory resource this regular expression will be matched against the names of the error/crash files created under that directory. <p>Self-Healing Services uses standard Java 1.4 regular expression matching and is constrained as such.</p> <p>Special characters such as () [], etc. must be preceded by a backslash (\) in the regular expression. The pattern string is case-sensitive.</p>

Add or Modify a Trigger

You can add or modify triggers for any HP OpenView products or applications that support triggers. A trigger is defined by the parameters described in Table 3-3. If you are adding a new trigger, you must provide values for all four parameters. For more information about applications supported by Self-Healing Servers, see this document:

http://support.openview.hp.com/pdf/selfhealing-supported-apps_ver2-6.pdf

To add or modify a trigger rule for a supported application or a product:

1. In the managed client view, click **Trigger settings** in the left navigation menu.
2. From the **Product or application** list, select the product or application that you want to work with.
3. From the **Monitored resource** list, select the resource that you want to work with.
4. Click **Refresh** to refresh the Resource Path and the set of triggers for the monitored resource selected. The Resource Path is the path of the log file or directory associated with this monitored resource.

The following information is displayed for each trigger that is listed:

- Activate Flag** Whether this trigger is active for monitoring
- Trigger Description** A short description of the trigger's purpose
- Trigger ID** The unique identifier assigned to the trigger
- Context** The context passed to the collector when this trigger fires

5. To add a new trigger, click **Click here to add a new trigger** (see “Add or Modify a Trigger” on page 85). To view or modify an existing trigger, click the trigger description link for that trigger.
6. Provide values for the four trigger parameters described in Table 3-3.

- a. If you are adding a new trigger, type a unique identifier for the new trigger **Trigger ID** box.
If you are modifying an existing trigger rule, this box will be read-only.
- b. In the **Trigger description** box, type a short description of the trigger's purpose.
- c. From the **Context name** list, select the context for this trigger rule.

NOTE

Self-Healing Services attempts to populate the **Context name** drop-down list using the information in the `<ProductName>.xml` file. If this file is missing or not readable, the list is not created. If the drop-down list is not available, you can type in the context name.

- d. In the **Error pattern** box, type the regular expression that you want Self-Healing Services to match in the log file or error/crash file.
7. Click **Save trigger**.

Figure 3-19 Trigger Page for an Existing Rule

Add rule Information

Enter trigger details

* = required field

Trigger ID* 150-2

Trigger description* PD: Database startup error

Context name* pd

Pattern*

```
\\(PDCentral\) unable to run database startup script
```

« Back To Search Results Save trigger »

Advanced Functions

The following functions are described in this section:

- “Deactivate a Configuration Center” on page 88
- “Deactivate a Communication Gateway” on page 91
- “View or Modify the Configuration Center Settings” on page 92

These functions are discussed separately, as they are not part of the typical setup or operation of Self-Healing Services. They are useful when you want to restructure your Self-Healing Services managed environment.

Deactivate a Configuration Center

After you establish a configuration center, you can deactivate it at any time. This action disables only the configuration center functionality for a given Self-Healing Services client. That client continues to serve as a managed client. It can still detect faults, process incidents, and submit them to HP (if it is connected to an active communication gateway). It cannot, however, receive configuration updates unless it is connected to another configuration center. If this client was set up as a Communication Gateway, it continues to function in that role.

To deactivate a configuration center:

1. In the left navigation menu for a configuration center, click **Deactivate configuration center**.

Figure 3-20 Deactivate Configuration Center Page

Deactivate configuration center

Information

Deactivate local configuration center

This action will disable the configuration center functionality for this Self-Healing Services client. If you take this action, this client will continue to detect faults, collect data, and submit incidents to HP (provided that it is associated with a communication gateway). It will not, however, be able to receive configuration updates until you connect it to another configuration center.

Cancel » **Deactivate »**

2. Click the **Deactivate** button.

After the configuration center is deactivated, the Add a Configuration Center page opens.

Figure 3-21 Add a Configuration Center Page

Add configuration center node

1. This Self-Healing Services client no longer serves as a configuration center.

Instructions

To connect this local managed client to an existing configuration center, specify the host name and port for that configuration center, and click the 'Save' button.

To keep this client disconnected from any configuration center, click the 'Cancel' button.

To set up this client as a configuration center, click the 'Self-Healing Services setup' link on the left navigation menu.

Add configuration center

* = required fields

Host name*

Port*

Configuration update period Hours Minutes

3. If you want to associate this managed client with a different configuration center, follow these steps:
 - a. In the **Host name** box, type the host name of the new configuration center.
 - b. In the **Port** box, type the port number that the new configuration center will use to communicate with this managed client.
 - c. In the **Configuration update period** field, select the time in hours and minutes that this managed client should wait before retrieving updated configuration information from the configuration center. The minimum setting is 5 minutes, and the maximum is 24 hours (the default).

If you specify 6 hours 0 minutes, for example, the managed client will attempt to retrieve configuration information from the configuration center every 6 hours.

NOTE

Configuration updates cause heavy network traffic. If you make the update period too short, this may degrade network performance.

- d. Click **Save**.

If you do not want to associate this managed client with a configuration center, click **Cancel**.

To reactivate a configuration center:

1. In the left navigation menu, click **Self-Healing Services setup**.
2. Click the **Set up a new configuration center** link.
3. Follow steps 1 through 5 in the Self-Healing Services setup process.

Deactivate a Communication Gateway

After you establish a local communication gateway, you can deactivate it at any time. This action disables only the local communication gateway functionality for a given Self-Healing Services client. That client continues to serve as a managed client. It can still detect faults, process incidents, and receive configuration updates from its configuration center. It cannot, however, submit incidents to HP.

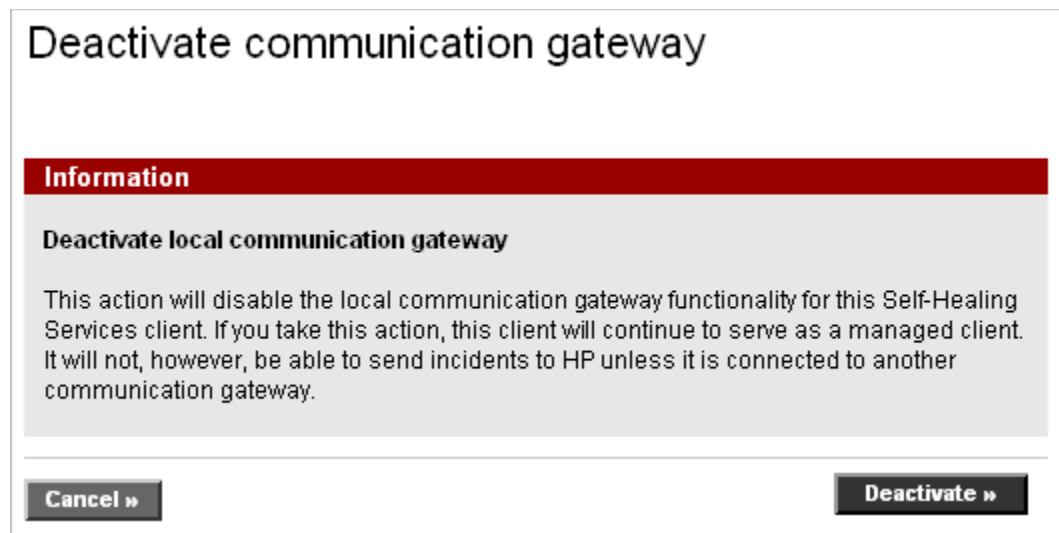
NOTE

If other managed clients depend on this gateway to submit incident data to HP, they will be affected if it is deactivated. If this gateway is the only gateway with which another client is associated, that client will operate in disconnected mode until it is associated with a new gateway. If this gateway is one of multiple gateways with which another client is associated, that client will continue operating in connected mode and will use one of its other gateways to send data to HP.

To deactivate a communication gateway:

1. In the left navigation menu for a managed client, click **Deactivate communication gateway**.

Figure 3-22 Deactivate Communication Gateway Page



2. Click the **Deactivate** button.

After the communication gateway is deactivated, the Local Managed Client page opens.

To reactivate a communication gateway:

1. In the left navigation menu, click **Self-Healing Services setup**.
2. Click either the **Set up a new configuration center** link or the **Use existing configuration center** link.
3. Follow steps 1 through 5 in the Self-Healing Services setup process.

Select **Local communication gateway** to reactivate the communication gateway functionality for this client.

View or Modify the Configuration Center Settings

When the managed client that you are working with is associated with a remote configuration center, you can view or change this association. The initial association between a configuration center and a managed client is established during the setup process. You can change this association, however, at any time.

To view or change the configuration center for a managed client:

1. On the left navigation menu, click **Local managed client**.
2. On the Local Managed Client page, click the **Configuration center** link. This link is located in the lower right corner of the page.

Figure 3-23 Edit Configuration Center Node Page

Edit Configuration Center node

Edit configuration center

* = required fields

Host name*

Port*

Configuration update period Hours Minutes

3. If you want to change any of the configuration center settings, follow these steps:
 - a. In the **Host name** box, type the fully qualified host name for system where the new configuration center resides.
 - b. In the **Port** box, type the port number that the managed client will use to communicate with the configuration center.
 - c. In the **Configuration update period** field, select the time in hours and minutes that this managed client should wait before retrieving updated configuration information from the configuration center. The minimum setting is 5 minutes, and the maximum is 24 hours (the default).

If you specify 6 hours 0 minutes, for example, the managed client will attempt to retrieve configuration information from the configuration center every 6 hours.

NOTE

Configuration updates cause heavy network traffic. If you make the update period too short, this may degrade network performance.

- d. Click **Save**.

You can also reset the configuration center association for a particular managed client. This disconnects the managed client from its configuration center. When a managed client is not associated with a configuration center, it cannot receive configuration updates. It can still detect faults and submit them, provided that it is associated with an active communication gateway.

To disconnect a managed client from its configuration center:

1. On the Local Managed Client page, click the **Configuration center** link. This link is located in the lower right corner of the page.
2. Click **Reset Configuration Center**.
3. Click **Save**.

4 **Managing Incidents**

This chapter explains how to view your detected faults, incident packages, and incident summary reports. It explains how to submit an incident to HP that is on hold, submit additional data to HP for a previously submitted fault, and send a system assessment to HP. It also explains how to configure your filter policy and how to manually submit a fault.

In This Chapter

There are two ways to view incident information in the Self-Healing Services client user interface (UI). The **incident viewer** lists the individual incidents processed by a managed client and shows the status of each incident. An **incident summary report** contains an overview of all incident activity for a particular managed client; it lists the number of incidents in each state of the incident life cycle.

This chapter contains the following topics:

- “View Incidents and Collected Data” on page 97
- “View an Incident Summary Report” on page 108
- “Submit Incidents on Hold” on page 112
- “Change Your Filter Settings” on page 113
- “Submit a System Assessment” on page 116
- “Manually Submit an Incident” on page 118

View Incidents and Collected Data

You can use a managed client's Incident Viewer to see a list of incidents that match specific search criteria (see Figure 4-1). You can view all or a subset of the incidents that have occurred on that client, and you can view the data that has been collected for each incident.

To use the Incident Viewer:

1. In the managed client view, click **Incident viewer** in the left navigation menu.
2. *Optional:* In the **Status** box, select one or more options (see Table 4-1 on page 98 for status descriptions).

To select multiple options, hold the **CTRL** key down and click each option that you want to select.
3. *Optional:* In the **Product or application** box, select one or more applications.

In this context, the **Product or application** box lists only those applications that have at least one associated incident on this managed client.
4. Click **Search**. The **Incident viewer** search results page is displayed (see Figure 4-2 on page 100).

NOTE

If you click **Search** without selecting any search parameters, Self-Healing Services searches for all incidents associated with all supported applications installed on this system.

The list of incidents does not automatically refresh when a new fault is detected or when the state of an existing incident changes. You must click **Search** again to refresh the list.

Figure 4-1 Incident Viewer Prior to Search

Incident viewer

Instructions

You can use this page to search for incidents present in the system. You can filter your search by incident status, product or application, or both. Use CTRL+Click to select multiple items. The search results are not automatically refreshed when new incidents are added or the status of an existing incident changes. To refresh the results, click **Search**.

Incident search criteria

Status

Failed
Hold
Offline
Received
Submitted

Product or application

Self-Healing Services
Network Node Manager

Reset »

Search »

Table 4-1 Incident Viewer Status Fields

Status	Description
Received	An incident is marked Received from the point at which a fault is detected in a supported application until Self-Healing Services decides whether the incident should be Suppressed, Ignored, Held, Submitted, or Failed.
Failed	An incident is marked Failed if it was supposed to be submitted to HP, but the submission process failed. If submission fails, it is re-attempted a set number of times with a certain time interval between retries. Once the number of retries has been exceeded, the incident is placed on Hold. To submit it after submission failed, perform the steps in “Submit Incidents on Hold” on page 112.
Hold	An incident is marked Hold under two conditions: (1) the action for the fault rule associated with this type of fault is set to Hold; (2) the action for the fault rule associated with this type of fault is set to Submit, but the submission process has failed (<i>see</i> Failed).
Ignored	An incident is marked Ignored if the fault rule for this type of fault is set to Ignore. The incident will not be processed further at any time.
Submitted	An incident is marked Submitted if it was successfully submitted to HP.

Table 4-1 Incident Viewer Status Fields (Continued)

Status	Description
Suppressed	An incident is marked Suppressed if Self-Healing Services detected a fault in a supported application, but it is a duplicate of a previous fault and is within the suppression time limit. Once the suppression time limit has expired, the next incident of this type will be submitted.
Offline	An incident is marked Offline if the managed client was not connected to an active communication gateway at the time the incident was generated. You can resubmit an Offline incident—the same way that you can submit an incident on Hold—after the managed client is connected to a communication gateway.

Figure 4-2 Incident Viewer Search Results

Incident viewer

Instructions

You can use this page to search for incidents present in the system. You can filter your search by incident status, product or application, or both. Use CTRL+Click to select multiple items. The search results are not automatically refreshed when new incidents are added or the status of an existing incident changes. To refresh the results, click **Search**.

Incident search criteria

Status

Failed
Hold
Offline
Received
Submitted

Product or application

Self-Healing Services
Network Node Manager

Reset »

Search »

Incident search results (1-4) of 4

Click the incident name link to edit or view the incident properties. Check the incidents that you want to delete and then click the "Delete Checked Incidents" button.

<input type="checkbox"/>	<u>Incident name</u>	<u>Status</u>	<u>Date/time</u>	<u>Product or application</u>
<input type="checkbox"/>	Post-Installation Test	Submitted	Jan 28, 2007 / 00:31:41 AM (GMT)	Self-Healing Services
<input type="checkbox"/>	Test 1 - Single system configuration	Submitted	Jan 28, 2007 / 00:32:31 AM (GMT)	Self-Healing Services
<input type="checkbox"/>	Test A - Remove Gateway	Hold	Jan 28, 2007 / 00:33:03 AM (GMT)	Self-Healing Services
<input type="checkbox"/>	Test B - Replace Gateway	Submitted	Jan 28, 2007 / 00:34:03 AM (GMT)	Self-Healing Services

Previous | **1** | Next

TIP You can sort the Incident Search Results table by Incident name, Status, Date/Time, or Source. To do so, click the link at the top of the column that you want to sort by.

To permanently delete one or more incidents from the list:

1. In the far left column, select the check box for each incident that you want to delete.
2. Click **Delete Checked Incidents**.

IMPORTANT

Deleted faults cannot be recovered. Any collected data stored for this incident is also deleted. This operation cannot be undone.

To view the details for an incident:

Click the **Incident name**. The **Incident details** page is displayed (see Figure 4-3).

Figure 4-3

Incident Details for a Submitted Incident

Incident Details

Incident information

List of incident information.

Incident ID	000A9DFE258B-27810910-1365976638-1569744301485
Product or application	Self-Healing Services
Date/Time	Jan 28, 2007 (0:31:41 AM (GMT))
Description	manual , Post-Installation Test
Details	First incident submitted after installation

[» View collected data submission settings](#)

Upload additional data

You may upload one file containing additional data for this incident. The file size must not be more than 1 MB. Spaces in file names will be replaced with underscores.

File name

View Data Collected for a Particular Incident

The Incident Details page provides information about the incident as well as a link that you can follow to view the data collected by the Self-Healing Services client. If the incident either was submitted or is on hold, you can view the data collected (see Figure 4-5 on page 104 and Figure 4-6 on page 105, respectively). If the incident was previously submitted, you can upload additional information pertaining to it.

To view the data collected for a fault:

1. Open the **Incident viewer**, and display the incident details for a particular incident (see page 101).
2. Click the **View collected data submission settings** link. The **Collected data filter** page opens, (see Figure 4-5 on page 104).
3. When you are finished working with the data for this fault, click **Back to Search Results** to return to the **Incident viewer** page.

To upload additional data and submit it to HP:

1. Open the **Incident viewer**, and display the incident details for a particular incident (see page 101).
2. Click **Browse**.
3. Locate the file that you want to upload—only local files can be uploaded.
4. Click **Upload File**.

The file is uploaded, submitted to HP, and stored at HP with the other data collected for this incident. The maximum file size that can be uploaded is 1 MB. After submitting additional data to HP, you will receive an Additional Data Received service notification by e-mail confirming that your data has been received by HP.

NOTE

From the Incident Details page, you can also submit an incident that is on hold (see Figure 4-4 on page 103). This removes the incident from hold status and allows Self-Healing Services to submit it to HP.

To submit an incident that is on hold:

1. Click **Submit This Incident** (see Figure 4-4 on page 103).
 2. See “Submit Incidents on Hold” on page 112 for further instructions.
-

Figure 4-4 Incident Details for an Incident On Hold

Incident Details

Incident information

List of incident information.

Incident ID	000A9DEF298C-14082380-1325787930-1559948783703
Product or application	Self-Healing Services
Date/Time	Jan 28, 2007 (0:33:03 AM (GMT))
Description	manual , Test A - Remove Gateway
Details	This one should fail

[» View collected data submission settings](#)

Submit incident

You may submit this incident, enabling it to be removed from its hold status and submitted.

[Submit This Incident »](#)

[« Back to Search Results](#)

Establish Data Filter Settings

When you click the **View collected data submission settings** link from the Incident Details page, the Collected Data Filter—Table of Contents page opens. This page provides links to detailed information about the data collected for this incident. The data submission settings are read-only for incidents that have already been submitted to HP (see Figure 4-5). You can change the settings for faults that are on hold (see Figure 4-6 on page 105).

Figure 4-5 Collected Data Filter—Table of Contents Page for a Submitted Incident

Collected Data Filter
Table of contents

Instructions

The information on these pages is read-only because the incident has already been submitted. Click the link for each item to see details.

System configuration information

- [Basic system information](#)
- [Memory and swap information](#)
- [File system information](#)
- [Environment variables](#)

System resource information

- [DNS information](#)

Application information

- [operations for Windows](#)
- [service desk](#)
- [event correlation services](#)
- [omniback II](#)
- [network node manager](#)
- [data protector](#)
- [Self-Healing Services](#)
- [reporter](#)
- [emanate SNMP agent](#)
- [service information portal](#)
- [performance agent](#)
- [instant support enterprise edition](#)

Cancel »

Figure 4-6 Collected Data Filter—Table of Contents Page for an Incident on Hold

Collected Data Filter
Table of contents

Instructions

Click the link for an item below to see more detail. For some items, you can exclude data from the incident package before submitting it to HP for analysis.

System configuration information

- [Basic system information](#)
- [Memory and swap information](#)
- [File system information](#)
- [Environment variables](#)

System resource information

- [DNS information](#)

Application information

- [operations for Windows](#)
- [service desk](#)
- [event correlation services](#)
- [omniback II](#)
- [network node manager](#)
- [data protector](#)
- [Self-Healing Services](#)
- [reporter](#)
- [emanate SNMP agent](#)
- [service information portal](#)
- [performance agent](#)
- [instant support enterprise edition](#)

Cancel »

You can exclude data items from an incident package before it is submitted to HP for analysis. This is useful if you have sensitive or confidential data items that you do not want to send outside your company. There are two ways to exclude data items from an incident package:

- Using the filter policy settings (see “Change Your Filter Settings” on page 113)
- Manually specifying exclusions while the package is on hold

When an incident is on hold, you can view and alter the data filter settings for that incident package. If your filter policy excludes certain data items from being submitted to HP, those items are marked as excluded on the Collected Data Filter page (see Figure 4-7). In addition to the data items excluded by your filter policy, you can manually exclude other data items. You can also override your filter policy (in part or entirely) to allow additional data to be submitted to HP.

Figure 4-7 Excluded Data

The screenshot shows a web interface titled "Collected Data Filter" with the subtitle "System configuration information". Below this is a red header bar labeled "Environment variables". Underneath is a table with three columns: "Exclude", "Name", and "Value". The table lists several environment variables, some of which are checked in the "Exclude" column.

Exclude	Name	Value
<input type="checkbox"/>	DISPLAY	:0.0
<input type="checkbox"/>	INSTALL_DIR	C:\PROGRA~1\HPOPEN~1
<input type="checkbox"/>	PROCESSOR_ARCHITECTURE	x86
<input type="checkbox"/>	META_CONF	C:\PROGRA~1\HPOPEN~1\newconfig\shs\META-IN
<input checked="" type="checkbox"/>	SYSTEMJAVAPATH	c:\j2sdk
<input type="checkbox"/>	FP_NO_HOST_CHECK	NO
<input checked="" type="checkbox"/>	PATH	C:\PROGRA~1\MKSTOO~1\bin;C:\PROGRA~1\MKE~1\Client_1\jre\1.4.2\bin\client;C:\Oracle\product\10.1.1\Files\Common Files\GTK\2.0\bin; C:\j2sdk\bin;C:\P~1\Documents\Susan\m10\Tools and Infrastructure\S~1\Files\Perforce;C:\Program Files\Hewlett-Packard\is...
<input type="checkbox"/>	SYSTEMCLASSPATH	C:\J2SDK\LIB\TOOLS.JAR;C:\Program Files\Java\j2
<input checked="" type="checkbox"/>	TERMCAP	C:\PROGRA~1\MKSTOO~1\etc\termcap
<input type="checkbox"/>	CONF	C:\PROGRA~1\MKSTOO~1\etc\termcap

When you are working with a particular incident on hold, you can change the filter policy for all future incidents (see “Change Your Filter Settings” on page 113).

NOTE

When an incident has already been submitted to HP, any data items excluded from the incident package do not appear on the Collected Data Filter page. After the incident shown in Figure 4-7 is submitted, for example, the SYSTEMJAVAPATH, PATH, and TERMCAP environment variables will not appear on the Collected Data Filter page for that incident.

If all the data items in a particular category are excluded, that category no longer appears in the table of contents for the incident.

To exclude data items from an incident package:

1. Open the **Incident viewer**, and display the **Incident details** for a particular incident (see page 97).
2. Click **View collected data submission settings**.
3. Click the link in the table of contents that pertains to the category of data items that you want to exclude.

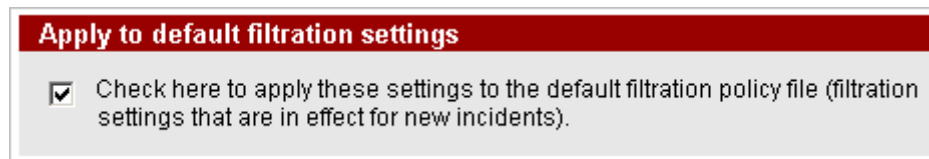
NOTE

If an application that appears in the **Application Information** list is not installed—or if it is installed, but some of its files have become corrupted—the status of that application will be listed as **unknown**. This can also happen if an application is installed using a nonstandard installation process.

4. In the **Exclude** column, select the check box for each data item that you want to exclude.

Not all data that is visible on the Collected Data page is eligible for filtering. If a particular data item cannot be filtered, a check box does not appear for that item in the **Exclude** column.

5. *Optional:* If you want to exclude these items from this and all *future* incident packages, select the **Apply to default filtration settings** box.



If you do not select this box, the data items will only be excluded from this incident package.

6. Click the **Save <category name> settings** button to save your new settings. In this case, **<category name>** matches the table of contents link that you clicked in step 3.
7. Repeat steps 3 through 5 until you have selected all the data items that you want to exclude from this incident package.

View an Incident Summary Report

Self-Healing Services provides an incident summary report in both the managed client and configuration center views. From the managed client view, the incident summary report shows the number of incidents either submitted to HP or placed on hold by that managed client. From the configuration center view, the incident summary report shows this information for each of the managed clients assigned to that configuration center.

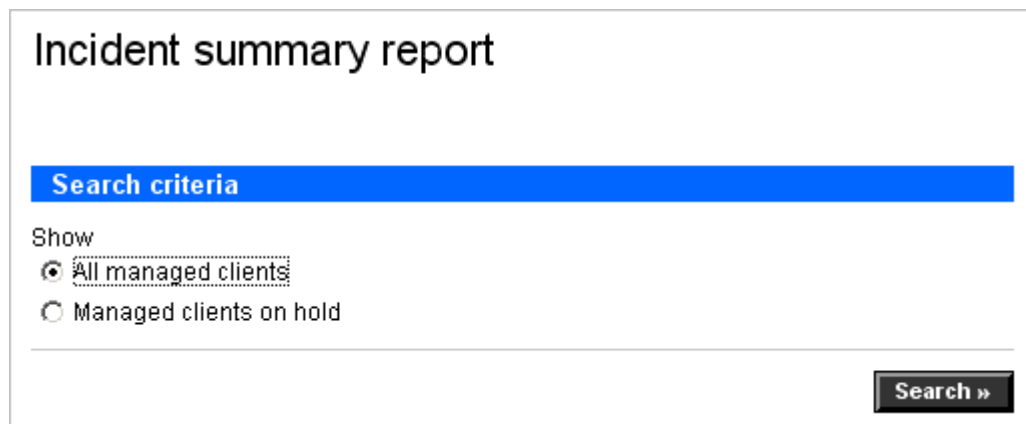
To view an incident summary report:

Click **Incident summary report** in the left navigation menu.

- If you are accessing a configuration center, the search page opens (see Figure 4-8 on page 108). Follow these steps:
 1. Choose one of the following options:
 - Select **All managed clients** to view the incident summary report for all managed clients assigned to this configuration center.
 - Select **Managed clients on hold** to view the incident summary report for only those managed clients assigned to this configuration center that have faults on hold.
 2. Click **Search**.

The **Incident summary** search results page is displayed (see Figure 4-9 on page 109).
 3. Choose one of the following options:
 - Click the host name of one of the managed clients listed in the search results to see the incident summary report for that client.
 - Click the value in the Hold column to see the incident viewer for that client.
- If you are accessing a managed client, the incident summary report for that client opens immediately.

Figure 4-8 Incident Summary Report Search Page



Incident summary report

Search criteria

Show

All managed clients

Managed clients on hold

Search »

Figure 4-9 Incident Summary Report Search Results Page

Incident summary report

Search criteria

Show

All managed clients

Managed clients on hold

[Search »](#)

Incident summary search results

Click a host name to view the incident summary report for a specific managed client. Click the 'On hold' value to view a list of incidents for a specific client.

Host name	Port	On hold	Hold information updated	Today	Yesterday	All
myserver.us.mycompany.com	5814	0	Dec 03, 2006	0	0	0
sales.uk.mycompany.com	5814	0	Dec 03, 2006	2	2	4

The links in the **Host name** column take you to the individual incident summary reports for the managed clients associated with this configuration center. The incident viewer lists the faults detected by that client and the status of each related incident. See “About the Incident Summary Report” on page 109 for additional information.

The links in the **On hold** column take you to the incident viewers for the clients in the list (see “View Incidents and Collected Data” on page 97 for further information). You can use the incident viewer to search for incidents that match specific search criteria

NOTE

When you click a link in the **Host name** or **On hold** column for a managed client other than the configuration center, the Sign-in page opens in a new window (see Figure 2-1 on page 37). You must sign in to the Self-Healing Services client UI for that managed client before you can see its incident summary report or incident viewer.

About the Incident Summary Report

Each managed client has an incident summary report. An incident summary report lists the faults detected by that client and the status of each related incident (see Table 4-1 on page 98 for status descriptions).

The incident summary report includes three tabbed pages (see Figure 4-10 on page 110):

- The **Today** tab shows the number of faults detected by the managed client today (starting at midnight) and the status of each related incident.

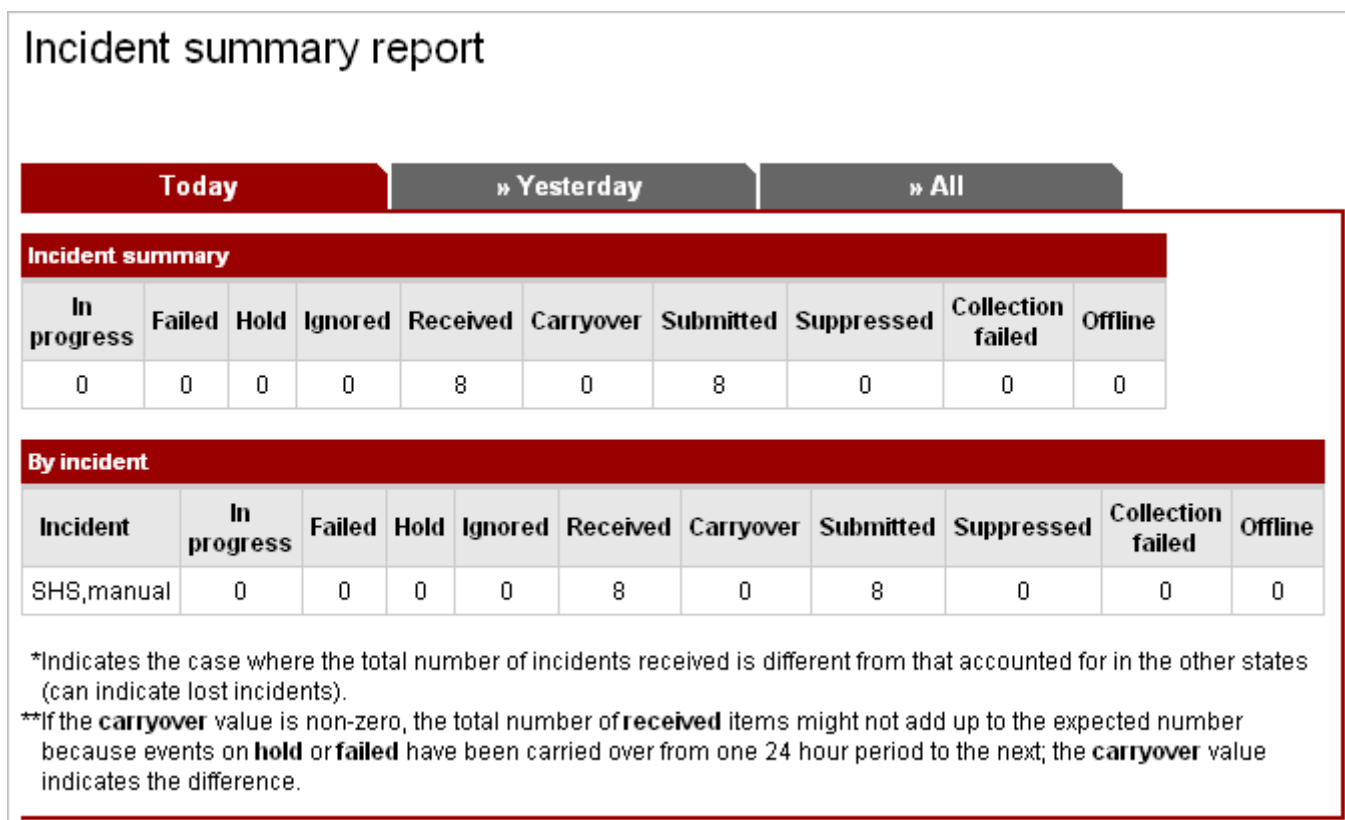
- The **Yesterday** tab shows the number of faults detected by the managed client yesterday (starting at midnight) and the status of each related incident.
- The **All** tab lists the total number of incidents in each status category that have been processed on this client since the Self-Healing Services client was installed.

Each tabbed page in the incident summary report contains the same two tables. If no data exists for a table, however, the table is not displayed.

The **Incident summary** table lists the number of incidents processed during the pertinent time interval (today, yesterday, or all) by their status.

The **By incident** table lists the types of faults detected during the time interval (today, yesterday, or all), how many times each occurred, and the status of each related incident.

Figure 4-10 Incident Summary Report



To view an incident summary report from the configuration center:

1. In the configuration center view, click **Incident summary report** in the left navigation menu. The search page opens (see Figure 4-8 on page 108).
2. Select either **All managed clients** or **Managed clients on hold**.
3. Click **Search**.
4. Click a link in the **Host name** column to view the incident summary report for one of the managed clients assigned to this configuration center.

When you click a link to view an incident summary report for another client, the Sign-in page opens in a new window (see Figure 2-1 on page 37). Sign in to the Self-Healing Services client UI for that managed client. The **Incident summary report** page is displayed (see Figure 4-10 on page 110).

To view the incident viewer for a specific managed client by accessing it directly:

1. In the managed client view, click the **Incident summary report** link in the left navigation menu. The report for this client opens.
2. Click the tab for the time period you are interested in: **Today**, **Yesterday**, or **All**.

Submit Incidents on Hold

There may be times when you want to create an incident package (collect data) when a fault occurs but not submit that incident package to HP. This is useful in the following situations:

- When you want to attempt to solve the problem yourself.
- When you want to view the incident package before it is submitted.
- When you want to remove certain sensitive pieces of data from the package before it is submitted to HP.

In any of these scenarios, the rule for this fault should be set to Hold (see “Customize the Default Rule Settings” on page 55). When the rule is set to Hold, the Self-Healing Services client collects context-specific troubleshooting and system data at the time the fault occurs and places that data in an incident package. The incident package is then held until you explicitly release it for submittal to HP.

To submit an incident that is on hold to HP:

1. In the managed client view, open the **Incident viewer**, and display the **Incident details** for a particular fault (see page 97).
2. Click **Submit This Incident**. The incident is removed from its hold status and submitted to HP.

Incident Details

Incident information

List of incident information.

Incident ID	0000000000000-1111111-222222222-333333333
Product or application	Self-Healing Services
Date/Time	Dec 04, 2006 (3:28:37 AM (GMT))
Description	manual , Test 9
Details	Test 9

[» View collected data submission settings](#)

Submit incident

You may submit this incident, enabling it to be removed from its hold status and submitted.

Submit This Incident »

Change Your Filter Settings

Your filter settings automatically exclude specific types of collected data from your incident packages before they are submitted to HP. Each managed client has its own filter settings.

The first time that you open the Filter Settings page for a given managed client, the page is empty, as shown in Figure 4-11. To establish your initial filter settings, you must view the collected data for an incident that is on hold and explicitly exclude one or more data items from the incident package. Then, you must apply your settings for that incident package to the filtration settings for that managed client.

Figure 4-11 Empty Filtration Settings Page

The screenshot shows a web interface titled "Filter settings". It contains three sections, each with a red header bar and a message below it:

- Data files**: No information available.
- Environment variables**: No information available.
- Commands**: No information available.

At the bottom of the page, there are two buttons: "Cancel »" on the left and "Save »" on the right.

To create the initial filter settings for a managed client:

1. Open the **Incident viewer**, and display the **Incident details** for a particular fault that is on hold (see page 97).
2. Click **View collected data submission settings**.
3. Click the link in the table of contents that pertains to the data item (or items) that you want to filter out.
4. In the **Exclude** column, select the check box for each data item that you want to filter out.

5. Select the **Apply to default filter settings** box at the bottom of the page:

Apply to default filter settings

Check here to apply these settings to the default filter policy file (filter settings that are in effect for new incidents).

Cancel » **Save environment variable settings »**

6. Click the **Save <category name> settings** button to save your new settings. In this case, **<category name>** matches the table of contents link that you clicked in step 3.

7. Repeat steps 3 through 6 until you have selected all the data items that you want to filter out.

After you create the initial filter settings for a managed client, you can view the settings by using the **Filter settings** link in the left navigation menu. Any data items that will be filtered out of the incident packages are listed. In the example shown in Figure 4-12, three environment variables are filtered out.

Figure 4-12 Existing Filter Policy

Filter settings

Data files

No information available.

Environment variables

Remove	Description
<input type="checkbox"/>	PATH
<input type="checkbox"/>	SYSTEMJAVAPATH
<input type="checkbox"/>	TERMCAP

Commands

No information available.

Cancel » **Save »**

NOTE

When you view the Filter Policy page (see Figure 4-12), only data items that are filtered out are listed, and the **Remove** check box for each filtered data item is cleared.

When you view the Collected Data Filter page for a particular incident (see Figure 4-7 on page 106), *all* data items are listed, and the **Exclude** check box is selected for those data items that will be excluded.

To view or modify the filter settings for a managed client:

1. In the managed client view, click the **Filter settings** link in the left navigation menu. The Filter Settings page opens.
2. In the **Remove** column, select the check box for any data item that you want to remove from the filter. This allows that data item to be submitted to HP.
3. Click **Save** to save any changes that you have made.

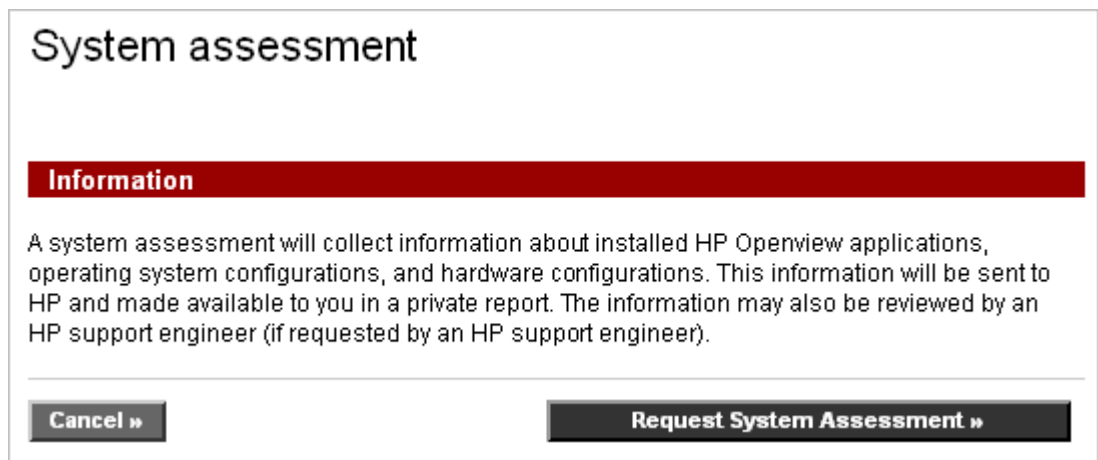
NOTE

You can also change the filter settings for a managed client when you modify the filter settings for a particular incident on that client. See page 107 for additional information.

Submit a System Assessment

A system assessment generates a report about the HP software installed on a managed client and all of the other managed clients, if any, assigned to the same configuration center. It offers a software inventory of the configuration center topology and updates all of the baseline information for the managed client from which it is submitted. When the system assessment is completed, Self-Healing Services sends a notification e-mail message to the service notification recipients listed on the Notification Settings page for the configuration center. This e-mail message contains a link to a detailed system assessment report. (see Figure 4-13).

Figure 4-13 System Assessment Page

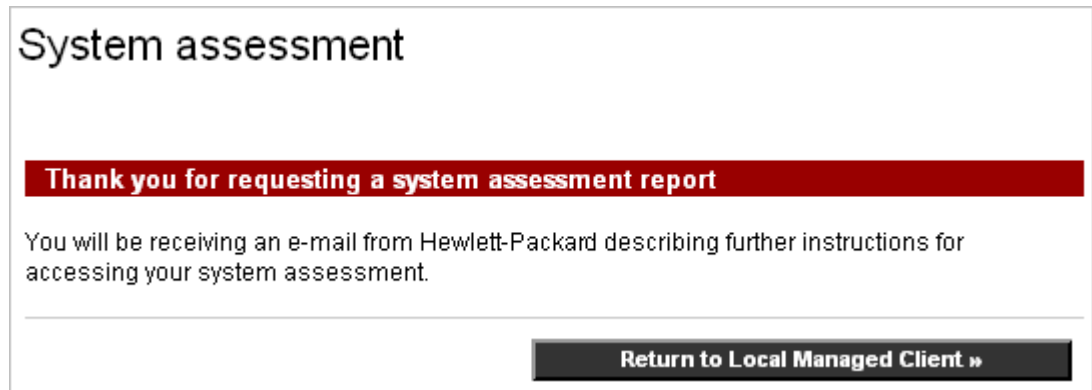


To submit a system assessment:

1. Open the Self-Healing Services user interface on the pertinent node (see “Start the Self-Healing Services User Interface” on page 37 for more information).
2. In the managed client view, click the **System assessment** link in the left navigation menu. The System Assessment page opens (see Figure 4-13).
3. Read the **Information** message.

4. Click **Request System Assessment**. The System Assessment Thank You page appears (see Figure 4-14).

Figure 4-14 System Assessment—Thank You Page



You will receive an e-mail notification containing a link to an incident analysis report that contains the results of your system assessment. Click this link to access your report (see Chapter , “Access the Self-Healing Services Support Web Site,” on page 127).

Manually Submit an Incident

If you experience a problem that is not recognized as a fault by the supported HP OpenView applications on your systems, you can manually submit an incident from the Self-Healing Services user interface (UI). This will trigger the Self-Healing Services process to generate an incident package and submit it to HP for analysis. Manually submitted incidents are processed the same as incidents generated when faults are automatically detected by Self-Healing Services with one exception: fault rules are not applied to manually submitted incidents.

To manually submit an incident:

1. In the local managed client view, click the **Manual submission** link. The Manual Submission page appears.

NOTE

You can also submit an incident manually from the configuration center view. You must first choose the managed client that you want to submit the incident. All the managed clients assigned to this configuration center are listed when you click the **Manual incident submission** link (Figure 4-15 on page 120).

Click the name of the client that you want to manually submit the incident.

If you choose a different client than the one you are currently logged on to, the Sign-in page for that client opens in a new window (see Figure 2-1 on page 37). Sign in to the UI for that client to complete the manual submission process.

If the system with which you are working has a dynamic IP address, both `localhost` and the fully qualified host name may appear in the list. If this is the case, click `localhost` to submit an incident from this system.

2. Select an application for from the **Product** list. This list contains all the applications supported by the Self-Healing Services client that are installed on this client (see Figure 4-16 on page 120). If you do not see the application that you want to use, click **Refresh**.
3. Type the actual error text for the incident in the **Problem title** field.
4. Type a description for the fault in the **Problem description** field.
5. Click **Submit**.

If you configured your notification and e-mail server settings so that you receive fault notifications, you should receive a fault notification from Self-Healing Services shortly after you manually submit a fault (see Figure 3-3 on page 58).

You should receive a service notification from Self-Healing Services later indicating that an incident analysis report is available (see Figure 6-2 on page 182). If the incident package fails the entitlement check, however, you will not receive this service notification.

If the incident package fails the entitlement check, you will receive a service notification from Self-Healing Services indicating that the system handle/SAID submitted with the incident package is invalid (see Figure 6-4 on page 185).

You will receive fault and service notifications from HP in the manner you specify on the Notification Settings page of the Self-Healing Services client user interface (see “Configure the Notification Settings” on page 57).

Figure 4-15 Manual Submission Client Selection Page on the Configuration Center

Manual incident submission

Click the link for the Self-Healing Services managed client from which you would like to submit an incident.

Host name	Port
myserver.us.mycompany.com	5814
myconfigctr.us.mycompany.com	5814
sales.uk.mycompany.com	5814

Cancel »

Figure 4-16 Manual Submission Page

Manual incident submission

Manual submission information

Client: myserver.us.mycompany.com

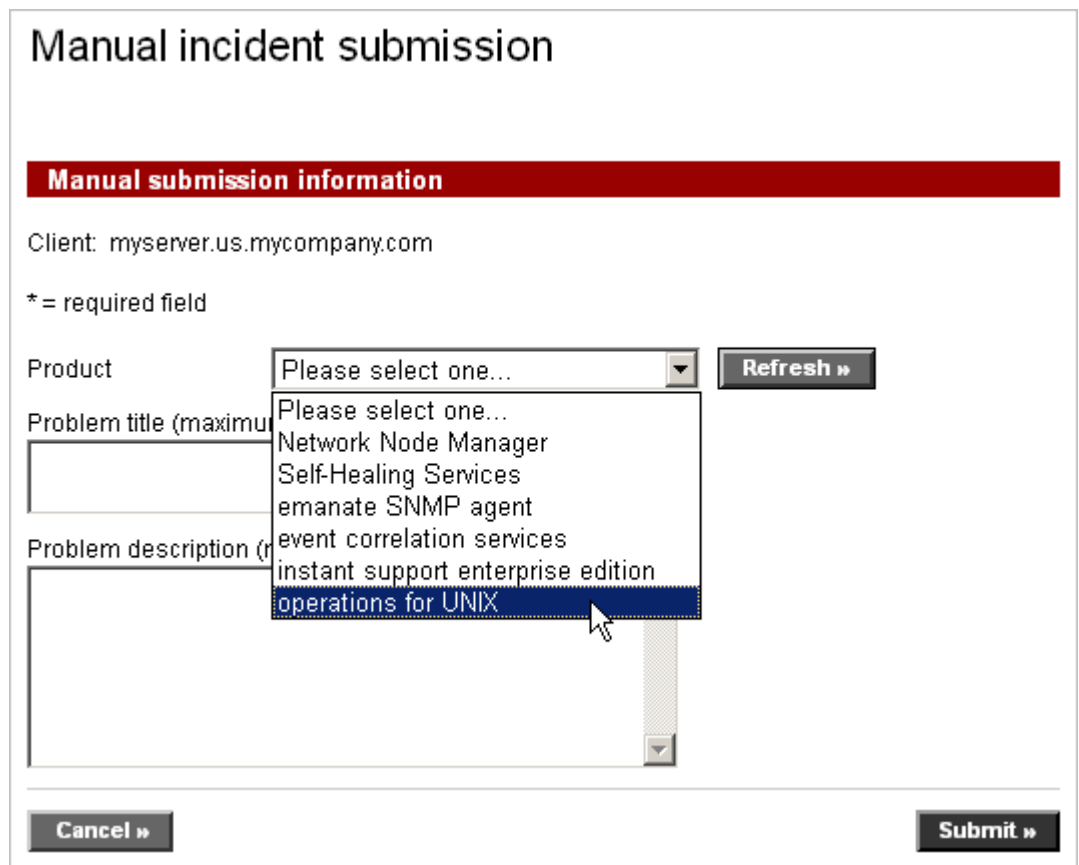
* = required field

Product **Refresh »**

Problem title (maximum 255 characters)

Problem description (maximum 1024 characters)

Cancel » **Submit »**



View or Modify Incident Deletion Settings

You can specify how long incident packages are stored on each client system. You can also specify how many incident packages can be stored at any given time. These settings help you manage the amount of disk space consumed by incident packages.

To configure the incident deletion settings:

1. In the left navigation menu, click **Incident Deletion**.

Figure 4-17 Incident Deletion Settings Page

Incident deletion

Instructions

This page enables you to specify two things: how long a single incident package is stored on this system, and how many incident packages can be stored on this system. You can specify the time, the number of incidents, or both.

Incident deletion settings

Enter the number of days that an incident package will be stored on this system (1-999).

days

Enter the maximum number of incident packages that can be stored on this system (1-99,999)

Cancel **Save**

2. If you want to specify how long a particular incident package is stored on this client system, follow these steps:
 - a. Select **Enter the number of days that an incident package will be stored on this system (1 - 999)**.
 - b. Enter the number of days an incident can be stored. The default is 30 days. When an incident becomes older than this number of days, it is automatically deleted from the system.
3. If you want to specify how many incident packages can be stored on this client at one time, follow these steps:
 - a. Select **Enter the maximum number of incident packages that can be stored on this system (1 - 99,999)**.

- b. Enter the number of incidents that can be stored. The default is 1000. If this limit is exceeded, the oldest incidents on this system are automatically deleted until the total number is equal to this limit.

4. Click **Save**.

Self-Healing Services runs a deletion cycle once every hour. Therefore, it is possible to temporarily exceed the incident limit between deletion cycles. Consider the following example:

- The incident limit is 100.
- 100 incident packages are stored on the system.
- Two new incidents are generated, making the total number of incidents 102.

After the next deletion cycle, the two oldest incident packages are deleted.

If you set the maximum number of incidents to a number lower than the current number of incidents, Self-Healing Services deletes the surplus incidents at the next deletion cycle. For example:

- The incident limit is 100.
- 100 incident packages are stored on the system.
- You reset the incident limit to 80.

After the next deletion cycle, the 20 oldest incident packages are deleted.

Managing Incidents

[View or Modify Incident Deletion Settings](#)

5 Incident Analysis Reports

This chapter describes how to access and use your incident analysis reports. These reports are located on the secure HP OpenView Self-Healing Services web site.

In This Chapter

This chapter contains all the instructions you need to access and use your incident analysis reports on the HP OpenView Self-Healing Services Support web site.

It contains the following topics:

“Access the Self-Healing Services Support Web Site” on page 127

“Find an Incident Analysis Report” on page 132

“The Incident Analysis Report” on page 137

“Open a Support Case” on page 148

“Submit Feedback to HP” on page 154

“Change the System Handle/SAID Associated with an Incident” on page 159

“View Your Support Contract Information” on page 162

“Metric Reports” on page 167

“Download Client Software” on page 171

“About HP Passport” on page 174

Access the Self-Healing Services Support Web Site

You can access your Self-Healing Services incident analysis reports from the HP OpenView Self-Healing Services Support web site. From this site, you can also do the following things:

- Review your support contract information.
- Re-associate an incident with a new system handle/SAID.
- Provide feedback to HP regarding an incident analysis report.
- Open a support case for an incident.
- Investigate your HP support contract.
- Download the latest version of the Self-Healing Services or ISEE client.
- View this user guide and the *Self-Healing Services Installation Guide* online.

To access the HP OpenView Self-Healing Services Support web site:

1. Open a web browser and go to the following address:

<http://support.openview.hp.com/software/analysis/main>

The HP Passport Sign-In page appears (see Figure 5-1).

2. In the **User ID** box, type your HP Passport user ID.
3. In the **Password** box, type your HP Passport password.
4. Click **Sign-in**.

NOTE If you forgot your user ID or password, or are a new user, see “About HP Passport” on page 174.

Figure 5-1 HP Passport—Sign-In Page

HP Passport sign-in

HP Passport is a single login service that lets you register with HP Passport-enabled Web sites using a single user identifier and password of your choice.

* = Required field

Sign-in to HP Passport

User ID* i

Password*

Remember my user ID and password

[» New users - please register](#)

[HP Passport is secure](#)

Use the Incident Manager

After you have signed in to HP Passport, the Incident Manager page appears. This page provides a list of links to your incident analysis reports (see Figure 5-2). For each incident listed, it tells you when the incident was created, whether it is open or closed, and what its support case status is.

NOTE

Only incidents associated with the system handles/SAIDs in your HP Passport profile are listed on this page.

If you see the Support Contract Information page when you sign in to HP Passport—instead of the Incident Manager page or one of your incident analysis reports—you do not have a valid system handle/SAID in your HP Passport profile.

Click the **Support contract info** link, and add a valid system handle/SAID to your HP Passport profile. See “View Your Support Contract Information” on page 162 for additional information.

In addition to the incident analysis reports, the Incident Manager page provides links to the following Self-Healing Services functions:

- Find incident analysis reports—use this function to search for reports based on their characteristics (see “Find an Incident Analysis Report” on page 132).
- Re-associate incidents with new system handles/SAIDs—use this function to view an incident that was submitted with an invalid system handle (see “Change the System Handle/SAID Associated with an Incident” on page 159).
- View metric reports summarizing the Self-Healing Services activity in your environment over a specified date range.
- View support contract information—use this function to view the system handles/SAIDs associated with your support contract (see “View Your Support Contract Information” on page 162).
- Download self-healing software—use this function to download a copy of the Self-Healing Services client software or the ISEE client software (see “Download Client Software” on page 171).

The Incident Manager also provides links to the following information resources:

- User’s Guide—full text of the *HP OpenView Self-Healing Services User’s Guide*.
- Help information—online help for the Self-Healing Services Support web site.
- Installation Guide—full text of the *HP OpenView Self-Healing Services Installation Guide* for all platforms.
- Product data sheet—technical details about Self-Healing Services.

TIP

In most cases, you can return to the Incident Manager page by using the bread crumbs at the top of the page:

[Software](#) > [Management software](#) > [Support](#) > [Troubleshooting](#) > [Incident manager](#)

Figure 5-2 Incident Manager

[Software](#) > [Management software](#) > [Support](#) > [Troubleshooting](#)

HP OpenView self-healing services

Welcome, John Smith

HP OpenView self-healing incident manager attempts to analyze your incidents and deliver self-solve solutions.

- » Find incident analysis reports
- » Re-associate incidents with new system handles/SAIDs
- » View metric reports
- » View support contract information
- » Download self-healing software
- » Help information
- » User guide (pdf)*
- » Installation guide (pdf)*
- » Product datasheet (pdf)*

Incident analysis reports

Report List: This table shows the incidents that have had incident analysis reports generated. Select an incident analysis report identifier to view its details. Select a column heading to sort the reports. Incident analysis reports can be closed or reopened from this page.

Incident ID/Summary	↓ Date/Time	Incident status	Case status
0010C6C7144F-28544220-2073866231-1153739232787 Fault Self-Healing Services Test for HOLD <i>myserver.us.mycompany.com</i>	Aug 4, 2006 4:20:20 AM GMT	Open (Close report)	Not created
001185880802-28607378-899151465-1154360897964 Fault network node manager NNM: ovdcheck fails with "failure to connect... embedded database not started", <i>sales.uk.mycompany.com</i>	Jul 31, 2006 3:48:16 PM GMT	Open (Close report)	Not created
0010C6C7144F-13158358-2073866231-1153719961436 Fault performance manager test OVPM <i>support.asia.mycompany.com</i>	Jul 24, 2006 11:07:12 AM GMT	Open (Close report)	Not created

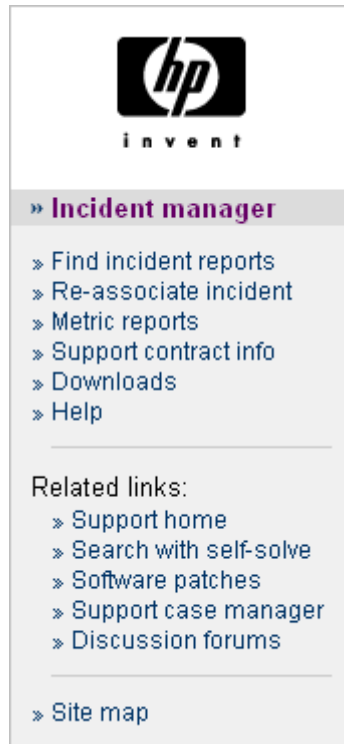
First | Previous | **1** | Next | Last

To view an incident analysis report:

In the **Incident ID/Summary** column, click the incident ID for the report you want to see.

NOTE The left navigation menu on the Incident Manager page contains links to the HP OpenView Support web site home page, the self-solve search engine, the software patches page, the support case manager page, and the discussion forums web page.

Figure 5-3 Incident Manager (left navigation menu)



Find an Incident Analysis Report

You can access an incident analysis report one of three ways:

- Click the incident ID listed in the table on the Incident Manager main page (see page 130).
- Search for the report either by incident ID or by specific criteria using the Find Reports function (see below).
- Click the link to the report in your Report Available service notification e-mail (see page 182).

All three methods require you to sign in to HP Passport before you can view an incident analysis report.

To search for an incident analysis report by incident ID:

1. Access the HP OpenView Self-Healing Services Support web site by using the instructions on page 127.
2. Click the **Find incident reports** link in the left navigation menu. The Find Incident Analysis Reports page opens (see Figure 5-4 on page 134).
3. In the **Enter an incident identifier** box, type or paste the incident ID for the report that you want to find.
4. Click **Find Report**.

TIP

The incident ID for a particular report is shown in the Report Available service notification e-mail you received (see Figure 6-2 on page 182).

To search for incident analysis reports by specific criteria:

1. Access the HP OpenView Self-Healing Services Support web site using the instructions on page 127.
2. Click the **Find incident reports** link in the left navigation menu. The Find Incident Analysis Reports page opens (see Figure 5-4).
3. *Required:* On the **Incident type** line, select **Fault**, **System assessment**, or both.
A fault report is generated when Self-Healing Services detects a fault in a supported application. A system assessment report is generated when you initiate a system assessment from the Self-Healing Services user interface.
4. *Required:* On the **Incident status** line, select **Open**, **Closed**, or both.
Incidents are open until you explicitly close them.
5. *Required:* On the **Support case status** line, select **Open**, **Closed**, **Not Created**, or any combination of these three options.
If you create a support case for a particular incident, that support case remains open until you explicitly close it.
6. *Recommended:* Narrow your search by specifying any or all of the following optional search criteria:

- a. *Optional:* From the **System handle/SAID** list, select the system handle or SAID that is associated with the incident analysis reports that you want to find.

If you do not select a specific system handle/SAID, the search will include all valid system handles/SAIDs associated with your HP Passport profile.

NOTE

If you do not see the system handle/SAID that you want to specify in the list, add that system handle/SAID to your HP Passport profile. See “About HP Passport” on page 174.

- b. *Optional:* From the **Submitted since** list, choose the time interval that you want to search.

If you do not specify a time interval, the search will include all time intervals.

- c. *Optional:* From the **Product** list, choose the HP OpenView product associated with the reports that you want to find.

If you do not specify a product, the search will include all supported products.

- d. *Optional:* From the **Managed client** list, choose the managed client associated with the reports that you want to find.

If you do not specify a node, the search will include all managed clients for which incident analysis reports exist.

- e. *Optional:* In the **Contact last name** box, type or paste the last name of the individual specified on the Contact Information page in the Self-Healing Services UI when the reports that you want to find were published.

- f. *Optional:* From the **Reports per page** list, choose the number of reports that you want to appear on each page in the search results: 10, 20, or 25.

7. Click **Find Reports**.

The List of Incident Analysis Reports page opens (see Figure 5-5 on page 135).

NOTE

Only incident analysis reports associated with valid system handles/SAIDs that you have added to your HP Passport profile are displayed in the search results. Incident analysis reports associated with an expired system handle/SAID are not displayed.

To add system handles/SAIDs to your HP Passport profile, follow the instructions in “View Your Support Contract Information” on page 162.

To view an incident analysis report associated with an expired system handle/SAID, re-associate the incident analysis report with a valid (not expired) system handle/SAID, following the instructions in “Change the System Handle/SAID Associated with an Incident” on page 159.

Figure 5-4 Find Incident Analysis Reports Page

[Software](#) > [Management software](#) > [Support](#) > [Troubleshooting](#) > [Incident manager](#)

Find incident analysis reports

Find incident analysis report by incident identifier

If you know your incident id please enter it here, and click the "Find Report" button to retrieve the incident analysis report

Enter an incident identifier

i [Where do I find an incident identifier?](#) **Find Report »**

Find incident analysis report(s) by criteria

Choose the following criteria to return a list of incident analysis reports. Click the "Find Reports" button to start the search.

* = required field

Incident type*	<input checked="" type="checkbox"/> Fault <input checked="" type="checkbox"/> System assessment
Incident status*	<input checked="" type="checkbox"/> Open <input type="checkbox"/> Closed
Support case status*	<input checked="" type="checkbox"/> Open <input type="checkbox"/> Closed <input checked="" type="checkbox"/> Not created
System handle/SAID	All system handles/SAIDs <input type="button" value="i"/> More info
Submitted since	All incident analysis reports <input type="button" value="i"/> More info
Product	All products <input type="button" value="i"/> More info
Managed client	All managed clients <input type="button" value="i"/> More info
Contact last name	<input type="text"/>
Reports per page	10 reports per page <input type="button" value="i"/> More info

Reset » **Find Reports »**

Figure 5-5 Results of Find Reports Operation

[Software](#) > [Management software](#) > [Support](#) > [Troubleshooting](#) > [Incident manager](#) > [Find reports](#)

List of incident analysis reports

Incident analysis report search criteria

Incident type	Fault
Incident status	Open
Support case status	Open, Not created
System handle/SAID	All system handles/SAIDs
Submitted since	Last 2 days
Product	network node manager
Managed node	
Contact last name	
Reports per page	10 reports per page

[« Return to Find Reports](#)

1–10 of 15 incident analysis reports

Incident ID/Summary	↓ Date/Time	Incident status	Case status
080009FD856B-1080475476-1499123795-1114192178149 Fault network node manager Fri Apr 22 10:48:39 IP Topology Replicator (ovrepld) on who.na.acme.com exiting, who.na.mycompany.com	Apr 22, 2005 5:49:36 PM GMT	Closed (Reopen report)	Not created
000BCDE32B08-20229888-1979199406-1119452609229 Fault network node manager netmon terminated sales.uk.mycompany.com	Jun 22, 2005 3:03:29 PM GMT	Open (Close report)	Not created
0003baa26d22-9051768-834589668-1119427032006 Fault network node manager Exiting on fatal database error support.asia.mycompany.com	Jun 22, 2005 7:57:11 AM GMT	Open (Close report)	Not created
0003baa26d22-2760636-834589668-1119426431753 Fault network node manager Exiting on fatal database error support.sa.mycompany.com	Jun 22, 2005 7:47:10 AM GMT	Open (Close report)	Not created

First | Previous | **1** | Next | Last

The List of Incident Analysis Reports page lists the incident IDs for the incident analysis reports that match the search criteria you specified. It shows the date and time each incident was created, the incident's status, and the incident's support case status. In the example shown in Figure 5-5 on page 135, the list contains all the reports published in the last 2 days for fault associated with the HP OpenView Network Node Manager (NNM) product.

To view a report, click the incident ID associated with that report.

To perform a new search, click **Return to Find Reports**.

The Incident Analysis Report

A custom incident analysis report is generated by Self-Healing Services every time an incident package is submitted to HP. The time it takes to generate the incident analysis report can vary because of data collection time and network delays.

When a new incident analysis report is published to the HP OpenView Self-Healing Services Support web site and is available to you, you (and anyone else that you specify) receive a Report Available service notification by e-mail that contains a link to the analysis incident report (see Figure 6-2 on page 182).

You can access an incident analysis report two ways. You can follow the instructions in “Find an Incident Analysis Report” on page 132, or you can click the link in the Report Available service notification you have received. Both methods require you to sign-in to HP Passport.

If the Support Contract Information page is displayed when you sign-in to HP Passport, this means that you do not have a valid system handle/SAID in your HP Passport profile. Click the **Support contract info** link, and add a valid system handle/SAID to your HP Passport profile. See “About HP Passport” on page 174 for additional information.

NOTE

You can only view an incident analysis report if the system handle/SAID associated with that report is in your HP Passport profile, the system handle/SAID associated with it is valid (not expired), and the incident analysis report has not been deleted (see “Report Life Cycle” on page 31).

To add system handles/SAIDs to your HP Passport profile, follow the instructions in “View Your Support Contract Information” on page 162.

To view an incident analysis report associated with an invalid system handle/SAID, re-associate the incident analysis report with a valid system handle/SAID, following the instructions in “Change the System Handle/SAID Associated with an Incident” on page 159.

An incident analysis report is a single web page that has three major sections:

- “Incident Summary” on page 138
- “Detailed Incident Analysis Report” on page 140
- “Case Management and Report Feedback Utilities” on page 147

Each of these sections is described in detail in this chapter.

Incident Summary

The Incident Summary contains basic information that identifies the incident, its status, system information for the managed client on which the fault occurred, the configuration center to which the managed client is assigned, and contact information associated with the incident (see Figure 5-6 on page 138). It also includes the system handle/SAID associated with the incident.

Figure 5-6 Incident Analysis Report—Incident Summary

[Software](#) > [Management software](#) > [Support](#) > [Troubleshooting](#) > [Incident manager](#)

Incident analysis report

Report information

This report contains information about your incident, as well as detailed [product configuration](#), [patch](#), [technical document](#), and [discussion forum](#) analysis that may be pertinent to resolving the incident. Options for [submitting a support case](#) or providing feedback on the analysis are also available.

Incident summary

Incident ID	090013AB842C-1950483431-1529184787-1153192738155
Incident date/time	Jan 18, 2007 5:49:36 PM GMT
Last modified date/time	Jan 20, 2007 10:00:25 PM GMT
Incident description	Thu Jan 18, 2007 5:46:21 IP Topology Replicator (ovrepld) on datactr1.uk.mycompany.com exiting, (View full description)
Incident type	Fault
Incident status	Closed (Reopen this incident)
Support case status	Not Created

Product	network node manager
Product related component	Server
Operating system	HP-UX B.11.11
Configuration center	myserver.us.mycompany.com
Managed client	datactr1.uk.mycompany.com
Self-Healing client version	02.60.092
System handle/SAID	MYCOMPANY2007

Contact name	john smith
E-mail address(es)	jsmith@mycompany.com
Phone number	1-866-555-1212

[Top of page](#)

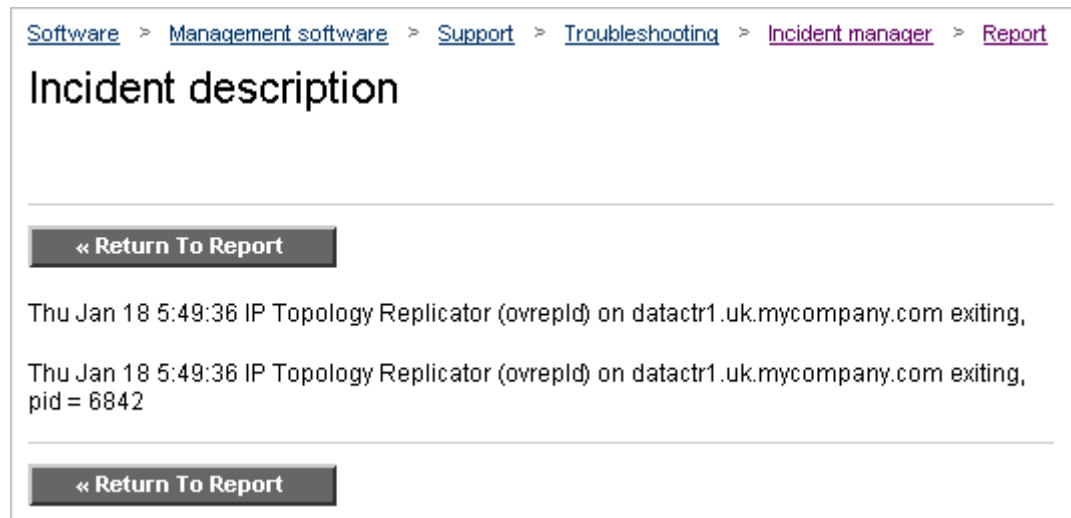
From the incident summary, you can view the full description of the incident. You can also close an incident if you no longer need it or reopen an incident that was previously closed.

To view the full incident description:

In the Incident Summary, click **View full description**. The Incident Description page opens (see Figure 5-7). Two items are displayed. The first item is a brief description of the incident; the second item is a detailed description. The items are separated by a blank line.

Figure 5-7

Incident Description Page



To close an incident:

In the Incident Summary, click **Close this incident**.

IMPORTANT

Closed incidents are deleted from the HP OpenView Self-Healing Services Support web site if they are not re-opened within 90 days (see "Report Life Cycle" on page 31 for further information).

To reopen a closed incident:

In the Incident Summary, click **Reopen this incident**.

Detailed Incident Analysis Report

The detailed Incident Analysis Report section of the report includes the following items:

- Product configuration analysis
- Patch analysis
- Document analysis
- Discussion forum analysis

NOTE

For a particular fault, some components of the report may not be included, or they may be empty.

Product Configuration Analysis

The product configuration analysis shows the parameter configuration values for the managed client that submitted the incident and compares these values to the minimum required values. Those parameters that do not have a status of “Unacceptable Values.” Those that do have a status of “Acceptable.” To view the configured and required parameter configuration values, click the name of a product in the Product Configuration Analysis table (see Figures Figure 5-8 on page 141 and Figure 5-9 on page 142). Parameter configuration values displayed in red text on the Product Configuration Analysis page are unacceptable values.

Figure 5-8 Product Configuration Analysis Example (page 1 of 2)

[Software](#) > [Management software](#) > [Support](#) > [Troubleshooting](#) > [Incident manager](#) > [Report](#)

Product configuration analysis

[« Return To Report](#)

Introduction

This report contains information about your product configuration analysis. Rows that are in **bold** are unacceptable values.

Incident summary

Incident ID	001735885805-25207778-838651725-1166368697024
Incident date/time	Jul 31, 2006 10:48:16 AM CDT
Product	network node manager
Product related component	Server 7.50
Operating system	Windows XP
Managed client	datactr2.us.mycompany.com

Reports for network node manager

- » [Physical Memory](#)
- » [Swap Space](#)

Product configuration analysis reports

Physical Memory

Configuration item	Description	Configured value	Relation	Required-value
NNM required memory ¹		1098823761920 bytes	>=	536870912 bytes

¹ Physical memory should be greater than or equal to 512MB. A higher setting may be needed to accommodate other installed software products.

[Top of page](#)

Figure 5-9 Product Configuration Analysis Example (page 2 of 2)

Swap Space

Configuration item	Description	Configured value	Relation	Required-value
NNM required swap space ¹		1819635875840 bytes	>=	536870912 bytes

¹ Operating system free swap space should greater than or equal to 512MB. A higher setting may be needed to accommodate other installed software products.

[Top of page](#)

[« Return To Report](#)

Patch Analysis

The patch analysis lists the HP OpenView application patches currently installed on the managed client that submitted the incident. This list only includes patches for applications currently supported by Self-Healing Services; it does not include operating system patches (see Figure 5-10).

Figure 5-10 Patch Analysis Summary Example (page 1 of 2)

Patch analysis

This table shows products that had a patch analysis run. Click the product to view the patch analysis for that product. There is also the option to [register for proactive patch e-mail notification](#).

Patch analysis report	Version	Patches available
Self-Healing Services	02.60.094	No
emanate SNMP agent	15.3.1.0	No
event correlation services	A.03.33	Yes
instant support enterprise edition	A.03.95.500.24	No
network node manager	7.50	Yes
operations for UNIX	A.07.22	Yes

[Top of page](#)

The **Version** column lists the application versions installed on the Self-Healing Services managed client that submitted the incident.

The **Patches Available** column indicates whether or not more recent patches are available for the application.

To see the list of patches for a specific application, click the name of the application. The detailed Patch Analysis page is displayed (see Figure 5-10 on page 142, Figure 5-11 on page 144, and Figure 5-13 on page 146). This page also lists application patches that are available, but not installed on the managed client. Click the links for each patch on this page to display additional details about the patch, so you can determine whether or not to install the patch on the managed client that submitted the incident.

Figure 5-11 Patch Analysis Detail Example for NNM (page 1 of 3)

Patch analysis

[« Return To Report](#)

Introduction

This report contains information about your patch analysis.

Incident summary

Incident ID	0007cfa24382-10387415-209848559-1952795841862
Incident date/time	Jan 26, 2007 7:16:01 AM GMT
Product	network node manager
Product related component	Server
Product version	7.50
Operating system	SunOS 5.10
Managed client	shs12

Reports for network node manager

- » Patch analysis information
 - » Current patch summary
 - » Recommended patches available for installation
 - » Optional patches available for installation
 - » Supplemental analysis notes
- » Disclaimer information
- » Generation information
- » Helpful information

Patch analysis information

Current patch summary

Patch ID	Description	Install date	Superseded by patch
PSOV_03441	Solid Database Update	Thu Dec 28 15:23:42 2006	None
PSOV_03459	Consolidated Patch 4	Thu Dec 28 15:43:15 2006	None

[Top of page](#)

Figure 5-12 Patch Analysis Detail Example for NNM (page 2 of 3)

Recommended patches available for installation

Patch ID/Description	Patch information	↓ Release date
NNMCPTSUN_00002 NNM Component Upgrade version 00002	Critical patch: None Patch dependencies: None Patch dependencies met: Hardware dependencies: None Other dependencies: None Special instructions: Yes	Jan 27, 2006
PSOV_03436 Consolidated Patch 3	Critical patch: None Patch dependencies: None Patch dependencies met: Hardware dependencies: None Other dependencies: Yes Special instructions: Yes	Jan 30, 2006
PSOV_03439 Intermediate Patch 12	Critical patch: Yes Patch dependencies: Yes PSOV_03436 Patch dependencies met: Hardware dependencies: None Other dependencies: None Special instructions: Yes	Mar 6, 2006
PSOV_03446 NNM OVPI Integration Patch	Critical patch: None Patch dependencies: None Patch dependencies met: Hardware dependencies: None Other dependencies: None Special instructions: Yes	Apr 25, 2006

[Top of page](#)

Optional patches available for installation

Patch ID/Description	Patch information	↓ Release date
None		

[Top of page](#)

Supplemental analysis notes

Patch ID	Description
None	

[Top of page](#)

Figure 5-13 Patch Analysis Detail Example for NNM (page 3 of 3)

Disclaimer information

The inventory of installed OpenView patches on a Solaris system relies on the OpenView patch text documents located in the /opt/OV/ReleaseNotes/patches directory. If these documents have been removed or they do not accurately reflect the true state of the installed OpenView patches, the patch analysis report will not accurately reflect the OpenView patches installed.

[Top of page](#)

Generation information

The following is information about the OpenView application patch analysis system (OAPAS).

OAPAS Version: oapasmgr 1.05.00 2003-02-11

[Top of page](#)

Helpful information

- » Self-solve
- » Software patches
- » Patch e-mail notification

[Top of page](#)

[« Return To Report](#)

Document Analysis

The document analysis lists the documents in the HP Support Knowledge Base that may contain information relevant to the incident. The documents are listed in order of relevance. The Score column indicates the how relevant a document is to the fault. Scores range from 0% (not relevant) to 100% (perfect match).

If a large number of documents are relevant, only the highest scoring documents are shown on the main page of the detailed Incident Analysis Report. Click the **View all document analyses for this incident** link to see a comprehensive list. To view one of the documents listed, click its title.

Figure 5-14 Document Analysis Example

Document analysis

This table shows the first 1 of 1 documents that were returned based on the analysis of your incident. The documents are sorted in descending order by score.

Title/Summary	↓ Score	Type	Date
SIGBUS in CapFilter::SymbolList using OVwAPILevel=4 in NNM application network node manager (8606340619) OVw callbacks OVwConfirmCreateSymbolsCB() and OVwConfirmDeleteSymbolsCB()	42%	known problem	Jun 4, 2004

[Top of page](#)

Discussion Forum Analysis

The discussion forum analysis lists messages from the IT Resource Center (ITRC) forums that may contain information relevant to the incident. These messages are listed in order of relevance. Click the Subject links to view the messages. Only the most relevant messages are displayed on the main page of the incident analysis report. To view all the messages identified, click the **View all discussion forum analyses for this incident** link.

Figure 5-15 Discussion Forum Analysis Example

Discussion forum analysis
This table shows the first 3 of 15 messages that were returned based on the analysis of your incident. The messages are sorted in descending order by score. To view the message detail, click on the subject link. After you view the detail you will need to click the browser back button to return to this page.

Subject	↓ Score	Date
IT Resource Center forums - HP OPENVIEW TEST EXAMS	40%	Aug 21, 2001
IT Resource Center forums - How to force NNM troubleshooting tools to use "SNMP Preferred Address" ?	38%	Oct 13, 2006
IT Resource Center forums - NNM 7.51 on 2003 r2 error starting NNM services	38%	Aug 31, 2006

» [View all discussion forum analyses for this incident](#)

Case Management and Report Feedback Utilities

The Case Management and Report Feedback section provides links you can use to open a support case for the incident and to provide feedback to HP on the incident analysis report. See “Open a Support Case” on page 148 and “Submit Feedback to HP” on page 154 for further information.

Open a Support Case

If an incident analysis report does not provide you with enough information to solve a problem yourself, you can open a support case for the incident from the incident analysis report and submit it to the HP Response Center.

Self-Healing Services provides your HP support engineer with immediate access to the collected data and system information for the incident as soon as you submit a support case. This way, your HP support engineer can quickly come up to speed with your issue before talking with you. Hence, the support engineer's first interaction with you is about a solution and not about the problem. This saves you time, as you do not need to verbally explain the problem to the support engineer. Resolution of the support case is managed based on the service level agreement between HP and your organization.

To open a support case,

1. Access the HP OpenView Self-Healing Services Support web site using the instructions on page 127.
2. Locate the incident analysis report that you want to work with using the process described in “Find an Incident Analysis Report” on page 132.
3. If the incident status on the incident analysis report is Closed, click the **Reopen this incident** link in the report to reopen it.
4. Click the **Create a support case for this incident** link at the end of the incident analysis report (see Figure 5-14 on page 146). The Create a Support Case for This Incident page is displayed (see Figure 5-16 on page 150 and Figure 5-17 on page 151).

IMPORTANT

In the **Categorize the problem** section of this page, the **Product** and **System handle/SAID** fields are pre-populated. Do not delete or change these items.

5. From the **Product version** list, choose the product version installed on the managed client where the fault occurred.
6. From the **Operating system** list, choose the operating system running on the managed client where the fault occurred.
7. Choose an **Urgency** level (Normal, High, or Critical) for your support case from the drop-down list using the guidelines in Table 5-1.

Table 5-1

Support Case Urgency Levels

Level	Meaning
Normal	Choose <i>Normal</i> if the product is usable with some restrictions or a moderate work-around and no data loss has occurred. Also, choose <i>Normal</i> if the product is usable with a simple work-around that includes rare corner cases.
High	Choose <i>High</i> if the product is usable with severe restrictions or a difficult work-around and no data loss has occurred.

Table 5-1 Support Case Urgency Levels (Continued)

Level	Meaning
Critical	Choose <i>Critical</i> if the product is unusable with no work-around, or if data loss or data corruption has occurred. Any failure requiring a restart of the client or server should be submitted as <i>Critical</i> .

8. Review the **Case title** and **Case details** supplied by Self-Healing Services, and add any information you feel would be helpful to your support engineer.

9. Review the contact information shown for your case, and make any necessary modifications. The pre-populated e-mail address and telephone number come directly from your HP Passport profile.

If you would like to change this information permanently, click the **Edit your profile** link at the very top of the page. This will take you to the profile editing functions for your HP Passport account. See “About HP Passport” on page 174 for additional information.

If you want to change the e-mail address and telephone number for this support case but not alter the information stored with your HP Passport profile, edit the pre-populated e-mail address and telephone number information on the form (see Figure 5-17 on page 151). The HP support engineer who is assigned to the support case will only have visibility to the e-mail address and telephone number you have submitted on this form.

10. Click **Send Case** to submit your support case to the appropriate HP Response Center. The HP Response Center will be selected based on your support system handle or service agreement identifier (SAID).

The Create Support Case - Thank You page is displayed with a summary of the information you provided (see Figure 5-18 on page 152).

Figure 5-16 Create a Support Case for This Incident Page (page 1 of 2)

[Software](#) > [Management software](#) > [Support](#) > [Incident manager](#) > [Report](#)

Create a support case for this incident

Instructions

This form lets you submit a new support case directly to a Hewlett-Packard Support Center. After you have completed this form, press the 'Send Case' button at the bottom of the page.

* = required fields

1. Categorize the problem

Incident ID	090013AB842C-1950483431-1529184787-1153192738155
Incident datetime	Jan 18, 2007 5:49:36 PM GMT
Product	network node manager <input type="button" value="v"/>
Product version	Select one... <input type="button" value="v"/>
Operating system	Select one... <input type="button" value="v"/>
System handle/SAID	MYCOMPANY2007 <input type="button" value="v"/>
Urgency	Normal <input type="button" value="v"/> more info
Support case ID	Will be e-mailed to you after you submit the case.

2. Enter problem details

Case title (maximum of 70 characters)*

Thu Jan 18 5:46:21 IP Topology Replicator (ovrepld) on who.na.acme.com exiting,

characters remaining for case title

Case details (maximum of 4000 characters)*

Thu Jan 18 5:46:21 IP Topology Replicator (ovrepld) on who.na.acme.com exiting, pid = 6842

characters remaining for case details

Figure 5-17 Create a Support Case for This Incident Page (page 2 of 2)

3. Provide support case contact information

The case id will be sent to your e-mail address(es) that you enter here. If you want to enter multiple e-mail addresses separate them with a semicolon (;). It will also be used to keep you informed of any changes to your case.

E-mail address* [more info](#)

Telephone number* [more info](#)

Contact preference E-mail Telephone

Figure 5-18 Create Support Case—Thank You Page

[Software](#) > [Management software](#) > [Support](#) > [Incident manager](#) > [Report](#)

Thank you

Thank you, your support case has been submitted

- Your support case has been received.
- The information you submitted is displayed below.
- You may want to print this page for your records.
- Do not click the browser back button to resubmit this case; you may lose your case.
- [Return to the incident analysis report](#) you were viewing.
- Provide additional [feedback on the analysis](#) of this incident.

Problem categorization

Incident ID	090013AB842C-1950483431-1529184787-1153192738155
Incident date/time	Jan 18, 2007 5:49:36 PM GMT
Product	network node manager
Product version	all
Operating system	all
System handle/SAID	MYCOMPANY2007
Urgency	Normal
Support case ID	Will be e-mailed to you.

Problem details

Case title
Thu Jan 18 5:49:36 IP Topology Replicator (ovrepld) on datactr1.uk.mycompany.com exiting

Case details
Thu Jan 18 5:49:36 IP Topology Replicator (ovrepld) on datactr1.uk.mycompany.com exiting, pid = 6842

Support case contact information

E-mail address	jsmith@mycompany.com
Telephone number	1-866-555-1212
Contact preference	E-mail

[Return To Report »](#)

Once you create a support case, the **Create a support case for this incident** link at the end of the incident analysis report is replaced with a **View/edit case...** link as shown in Figure 5-19. Click this link to see information about your case while it is being addressed by the HP Response Center.

Figure 5-19 Incident Analysis Report page with Support Case Created

Support case management and analysis report feedback

The following links provide the ability to View/edit the support case that you have submitted associated with this incident and the ability to provide feedback on the analysis report.

- » [View/edit case ID 3568155489 \(case submitted on Jan 26, 2007 6:45:20 AM GMT\)](#)
- » [Provide additional feedback on the analysis of this incident](#)

[Top of page](#)

NOTE

In Figure 5-19, the customer has already provided feedback on the analysis to HP, so the link now reads **Provide additional feedback on the analysis of this incident**.

Submit Feedback to HP

You can submit feedback to HP regarding the quality and usefulness of an incident analysis report by clicking the **Provide feedback on the analysis of this incident** link at the end of the incident analysis report. Your feedback is used to improve the quality and relevance of the recommended solutions in future Self-Healing Services incident analysis reports.

To submit feedback,

1. Access the HP OpenView Self-Healing Services Support web site using the instructions on page 127.
2. Locate the incident analysis report that you want to work with using the process described in “Find an Incident Analysis Report” on page 132.
3. Click the **Provide feedback on the analysis of this incident** link at the end of the incident analysis report (see Figure 5-14 on page 146). The Incident Analysis Feedback page is displayed (see Figure 5-20 on page 155 and Figure 5-21 on page 156).
4. Complete the feedback form, providing feedback on how helpful each section of the report was to you, and provide any pertinent comments. Fields marked with an asterisk are required.
5. Click **Send Feedback**.
6. The Feedback - Thank You page is displayed with a summary of the information you provided (see Figure 5-22 on page 157).

Figure 5-20 Incident Analysis Feedback Form (page 1 of 2)

[Software](#) > [Management software](#) > [Support](#) > [Incident manager](#) > [Report](#)

Incident analysis feedback

Analysis feedback instructions

Help us improve our incident analysis report by providing some feedback.

* = required fields

1. General incident analysis feedback

How helpful was the incident analysis report?*

Please select one...

Provide comments you have about the incident analysis report

4000 characters remaining for comments

2. Product configuration analysis feedback

How helpful was the product configuration analysis?*

Please select one...

Describe what part of the product configuration analysis was helpful

4000 characters remaining for product configuration analysis comments

3. Patch analysis feedback

How helpful was the patch analysis?*

Please select one...

Describe what part of the patch analysis was helpful

4000 characters remaining for patch analysis comments

Figure 5-21 Incident Analysis Feedback Form (page 2 of 2)

4. Technical document analysis feedback

How helpful was the technical document analysis? *

Please select one... ▾

Select the technical documents that helped

Helped	Document title
<input type="checkbox"/>	Patch for Mar-05 s700_800 HP-UX 11.X network node manager 7.x (PHSS_33072)
<input type="checkbox"/>	Patch for Mar-05 s700_800 HP-UX 11.X network node manager 7.x (PHSS_33073)

List any additional documents (by doc id) that helped solve this problem

5. Discussion forum analysis feedback

How helpful was the discussion forum analysis?*

Please select one... ▾

Select the discussion forum messages that helped

Helped	Message title
<input type="checkbox"/>	IT Resource Center forums - firewall configuration for Remote Console on NT
<input type="checkbox"/>	IT Resource Center forums - Extreme Switch disappear from map
<input type="checkbox"/>	IT Resource Center forums - Object in OBJ-DB not removable with ovtopofix -r
<input type="checkbox"/>	IT Resource Center forums - specify symbol/bitmap for interface type
<input type="checkbox"/>	IT Resource Center forums - oid_to_sym equivalent for ifType
<input type="checkbox"/>	IT Resource Center forums - OVTrace
<input type="checkbox"/>	IT Resource Center forums - Items showing "REMOVED:" in SelectionName
<input type="checkbox"/>	IT Resource Center forums - Sorting NNM topology database
<input type="checkbox"/>	IT Resource Center forums - HPOV NNM topology dataware house
<input type="checkbox"/>	IT Resource Center forums - Problems for send an email in automatic actions
<input type="checkbox"/>	IT Resource Center forums - Can I force a router, that I dont manage, and cannot ping into the topology of node manager?

List additional discussion forum messages (by url) that helped solve this problem

Cancel » **Send Feedback »**

Figure 5-22 Feedback - Thank You Page (1 of 2)

[Software](#) > [Management software](#) > [Support](#) > [Incident manager](#) > [Report](#)

Thank you

Thank you for your feedback

- Your incident analysis feedback has been received.
- The feedback you submitted is displayed below.
- You may want to print this page for your records.
- You can [return to the incident analysis report](#) you were viewing.

General incident analysis feedback

How helpful was the incident analysis report?
Helped a lot

Provide comments you have about the incident analysis report
This was extremely helpful and saved me hours of investigation time.

Product configuration analysis feedback

How helpful was the product configuration analysis?
Helped a lot

Describe what part of the product configuration analysis was helpful
I found a problem with my configuration right away.

Patch analysis feedback

How helpful was the patch analysis?
Helped a lot

Describe what part of the patch analysis was helpful
I needed two patches that I was previously unaware of.

Technical document analysis feedback

How helpful was the technical document analysis?
Helped a lot

Select the technical documents that helped

- [Patch for Mar-05 s700 800 HP-UX 11.X network node manager 7.x \(PHSS 33072\)](#)
- [Patch for Mar-05 s700 800 HP-UX 11.X network node manager 7.x \(PHSS 33073\)](#)

List any additional documents (by doc id) that helped solve this problem

- No additional documents listed.

Figure 5-23 Feedback - Thank You Page (2 of 2)

Discussion forum analysis feedback

How helpful was the discussion forum analysis?
Helped a lot

Select the discussion forum messages that helped

- [IT Resource Center forums - HPOV NNM topology dataware house](#)
- [IT Resource Center forums - NNM and VLAN topology](#)
- [IT Resource Center forums - Sorting NNM topology database](#)

List any additional discussion forum messages (by url) that helped solve this problem

- No additional discussion forum messages listed.

[Return To Report »](#)

Change the System Handle/SAID Associated with an Incident

When an incident package is submitted to HP, the system handle/service agreement identifier (SAID) you provided on the Self-Healing Services client user interface (UI) Contact Information page is submitted with it. The system handle/SAID is used for entitlement to HP OpenView Self-Healing Services. If the system handle/SAID is valid, the incident passes the entitlement check. The incident is then “received” by Self-Healing Services, and a custom incident analysis report is generated.

The system handle/SAID submitted with an incident can expire. If it does, you will no longer have access to view the incident or its analysis report until you re-associate the incident with a new valid system handle/SAID and add the new system handle/SAID to your HP Passport profile.

You can change the system handle/SAID associated with any of your submitted incidents from your HP OpenView Self-Healing Support web pages.

To re-associate an incident:

1. Access the HP OpenView Self-Healing Services Support web site using the instructions on page 127.
2. Click the **Re-associate incident** link in the left navigation menu. The Re-associate Incident page is displayed (see Figure 5-24 on page 160).
3. In the **Incident ID** box, type or paste the incident ID.

TIP

The incident ID can be found in the Report Available service notification you received by e-mail (see Figure 6-2 on page 182).

4. From the **System handle/SAID** list, choose the new system handle/SAID that you want to associate with the incident.

NOTE

If you do not see the system handle or SAID that you want to use in the drop-down list, add the system handle/SAID to the list by clicking the **Support contract info** link and adding this system handle/SAID to your HP Passport profile as described in “View Your Support Contract Information” on page 162.

5. Select the **Update all incidents...** box if you also want to re-associate all the incidents associated with the same system handle/SAID as the incident you typed above.
6. Click **Next**. The Incidents to be Re-associated page is displayed (see Figure 5-25 on page 161).
7. If you approve of the incident re-associations listed on the Incidents to be Re-associated page, click **Re-associate Incidents**. The System Handle/SAID Updated page is displayed (see Figure 5-26 on page 161).
8. If you do *not* approve of the incident re-associations listed, click **Previous Page**, and change your selections.

Figure 5-24 Re-associate Incident Page

[Software](#) > [Management software](#) > [Support](#) > [Troubleshooting](#) > [Incident manager](#)

Re-associate incident

Step 1 of 2

Instructions

- Enter an incident id and select a system handle/SAID you want to associate with that incident.
- If you want to update all incidents that use the same system handle/SAID as the incident identifier you select below, please check the check box.
- Click 'Next' button to continue.

* = required field

System handle/SAID and incident information

Incident ID*

System handle/SAID*

Update all incidents that have the same system handle/SAID as the incident entered above.

Note: If you do not see a system handle/SAID in the drop-down list above that you want to use, please go to your [support contract information to update your system handles/SAIDs](#).

Figure 5-25 Incidents to be Re-associated Page

[Software](#) > [Management software](#) > [Support](#) > [Troubleshooting](#) > [Incident manager](#)

Incidents to be re-associated

Step 2 of 2

Important information

- The following incident ID's will be re-associated to the new system handle/SAID.
- In addition, any new incidents currently being processed will be updated.
- Select the "Re-associate Incidents" button to complete this change.

Incident ID	Date/Time	Old system handle/SAID	New system handle/SAID
0010B57A9D08-17330512-412101159-1110840170948	Jan 14, 2007 10:42:50 PM GMT	MYCOMPANY2006	MYCOMPANY2007

[« Previous Page](#) [Cancel »](#) [Re-associate Incidents »](#)

Figure 5-26 System Handle/SAID Updated page

[Software](#) > [Management software](#) > [Support](#) > [Troubleshooting](#) > [Incident manager](#)

System handle/SAID updated

Important information

- To avoid creation of additional incidents with the previous system handle/SAID you must update the system handle/SAID on the Self-Healing.
- All of your selected incidents should be updated with the new system handle/SAID within the next hour.
- To view other incidents you may want to [go to the main page](#).

System handle/SAID and incident information

Incident ID	0010B57A9D08-17330512-412101159-1110840170948
Incident date/time	Mar 14, 2005 4:42:50 PM CST
Incident description	Application Monitor did not get started since no fault configuration file could
Managed node	myserver.us.mycompany.com

Old system Handle/SAID	MYCOMPANY2006
New system Handle/SAID	MYCOMPANY2007

[Go to Main Page »](#)

View Your Support Contract Information

You can view and modify your HP support contract information at any time from your HP OpenView Self-Healing Services Support web pages. This information includes all system handles/SAIDs that you have added to your HP Passport profile. The following information is available for each of your system handles/SAIDs:

- Expiration date
- Status (Active or Inactive)
- Number of support contract incidents available for that system handle/SAID.

To view your HP support contract information:

1. Access the HP OpenView Self-Healing Services Support web site using the instructions on page 127.
2. Click the **Support contract info** link in the left navigation menu. The Support Contract Information page is displayed (see Figure 5-27 on page 163).

To add a system handle/SAID to your profile,

1. In the **System handle or SAID** box, type or paste the system handle or SAID exactly as it appears in your HP support contract. Your system handle/SAID is case-sensitive.

NOTE

Your HP support contract may refer to your System Handle/SAID as your “Support Account Reference.”

2. Click **Add System Handle/SAID to Profile**. The new system handle/SAID is added to your list.

If you are unable to add a system handle/SAID that you believe to be valid to your HP Passport profile, you can submit a request for HP to research your HP support contract.

To ask HP to research your support contract:

1. Click the **Investigate my contracts, system handles, or service agreement identifiers** link.
2. Provide as much of the information requested on the Investigate Support Contract page as you can to enable HP to research your support contract (see Figure 5-28 on page 164).
3. Click **Submit**. The Investigate Support Contract - Thank You page is displayed with a summary of the information you provided (see Figure 5-30 on page 166).
4. Click **Continue**.

To delete a system handle/SAID from your profile:

1. Click the **Delete** link for that system handle/SAID. A dialog box opens asking you if you really want to delete this system handle/SAID.
2. Click **OK**.

To get HP Sales contact information:

Click **Contact HP sales for assistance** to view a list of HP OpenView resellers, US and Canadian sales contact e-mail addresses and phone numbers, and international sales contact e-mail addresses and phone numbers.

Figure 5-27 Support Contract Information Page

[Software](#) > [HP OpenView](#) > [Support](#)

Support contract information

Support contract information

This table displays software contract system handles and/or service agreement identifiers (SAIDs) that are associated with your HP Passport profile.

System handle/ Service agreement ID (SAID)	Expiration date	Status	Incidents available	Delete
MYCOMPANY2007	Dec 11, 2005	Active	Not limited	Delete
MYCOMPANY2006	Dec 11, 2004	Inactive		Delete

Add a system handle or SAID to your profile

System handle or SAID:

Add System Handle/SAID to Profile »

Finished »

Assistance options

- » Investigate my contracts, system handles, or service agreement identifiers
- » Contact HP sales for sales assistance

NOTE Anytime that you want to return to the Self-Healing Services support web site, click **Finished**.

Figure 5-28 Investigate Support Contract Page (1 of 2)

[Software](#) > [HP OpenView](#) > [Support](#)

Investigate support contract

Instructions

Please complete as much as possible of the information requested below to enable Hewlett-Packard to research your contract. You can check on the status of the investigation by sending this form again. We try to complete all investigations within three business days, and notify customers of the findings via e-mail. Currently, Kanji characters are not supported.

* = required fields.

Contact information

First name:*	<input type="text" value="John"/>
Last name:*	<input type="text" value="Smith"/>
Title:	<input type="text"/>
Company/Organization:*	<input type="text"/>
Address:	<input type="text"/>
Address line 2:	<input type="text"/>
City:	<input type="text"/>
State/Province:	<input type="text"/>
Zip/Postal code:	<input type="text"/>
Country/Region:*	<input type="text" value="United States"/>
E-mail address:*	<input type="text" value="jsmith@mycompany.com"/>
Business phone:	<input type="text" value="+0"/>
Fax number:	<input type="text" value="+0"/>

Figure 5-29 Investigate Support Contract Page (2 of 2)

Investigation information

Your system handle or SAID:*

Product associated with contract:

Description of the situation and details about why a contract investigation is being requested:*

Figure 5-30 Investigate Support Contract - Thank You Page

[Software](#) > [HP OpenView](#) > [Support](#)

Investigate support contract

Thank you for your request

- Your support contract request has been received.
- The request you submitted is displayed below.
- You may want to print this page for your records.

Contact information

First name:	John
Last name:	Smith
Title:	IT
Company/Organization:	HP
Address:	128 Happy Canyon Road
Address line 2:	Suite 200
City:	Clear Valley
State/Province:	CA
Zip/Postal code:	12345
Country/Region:	United States
E-mail address:	jsmith@mycompany.com
Business phone:	1 (866) 555 1212
Fax number:	

Investigation information

Your system handle or SAID:	MYCOMPANY2007
Product associated with contract:	NNM

Description of the situation and details about why a contract investigation is being requested:
Unable to add valid system handle to HP Passport

Continue »

Metric Reports

Metric reports tally the number of faults that occur, incidents that are generated, or support cases that are opened for a single managed node or for all the managed nodes in a Self-Healing Services managed environment over a specific period of time.

Metric reports provide a snapshot of Self-Healing Services activities that have taken place in your environment over a specified period of time. Using a metric report, you can quickly determine the following things for any or all of your managed nodes:

- Number of faults that were detected
- Number of incidents that were submitted
- Number of support cases that were created

You can create and view metric reports in the Incident Manager on the HP OpenView Self-Healing Services Support web page. When you create a metric report, you can use the following filter criteria:

- HP OpenView product (or products)
- Managed node (or nodes)
- Date range
- System handle (or SAID)

You can create metric reports for one particular managed node or all the managed nodes associated with the system handle/SAID that you specify. Likewise, you can create reports for one specific product or all products associated with that system handle/SAID.

There are three types of metric reports available:

Report Type	Description
Incident frequency report	An incident frequency report shows you how many times a particular incident occurred during the specified time period. The data is summarized by month. Sample incident frequency report
Fault frequency report	A fault frequency report shows you the total number of incidents that occurred during the specified time period. The data is summarized by month. Unlike the incident frequency report, the fault frequency report does not indicate which specific incidents occurred or which HP OpenView products were involved. Sample fault frequency report
Case creation report	A case creation report shows you how many support cases were created during the specified time period. The data is organized by managed node and then by product. The total number of support cases is shown for each managed node included in the report. Sample case creation report

NOTE These reports only include incidents that are associated with actual faults. They do not include incidents associated with manually submitted incidents, system assessments, audits, additional data submissions, or connectivity tests.

TIP Metric reports are presented in portable document format (PDF). To view a metric report, you must use the Adobe Acrobat Reader. You can download a free copy of the reader at the following web site:

<http://www.adobe.com>

View your metric reports

You can view existing metric reports using the Incident Manager at the HP OpenView Self-Healing Services Support web site. You must have an active support contract and valid HP Passport sign-in to view your reports.

To access the HP OpenView Self-Healing Services Support web site:

1. Open a web browser and go to the following address:

<http://support.openview.hp.com/software/analysis/main>

The HP Passport Sign-In page opens.

2. In the **User ID** box, type your HP Passport user ID.
3. In the **Password** box, type your HP Passport password.
4. Click **Sign-in**.

To view an existing metric report:

1. In the left navigation menu, click **Metric reports**.

The Metric Report page appears. The reports are listed in order from most recent to least recent. Any reports generated during the last 24 hours have a **NEW!** icon. Only the 20 most recent reports created during the last 30 days are listed. Reports more than 30 days old are removed from the system.

2. To view a report, click the **Date/Time generated** link for that report.

The File Download dialog opens.

3. Choose one of the following options:

- Click **Open** to view the report from its current location.

The PDF file containing the report is displayed in a new window.

- Click **Save** to save a copy of the report locally.

Browse to a location of your choice, and save the PDF file.

Create a metric report

A metric report is truly a snapshot in time. After a metric report is created, it is not updated as new information becomes available. You can create a new metric report at any time, however, using the Metric Report page on the HP OpenView Self-Healing Services web site.

Before you can work with metric reports, you must log on to the web site using HP Passport. See view your metric reports for details. The following instructions assume that you have logged on and are now viewing the Metrics Report page.

To create a new metric report:

1. Click the **Create New Report** button.

The Create New Report page opens.

2. In the **Description of report** box, type a description for your report that will differentiate it from the other reports in the list.

3. From the **Report type** list, choose the type of report that you want to create.

For information about report types, see page 167.

4. From the **System Handle/SAID** list, choose the system handle (or SAID) that is associated with the faults, incidents, or support cases that you want to work with.

5. *Optional:* From the **Product** list, choose the specific HP OpenView product whose faults, incidents, or support cases you want to view, or choose All products.

6. *Optional:* From the **Managed node** list, choose the specific managed node that you want to work with, or choose All managed nodes.

7. Click the calendar button to the right of the **Start date** box, and choose the date that you want to start the reporting interval.

8. Click the calendar button to the right of the **End date** box, and choose the date that you want to end the reporting interval.

9. In the **E-mail address** box, type your e-mail address.

The E-mail address box is prepopulated with the e-mail address from your HP Passport profile. You can specify a different address if you prefer.

10. Click **Create Report**.

The Thank You page appears. After Self-Healing Services creates your report, it sends you an e-mail notifying you that the report is available and providing a link that you can click to view the report.

Copy a metric report

You can use an existing metric report as a template for a new report. This saves you time, for example, if you want to generate the same report you created last month and simply change the dates and title.

Before you can work with metric reports, you must log on to the web site using HP Passport. See view your metric reports for details for details. The following instructions assume that you have logged on and are now viewing the Metrics Report page.

To copy an existing metric report:

1. On the Metric Reports page, click the **Copy** link for the report that you want to copy.

The Copy of a Report page appears. The fields on this page are filled out identically to the report you copied.

2. Change any of the fields that you want to customize for the new report. To return all the fields to the state they were in when you clicked the Copy link, click **Reset**.
3. Click **Create Report**.

The Thank You page appears. After Self-Healing Services creates the new report, it sends you an e-mail notifying you that the report is available and providing a link you can click to view the report.

Delete a Metric Report

You can delete any metric report that you have the ability to view. After a report is deleted, it cannot be retrieved.

Before you can work with metric reports, you must log on to the web site using HP Passport. See view your metric reports for details. The following instructions assume that you have logged on and are now viewing the Metrics Report page.

To delete a metric report:

1. On the Metric Reports page, click the **Delete** link for the report that you want to delete.
2. Click **OK** to delete the report.

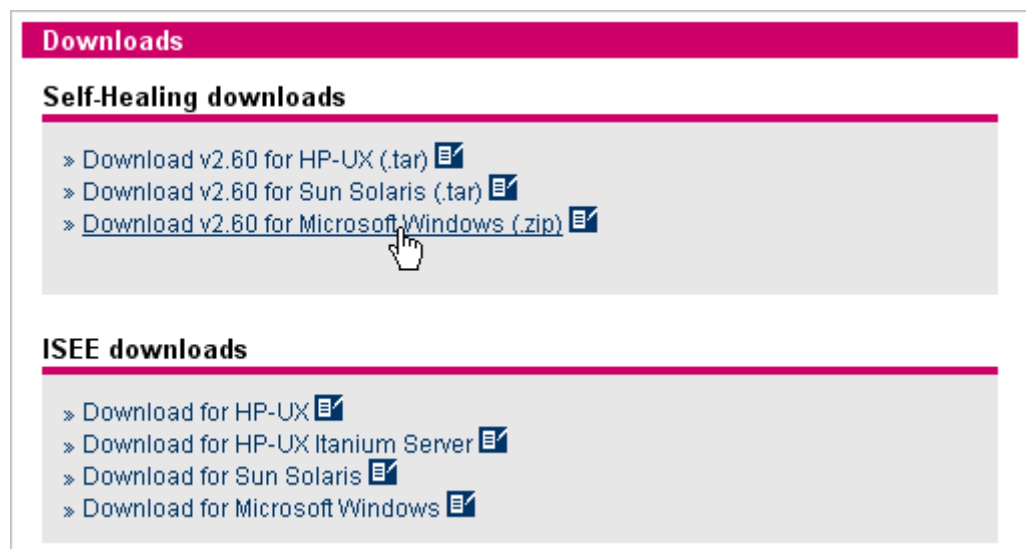
The report is deleted, and the table of reports is updated to reflect this.

Download Client Software

You can download the latest Self-Healing Services and/or ISEE client software from your HP OpenView Self-Healing Services Support web pages.

To download client software:

1. Access the HP OpenView Self-Healing Services Support web site using the instructions on page 127.
2. Click the **Downloads** link. The Download Software page is displayed.
3. In the Downloads section of the page, click the Self-Healing Services or ISEE client link for the operating system running on the node where you will install it.



4. Read the HP Software License Terms.
5. Click **I Agree** if you accept the terms of the license.
6. Save the file on your local system.

In addition to the client software, you can download the following documents from the Self-Healing Services Download Software page:

- *HP OpenView Self-Healing Services User's Guide*
- *HP OpenView Self-Healing Services Installation Guide*
- Quick Installation & Configuration Guides for the Self-Healing Services Client
- Quick Installation & Configuration Guides for the ISEE Client
- Frequently Asked Questions (FAQ)
- Self-Healing Services Data Sheet
- Self-Healing Services White Paper

NOTE You can also reach the Download Software page using the link in the Self-Healing Services user interface or directly using the following web address:

http://support.openview.hp.com/self_healing_downloads.jsp

Your Self-Healing Services Sign-In Information

If you forget your user name or password for Self-Healing Services, you can request this information from HP.

To retrieve your user name and password:

1. On the Sign-In page, click **Forgot user name and/or password**.
2. Click **Send info**.

Self-Healing Services will e-mail your user name and password to the e-mail address specified on your User Name & Password page. If you did not specify an e-mail address on the User Name & Password page, the e-mail address specified on your Contact Information page is used.

About HP Passport

HP Passport is a single login service that lets you register with HP Passport-enabled web sites using a single user identifier and password of your choice. HP Passport stores your basic personal information—user ID, password, name, e-mail address, country and language preferences—so you don't have to retype it when you return to one of HP's many web sites in the future.

HP Passport profile information is protected by industry-standard encryption technology and follows strict HP privacy policies.

If you have forgotten your HP Passport password, you must establish a new password.

To establish a new HP Passport password,

1. Click the **Forgot password** link. The **Forgot Your HP Passport Password** page is displayed (see Figure 5-31).
2. Follow the on-screen instructions to establish a new password.

Figure 5-31 Forgot Your HP Passport Password Page

Forgot HP Passport password


If you have forgotten your HP Passport password, you will need to choose a new one. Simply follow these steps:

- 1) **Enter your user ID and e-mail address below.** This information is used to authenticate your request.
- 2) You will **receive an e-mail message from HP** containing a Web hyperlink that authorizes you to change your password. Click the hyperlink in the e-mail message to begin the process.
- 3) You will be prompted to **enter your user ID again**, then **enter a new password**.


To begin, enter your user ID and e-mail address below, then click "Submit".

* = Required field

User information

User ID* 

E-mail address*

 **Secure**

If you are new to HP Support, you must create a new HP Passport user account.

To create a new HP Passport account:

1. Click the **New users - please register** link. The HP Passport New User Registration page is displayed (see Figure 5-32 on page 177).
2. Type the **User ID** and **Password** you want to use when you sign-in to HP Passport.
3. In the **Confirm password** box, type your password in again.
4. Type your **First name**, **Last name**, and **E-mail address**.
5. From the respective drop-down lists, select your **Preferred language** and your **Country/region** of residence.
6. In the HP Privacy Policy, select the appropriate radio buttons to specify how you want HP to contact you.
7. *Optional:* If you want to provide business or home contact information, click **Optional Contact Information**, and fill in the information that you want to provide.
8. Click **Continue**. This creates your HP Passport account.
9. To use your account with Self-Healing Services, you will need to add at least one system handle or SAID to your HP Passport profile. See “View Your Support Contract Information” on page 162 for additional information.


Figure 5-32 HP Passport New User Registration Page

HP Passport new user registration

HP Passport is a single login service that lets you register with HP Passport-enabled Web sites using a single user identifier and password of your choice.

* = Required field


Sign-in information

User ID* 
(Minimum 5 characters letters, numbers and special characters)

Password*
(Minimum 6 characters letters, numbers and special characters)

Confirm password*

Personal information

Title (Mr., Ms.) 

First name*

Middle name


Last name*

E-mail address*
(E-mail address must be different for each user ID)

Preferred language*

Country/Region of residence*

HP Privacy policy

Occasionally HP communicates information on products, services and/or support that may be relevant to you. This may include new product information, special offers or possibly an invitation to participate in market research. 


Click 'Yes' if HP may contact you by the method described, or click 'No' if you do not want HP to contact you by that method.

E-mail* Yes No

Postal mail Yes No

Phone Yes No

To provide business and home contact information, click "Optional Contact Information".

 **Secure**

6 Understanding Service Notifications

This chapter describes the Self-Healing Services service notifications you will receive from HP when you install Self-Healing Services, when an incident is submitted to HP through Self-Healing Services, when a fault is submitted to HP with an invalid system handle/SAID, or when you upload additional data for an open support case and submit it to HP through Self-Healing Services.

In This Chapter

This chapter describes the following service notifications:

- “Welcome to Self-Healing Services Notification” on page 181
- “Report Available Notification” on page 182
- “Entitlement Action Required Notification” on page 183
- “Additional Data Requested Notification” on page 187
- “Additional Data Received Notification” on page 188
- “Metric Report Available Notification” on page 189

Welcome to Self-Healing Services Notification

You will receive a Welcome to HP OpenView Self-Healing Services notification when the Self-Healing Services client is successfully installed and your connection to HP using ISEE is operating correctly (see Figure 6-1). You will also receive this notification each time you change your Contact Information in the Self-Healing Services client user interface and click the **Save and Send Connectivity Test** button.

Figure 6-1

Welcome to HP OpenView Self-Healing Services Notification

```
From: HP OpenView Software Support  
[mailto:openview-self-healing@hp.com]  
Sent: Sunday, December 03, 2006 10:26 AM  
To: Smith, John  
Subject: Welcome to HP OpenView Self-Healing Services!  
  
This message has been automatically generated. Please do not reply  
to this message.  
  
Welcome to HP OpenView Self-Healing Services! You have  
successfully configured your software and are now connected. These  
services will provide you with customized assistance to help you  
solve your software difficulties and keep your systems running  
smoothly.  
  
Date/Time:          Dec 3, 2006 5:24:54 PM GMT  
System name:       myserver.us.mycompany.com  
  
Your feedback is valuable to us. Please take a few minutes to  
participate in a short survey regarding your experience with  
installing and configuring HP OpenView Self-Healing Services.  
This survey should only take a few minutes and will help us to  
improve our service to you. If you would like to participate in  
the survey, please go to the below web address:  
  
Thank you,  
HP OpenView Self-Healing Services Team
```

Report Available Notification

When an incident is submitted to HP, a custom analysis incident report is created for that incident and published to a private HP OpenView Self-Healing Services Support web page. Once the analysis incident report is available on the web, you will receive a service notification containing a link to the analysis incident report (see Figure 6-2).

Figure 6-2 Report Available Notification

```
From: HP OpenView Software Support
[mailto:openview-self-healing@hp.com]
Sent: Saturday, December 02, 2006 12:22 PM
To: Smith, John
Subject: Report Available: "Test 1" - HP OpenView Self-Healing
Services

This message has been automatically generated. Please do not reply
to this message.

Your recently submitted HP OpenView Self-Healing Services incident
has been analyzed, a report has been generated and it is available
on the HP OpenView Support web site. Please view your HP OpenView
Incident Analysis Report at the following web address (HP Passport
sign-in & active support contract required):

-
http://support.openview.hp.com/software/analysis/report?incident=
000000000000-00000000-0000000000-000000000000

After you sign-in with an HP Passport account, you may need to
provide the HP OpenView Support system handle / service agreement
identifier (SAID) which was used to submit the incident. You can
find this system handle / SAID in the HP OpenView Self-Healing
Services client contact information located on the system from
which this incident was submitted.

This report will provide you with customized information and
assistance to help you solve your software difficulties and keep
your systems running smoothly. In the event that you require
personal assistance, you will also be able to create a support
case for this incident from the incident analysis report.

Incident Summary:

Date/Time:          Dec 2, 2006 7:15:09 PM GMT
System name:        myserver.us.mycompany.com
Product:            Self-Healing Services
Incident ID:        000000000000-00000000-0000000000-000000000000
Short description:  Test 1

Problem Detail:

This will test the submission path and notification flow.

Thank you,
HP OpenView Self-Healing Services Team
```

Entitlement Action Required Notification

If an incident or system assessment is submitted to HP with an invalid system handle or service agreement identifier (SAID), you will receive a service notification by e-mail informing you there is an entitlement issue and the incident cannot be processed by HP until it is corrected (see Figure 6-4 and Figure 6-5).

The following conditions will cause entitlement problems:

- Your support contract has expired.
- Your system handle or SAID has changed.
- You typed your system handle or SAID incorrectly when you customized your contact information using the Self-Healing Services client user interface (see Figure 3-7 on page 67)

NOTE

Your system handle is case-sensitive, so make sure your customer-specific HP OpenView application system handle or SAID in the **System handle/SAID** field on the Contact Information page exactly matches what appears in your HP support contract.

To correct an entitlement issue:

1. Read the entire e-mail message.
2. Click the link in the e-mail. If you are not already signed in to HP Passport, The HP Passport Sign-In page opens.
3. If the HP Passport Sign-In page opens, sign in to HP Passport. See “Access the Self-Healing Services Support Web Site” on page 127 for additional information.

After you sign in to HP Passport, the Invalid System Handle/SAID page opens (see Figure 6-3).

4. From the **System handle/SAID** list, select the system handle or SAID that you want to associate with the incident from the list.

If the system handle or SAID that you want to use does not appear in the list, follow these steps:

- a. Click the **support contract information to update your system handles/SAIDs** link at the bottom of the page.
 - b. Follow the instructions on page 162 to add the system handle or SAID to your HP Passport profile. Remember that your system handle/SAID is case-sensitive.
5. Follow the instructions in “Change the System Handle/SAID Associated with an Incident” on page 159 to re-associate the valid system handle/SAID with the incident.
 6. On the configuration center to which the managed client that submitted the incident is assigned, delete the invalid system handle/SAID, and replace it with a valid one (see “Change Your Contact Information” on page 66 for instructions).

NOTE If you are unable to correct the entitlement issue, you can initiate an investigation of your support contract from the Support Contract Information page (see Figure 5-27 on page 163) by clicking the **Investigate my contracts, system handles, or service agreement identifiers** link.

Figure 6-3 Invalid System Handle/SAID page

[Software](#) > [Management software](#) > [Support](#) > [Troubleshooting](#) > [Incident manager](#)

Invalid system handle/SAID

Step 1 of 2

Invalid system handle/service agreement identifier (SAID)

The system handle or service agreement identifier (SAID) you entered during the installation of Self-Healing Client does not match any of the system handles/SAIDs that are currently entitled on software support contract. This could be due to:

- You may have mistyped your system handle/SAID when you installed Self-Healing Client
- Your support contract may have expired.
- Your system handle/SAID may have changed.

System handle/SAID and incident information

Incident ID	000000000000-00000000-0000000000-000000000000
Incident date/time	December 3, 2006 05:25:07 PM GMT
Incident description	Test
Managed node	myserver.us.mycompany.com
Incorrect system handle/SAID	MYCOMPANY2006

Available system handles/SAIDs*

Update all incidents that have MYCOMPANY2006 as their system handle/SAID.

Note: If you do not see a system handle/SAID in the drop-down list above that you want to use, please go to your [support contract information to update your system handles/SAIDs](#).

Figure 6-4 Entitlement Action Required Notification for an Incident

```
From: HP OpenView Software Support
[mailto:openview-self-healing@hp.com]
Sent: Sunday, December 03, 2006 10:26 AM
To: Smith, John
Subject: Entitlement Action Required - HP OpenView Self-Healing
Services

This message has been automatically generated. Please do not reply
to this message.

HP OpenView Self-Healing software attempted to process your recent
submission. The processing has been temporarily suspended due to
an entitlement issue. The support system handle / service
agreement ID (SAID) under which the incident was originally
submitted under is not valid for HP OpenView Self-Healing Services
and must be reconciled before the incident can be processed.

Take the following steps to resolve this issue:

    1. Visit the following web address and correct your
entitlement for this incident: (HP Passport sign-in required)
-
http://support.openview.hp.com/software/analysis/invalid-
handle?incident=000000000000-00000000-0000000000-
000000000000&passkey=123456789

    2. Once you finish the process at the above web address,
correct the system handle / SAID in the Self-Healing software
configuration on the system where the incident originated so that
future submissions will be entitled.

If you are unable to reconcile your entitlement at the above web
address you may do the following to obtain a valid system handle /
SAID. However you will still need to perform the above two steps
for the incident to process.

    - Initiate an investigation of your system handle / SAID
    - Or contact your support agreement specialist

Incident Summary:

Date/Time:      Dec 3, 2006 5:25:07 PM GMT
System name:    myserver.us.mycompany.com
Product:
Incident ID:    000000000000-00000000-0000000000-000000000000
Short description:

Your information will be fully processed shortly after entitlement
has been verified.

Thank you,
HP OpenView Self-Healing Services Team
```

Figure 6-5 Entitlement Action Required Notification for a System Assessment

From: HP OpenView Software Support
[mailto:openview-self-healing@hp.com]
Sent: Sunday, December 03, 2006 10:26 AM
To: Smith, John
Subject: Entitlement Action Required - HP OpenView Self-Healing Services

This message has been automatically generated. Please do not reply to this message.

HP OpenView Self-Healing software attempted to process your recent system assessment submission. The processing has been temporarily suspended due to an entitlement issue. The support system handle / service agreement ID (SAID) under which the system assessment was originally submitted under is not valid for HP OpenView Self-Healing Services and must be reconciled before the incident can be processed.

A system assessment requires a Software Support Enhanced contract.

Take the following steps to resolve this issue:

1. Visit the following web address and correct your entitlement for this incident: (HP Passport sign-in required)
-
<http://support.openview.hp.com/software/analysis/invalid-handle?incident=000000000000-00000000-0000000000-000000000000&passkey=123456789>
2. Once you finish the process at the above web address, correct the system handle / SAID in the Self-Healing software configuration on the system where the incident originated so that future submissions will be entitled.

If you are unable to reconcile your entitlement at the above web address you may do the following to obtain a valid system handle / SAID. However you will still need to perform the above two steps for the incident to process.

- Initiate an investigation of your system handle / SAID
- Or contact your support agreement specialist

Incident Summary:

Date/Time: Dec 3, 2006 5:25:07 PM GMT
System name: myserver.us.mycompany.com
Product:
Incident ID: 000000000000-00000000-0000000000-000000000000
Short description:

Your information will be fully processed shortly after entitlement has been verified.

Thank you,
HP OpenView Self-Healing Services Team

Additional Data Requested Notification

If you have opened a support case for a particular incident, you may receive a request from Self-Healing Services for additional data. If a support engineer requests additional data about the incident, you will receive a notification asking you to view the incident analysis report and retrieve the request. You can fulfil the request by using the upload additional data function on the Self-Healing Services client user interface on the node where the incident occurred.

Figure 6-6

Additional Data Requested Notification Example

```
From: HP OpenView Software Support
[mailto:openview-selfhealing@hp.com]
Sent: Sunday, December 03, 2006 08:35 AM
To: Smith, John
Subject: Additional Data Requested for Support Case - HP Open View
Self-Healing Services

This message has been automatically generated. Please do not reply
to this message.

HP Software Support is requested additional data from you with
regard to the support case (SampleCaseID) that you submitted for
incident 000000000000-00000000-0000000000-000000000000. Please
view the additional data request and the instructions on how to
submit any data files at the web address below (HP Passport sign-
in & active support contract required):

- http://support.openview.hp.com/software/analysis/report?inc
ident=000000000000-00000000-0000000000-000000000000

Support Case Summary:

Date/Time:          December 3, 2006 12:02:55 AM GMT
Support Case ID:    SampleCaseID
Title:              Sample Support Case

Incident Summary:

Date/Time:          December 2, 2006 5:01:46 PM GMT
System name:        myserver.us.mycompany.com
Product:            network node manager
Incident ID:        000000000000-00000000-0000000000-
000000000000
Short description:  File does not exist

Problem Detail:

File does not exist.

Thank you,
HP OpenView Self-Healing Services Team
```

Additional Data Received Notification

You can provide HP with additional data pertaining to a previously submitted incident by uploading a file and submitting it to HP from the Incident Details page (see Figure 4-3 on page 101). Shortly after you submit additional data for an incident, you will receive a service notification indicating that the additional data was received and containing a link to view the incident package (see Figure 6-7 for an example).

Figure 6-7 Additional Data Received Notification

```
From: HP OpenView Software Support
[mailto:openview-self-healing@hp.com]
Sent: Sunday, December 03, 2006 11:44 AM
To: Smith, John
Subject: Additional Data Received - HP OpenView Self-Healing
Services

This message has been automatically generated. Please do not reply
to this message.

We have received additional data for a previously submitted
incident (000000000000-00000000-0000000000-000000000000). The web
address below can be used to view this incident (HP Passport sign-
in & active support contract required):
-
http://support.openview.hp.com/software/analysis/report?incident=000000000000-00000000-0000000000-000000000000

Incident Summary:

Date/Time:          Dec 2, 2006 5:01:46 PM GMT
System name:        myserver.us.mycompany.com
Product:            network node manager
Incident ID:        000000000000-00000000-0000000000-000000000000
Short description:  File does not exist

Problem Detail:

This will test the submission path and notification flow.

Thank you,
HP OpenView Self-Healing Services Team
```

Metric Report Available Notification

After Self-Healing Services generates a metric report for you, it sends you a service notification e-mail with instructions for accessing the report.

Figure 6-8

Metric Report Available

```
From: ovshs_feedback@hp.com
Sent: Sunday, December 03, 2006 10:15 PM
To: Smith, John
Subject: Metrics Report Available - HP OpenView Self-Healing
Services

This message has been automatically generated. Please do not reply
to this message.

Your recently submitted request for the Incident frequency report
has been processed and the data is now available on the HP
OpenView Support web site. Please access the report at the
following web address (HP Passport sign-in & active support
contract required):
- https://support.openview.hp.com/software/analysis/metric-
reports

After you sign-in with an HP Passport account, you may need to
provide the HP OpenView Support system handle / service agreement
identifier (SAID) which was used to submit the request.

Thank you,
HP OpenView Self-Healing Services Team
```

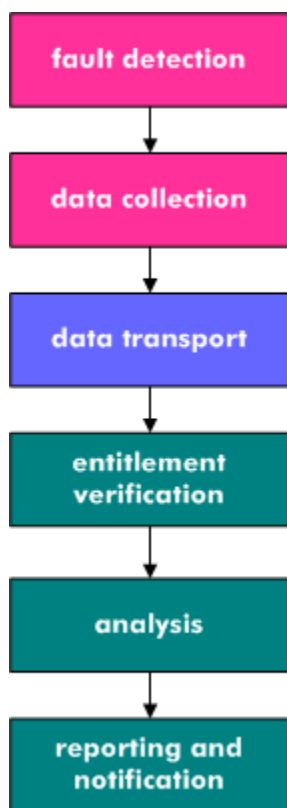
7 Troubleshooting Information

This chapter contains information you can use to troubleshoot problems with your Self-Healing Services managed environment.

Understanding Potential Problem Locations

The self-healing process has six primary steps, as discussed in “Self-Healing Process” on page 29. The first two steps, fault detection and data collection, take place entirely on the managed clients. The next step, data transport, takes place through ISEE. The ISEE client, which initiates the data transport, runs on one or more communication gateways and sends data to an HP ISEE server. The following three steps - entitlement verification, analysis, and reporting and notification - are initiated on a collection of HP OpenView support servers.

Self-Healing Services Process



Problems can potentially occur *during* each of these six primary steps or *between* them. The first troubleshooting task is to pinpoint the location of the problem. After you identify the location of the problem, you can proceed to determine its root cause and take action to resolve it.

Fault Detection Problems

Fault detection problems can occur for a number of reasons. For example, the Self-Healing Services client may not be installed correctly or the client may not be running. The OpenView application being monitored may not be able to communicate with the Self-Healing Services client. The fault rules may have been customized to suppress or ignore all potential faults.

Data Collection Problems

The Self-Healing Services client can fail to collect data when a fault occurs. You can view the data collected for a fault instance using the Incident Viewer (see “View Incidents and Collected Data” on page 97). If an error has occurred in the data collection process, an error message will be displayed in the Incident Viewer.

Data Transport Problems

Incident packages are transported to HP using the ISEE client installed on the communication gateway(s). If the ISEE client was not installed properly, it will be unable to send incident packages to HP. If the ISEE client cannot connect to the ISEE server, it will be unable to send incident packages to HP. This can occur, for example, if your Web proxy settings are not specified correctly in your ISEE client configuration.

Entitlement Verification Problems

Entitlement problems can occur if your system handle/service agreement identifier (SAID) has expired or if the system handle/SAID you provided in the Self-Healing Services client user interface (UI) Contact Information page is invalid.

Analysis Problems

Problems during data analysis are extremely rare. If Self-Healing Services cannot complete an incident analysis, it will send you a service notification by e-mail.

Reporting and Notification Problems

Reporting and notification problems can occur if the e-mail addresses specified in the Self-Healing Services client user interface Notification Settings page are invalid. These problems can also occur if either the OVO message browser or the NNM browser was specified as the preferred notification method and that browser is not running on your system.

The fault and service notifications you receive from HP will contain garbled (unreadable) text if your mail reader does not support UTF-8 encoding and you selected the UTF-8 check box on your Self-Healing Services client user interface Contact Information page for your configuration center. This is also true of any persons you have selected to receive your service notifications from HP on your Self-Healing Services client user interface Notification Settings page.

Diagnosing a Problem Using E-Mail Messages

The first sign that Self-Healing Services may not be operating correctly can be found in your e-mail box. If a fault is detected and the self-healing process is successfully executed, you will receive a service notification by e-mail indicating that an Incident Analysis Report is available for review from the HP OpenView Self-Healing Services Support web site (see “Report Available Notification” on page 182).

If you do not receive this service notification, there may be a problem with your installation or configuration. Self-Healing Services will also send you a service notification if a submitted incident package fails the entitlement check (see “Entitlement Action Required Notification” on page 183).

In all, Self-Healing Services sends four different types of service notifications (see Chapter 6, “Understanding Service Notifications,” on page 179 for further information). These service notifications and the likely location of the problem are summarized in Table 7-1.

Table 7-1 E-Mail Messages Sent By Self-Healing Services


Type	Service Notification	Likely Location of Problem
1	“Welcome to Self-Healing Services Notification”	If you do not receive this notification after performing a connectivity test, you likely have a problem with your installation or configuration. See “Test Your Installation” on page 91 of the <i>HP OpenView Self-Healing Services Installation Guide</i> for additional information.
2	“Report Available Notification”	If you do not receive this notification when Self-Healing Services submits a fault to HP, you likely have a problem with your installation or configuration. See “Test Your Installation” on page 91 of the <i>HP OpenView Self-Healing Services Installation Guide</i> for additional information.
3	“Entitlement Action Required Notification”	 This service notification provides instructions about how to change the system handle/SAID associated with the incident package or edit your HP Passport profile to include the system handle/SAID.

Table 7-1 E-Mail Messages Sent By Self-Healing Services (Continued)

Type	Service Notification	Likely Location of Problem
4	“Additional Data Received Notification”	If you do not receive this notification when you submit additional data for a previously submitted fault to HP using the Self-Healing Services UI, you likely have a problem with your configuration or installation. See “Test Your Installation” on page 91 of the <i>HP OpenView Self-Healing Services Installation Guide</i> for additional information.

Diagnosing a Problem Using Error Messages

Another sign that Self-Healing Services may not be operating correctly can be found in your Self-Healing Services log file, <DataDir>/log/shs/shs.log. The following error messages can appear in this file.

Table 7-2 Error Messages Logged By Self-Healing Services

Description	Implications	How to Troubleshoot the Problem
<p>Unable to connect to https://<hostname>: 5814</p> <p><i>This message appears in the web browser; it is not logged in a file.</i></p>	<p>A port conflict with the Self-Healing Services client has occurred.</p>	<p>Determine whether port 5814 is being listened to by typing the command:</p> <p>HP-UX and Solaris: netstat -an grep <port number></p> <p>Windows: netstat -an more</p> <p>NOTE: The default port number is 5814. If you changed the port number, it will be different.</p> <p>If port 5814 is not being listened to, stop and restart the Self-Healing Services client following the instructions in “Start or Stop the Self-Healing Services Client” on page 97 in the <i>HP OpenView Self-Healing Services Installation Guide</i>.</p> <p>NOTE: Be sure to wait a few minutes after starting Self-Healing Services before attempting to access the Self-Healing Services client user interface.</p> <p>If port 5814 is being listened to, you likely have a firewall between the machine running the web browser and the machine running the Self-Healing Services client. You can either open the port on your firewall or change the port on which your firewall allows traffic.</p> <p>See “Change the Self-Healing Services Client Port” on page 96 of the <i>HP OpenView Self-Healing Services Installation Guide</i> for additional information.</p>

Table 7-2 Error Messages Logged By Self-Healing Services (Continued)

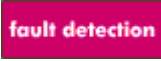
Description	Implications	How to Troubleshoot the Problem
This page cannot be displayed. <i>This message appears in the web browser; it is not logged in shs.log</i>	The URL may have specified http instead of https.	Be sure to specify https://<hostname>:<portnumber> to start the Self-Healing Services user interface.
Application Monitor could not be started due to initialization error.	Internal errors, such as a configuration file syntax error or an I/O error, have occurred.	 Call HP Support.

Table 7-2 Error Messages Logged By Self-Healing Services (Continued)

Description	Implications	How to Troubleshoot the Problem
<p>Error messages pertaining to potential port conflicts.</p>	<p>There may be port conflicts between Self-Healing Services and other applications. For example, there are known default port conflicts between NNM 7.5 and Self-Healing Services.</p> <p>Normally, the Self-Healing Services shutdown port must be changed to eliminate conflicts.</p>	<p>fault detection To determine whether a port conflict exists, look for indicators in the following files:</p> <pre><logDir>\stdout.log <logDir>\stderr.log</pre> <p>In this case, <i><logDir></i> is as follows:</p> <pre><installDir>\java\shs\jetty\logs</pre> <p>where <i><installDir></i> is the directory in which Self-Healing Services is installed.</p> <p><i>Windows:</i></p> <p>By default <i><installDir></i> is C:\Program Files\HP OpenView</p> <p><i>HP-UX or Solaris:</i></p> <p>By default, <i><installDir></i> is /opt/OV.</p> <p>You can determine the Self-Healing Services HTTPS port by using the following command:</p> <p><i>Windows:</i></p> <pre>cscript <installDir>/bin/shsctrl.vbs -getconf</pre> <p><i>HP-UX or Solaris:</i></p> <pre>/opt/OV/bin/shsctrl -getconf</pre> <p>For information about changing ports, run the <i>shsctrl</i> command with the <i>-help</i> option:</p> <p><i>Windows:</i></p> <pre>cscript <installDir>/bin/shsctrl.vbs -help</pre> <p><i>HP-UX or Solaris:</i></p> <pre>/opt/OV/bin/shsctrl -help</pre>

Table 7-3 Error Messages Logged By ISEE

Description	Implications	How to Troubleshoot the Problem
<p>Unable to connect to http://<client-node-name>:5060/ start.html</p> <p><i>Logged in</i></p> <p>HP-UX and Solaris: /var/opt/hpservices/log/mad.log</p> <p>Windows: C:\Program Files\ Hewlett-Packard\ISEE\ MotiveChorus\log\mad.log</p>	<p>A port conflict with the ISEE client has occurred.</p>	<p>Uninstall and reinstall the ISEE client. If that does not solve the problem, contact HP OpenView support.</p>

Diagnosing a Problem Using Other Indicators

If the service notifications you receive from Self-Healing Services by e-mail do not contain enough information for you to pinpoint the problem—or you do not receive any service notifications at all—use the indicators shown in Table 7-4 to focus your troubleshooting activities.

Table 7-4 Self-Healing Services Problem Indicators

Indicator	Implications	Suggested Solution
Incident search takes a long time to complete when the number of incidents is large	Old, obsolete incidents have not been deleted from the database.	Delete incidents that are no longer required using the Incident Viewer.
Self-Healing Services stops after HP OpenView Operations (OVO) is uninstalled.	Uninstalling OVO always stops Self-Healing Services, which must then be manually restarted. After this restart, Self-Healing Services works normally.	Start the Self-Healing Services client by following the instructions in “Start or Stop the Self-Healing Services Client” on page 36 of the <i>HP OpenView Self-Healing Services User’s Guide</i> .
Self-Healing Services incorrectly reports that an HP OpenView application is uninstalled when an incident is submitted manually for that application.	This occasionally happens after a supported application is upgraded. It is a known problem.	Resubmit the incident.
Self-Healing Services client log file shows no faults detected.	The client may need to be restarted, or the installation may be faulty.	<div data-bbox="1003 1188 1159 1230" style="background-color: #e91e63; color: white; padding: 2px;">fault detection</div> Stop the Self-Healing Services client and then restart it following the instructions in “Start or Stop the Self-Healing Services Client” on page 36 of the <i>HP OpenView Self-Healing Services User’s Guide</i> . Also see “Test Your Installation” on page 91 of the <i>HP OpenView Self-Healing Services Installation Guide</i> .

Table 7-4 Self-Healing Services Problem Indicators (Continued)

Indicator	Implications	Suggested Solution
<p>The Self-Healing Services client log file indicates that a fault has been detected but data has <i>not</i> been collected.</p>	<p>The client may need to be restarted, or the installation may be faulty. The permissions on the files accessed during data collection may be restrictive.</p>	<p>data collection You can stop and restart the Self-Healing Services client at any time following the instructions “Start or Stop the Self-Healing Services Client” on page 97 of the <i>HP OpenView Self-Healing Services Installation Guide</i>.</p> <p>Also see “Test Your Installation” on page 91 of the <i>HP OpenView Self-Healing Services Installation Guide</i>.</p>

Table 7-4 Self-Healing Services Problem Indicators (Continued)

Indicator	Implications	Suggested Solution
<p>You forgot your Self-Healing Services user name or password.</p>	<p>You either need to request that your user name and password be e-mailed to you or reset your user name and password to their initial state: user name = admin password = admin</p>	<p>To request that your user name and password be e-mailed to you, follow these steps:</p> <ol style="list-style-type: none"> 1. On the Self-Healing Services client user interface sign-in page, click Forgot user name and/or password? 2. On the next page displayed, click Send Info. <p>Self-Healing Services will then e-mail your user name and password to the e-mail address provided on the User Name & Password page.</p> <p>NOTE: This process only works if you have configured the e-mail server settings. See “Configure the E-mail Server Settings” on page 64.</p> <p>To reset your user name and password to their initial state, follow these steps:</p> <ol style="list-style-type: none"> 1. First, copy the <code>login.xml</code> file from the <code>newconfig</code> directory to the <code>conf</code> directory: <i>HP-UX and Solaris:</i> from <code>/opt/OV/newconfig/shs</code> to <code>/var/opt/OV/conf</code> <i>Windows:</i> from <code><installDir>\newconfig\shs</code> to <code><installDir>\data\Conf</code> For Windows, <code><installDir></code> is <code>C:\Program Files\HP OpenView</code> by default. 2. Stop and restart the Self-Healing Services client following the instructions in “Start or Stop the Self-Healing Services Client” on page 97 of the HP OpenView Self-Healing Services Installation Guide.

Table 7-4 Self-Healing Services Problem Indicators (Continued)

Indicator	Implications	Suggested Solution
<p>You can manually submit a fault using the UI, but you do not receive any service notification by e-mail from Self-Healing Services.</p> <p><i>and</i></p> <p>The Self-Healing Services client log file indicates that a fault has been detected, data has been collected, and the data has been sent to the ISEE client.</p>	<p>The e-mail address or addresses that you specified in the Notification Settings page of the UI may be incorrect.</p> <p><i>or</i></p> <p>The ISEE client is not successfully transporting your data to HP. This is often caused by errors in the web proxy specifications entered into the ISEE interface during installation and configuration. If your web proxy password changes, for example, you will need to reconfigure the ISEE client.</p>	<p>user interface See “Configure the Notification Settings” on page 57.</p> <p>data transport See “Verify Internet Connectivity for Communication Gateways” on page 30 of the <i>HP OpenView Self-Healing Services Installation Guide</i>.</p> <p>See “Test Your Installation” on page 91 of the <i>HP OpenView Self-Healing Services Installation Guide</i>.</p> <p>Also see the ISEE documentation available at the following web site: http://www.hp.com/hps/hardware/hw_enterprise.html</p>
<p>ISEE client log indicates that data has been received from the Self-Healing Services client, but was not sent to HP.</p>	<p>See above.</p>	<p>data transport See “Verify Internet Connectivity for Communication Gateways” on page 30 of the <i>HP OpenView Self-Healing Services Installation Guide</i>.</p> <p>Also see “Test Your Installation” on page 91 of the <i>HP OpenView Self-Healing Services Installation Guide</i>.</p>

Collecting Information for HP Support

If problems occur with your Self-Healing Services installation that you are unable to diagnose, you can use the following script to collect information and e-mail it to your HP Response Center support engineer:

HP-UX and Solaris:

```
/opt/OV/bin/hps_diag.sh
```

Windows:

```
<installDir>\bin\hps_diag.bat
```

where *<installDir>* is the application installation directory that you specified when you installed Self-Healing Services. By default, *<installDir>* is C:\Program Files\HP OpenView.

This script collects Self-Healing Services client log files and configuration files, and Instant Support Enterprise Edition (ISEE) client log files if the ISEE client is installed on the system.

The collected data is saved to:

HP-UX and Solaris:

```
/var/opt/OV/datafiles/shs/work/hps_diag.tar.Z
```

Windows:

```
<DataDir>\datafiles\shs\work\hps_diag\hps_diag.zip
```

where *<DataDir>* is the location of the data directory that you specified at install time. By default, this is C:\Program Files\HP OpenView\data.

A **Scripts**

This appendix contains locations and descriptions of scripts that you can use to configure, operate, and maintain your Self-Healing Services installation.

Available Scripts

The following table provides locations and descriptions of the scripts that are available for your Self-Healing Services installation. Unless otherwise indicated, files are located in the following directories.

HP-UX and Solaris:

/opt/OV/bin

Windows:

<installDir>\HP OpenView\bin

By default <installDir> is C:\Program Files\HP Open View on Windows systems.

NOTE

To invoke the shsctrl script on Windows systems, you must use the cscript command. For example, to start the Self-Healing Services web server, type:

cscript <installDir>\HP OpenView\bin\shsctrl.vbs -start

For HP-UX and Solaris systems, use the shsctrl command as stated in the table.

Script	Description
shsctrl -start	Starts the Self-Healing Services web server.
shsctrl -stop	Stops the Self-Healing Services web server.
shsctrl -restart	Stops and restarts the Self-Healing Services web server.
shsctrl -status	Tells you whether the Self-Healing Services web server is running.
shsctrl -gethttpsport	Tells you the port used for HTTPS communication by the Self-Healing Services web server. See “Change the Self-Healing Services Client Port” on page 96 in the <i>HP OpenView Self-Healing Services Installation Guide</i> .
shsctrl -sethttpsport	Sets the port used for HTTPS communication by the Self-Healing Services web server. See “Change the Self-Healing Services Client Port” on page 96 in the <i>HP OpenView Self-Healing Services Installation Guide</i> .
shsctrl -findvm	Search for virtual machines installed by other HP OpenView applications. If an acceptable virtual machine is found, configure Self-Healing Services to use that virtual machine.
shsctrl -getvm	Displays the location of the Java virtual machine that Self-Healing Services is configured to use.

Script	Description
shsctrl -setvm	Sets the location of the Java virtual machine that Self-Healing Services will use.
shsctrl -getshutdownport	Tells you the shutdown port that the Self-Healing Services web server is configured to use.
shsctrl -setshutdownport	Sets the shutdown port that the Self-Healing Services web server will use.
shsctrl -autoconfigure [reset]	<p>Auto configures HP OpenView Self-Healing Services.</p> <p>If the reset option is specified, Self-Healing Services is reconfigured back to its default values. If it is not specified, Self-Healing Services keeps the current configuration options unless they are invalid. If any options are found to be invalid, those options are reconfigured.</p>
shsctrl -validateconf	Validates the configuration details for Self-Healing Services.
shsctrl -h	Displays usage information for the shsctrl script.
hpservices start	<p>Starts the ISEE client. Located in <code>/sbin/init.d</code> on HP-UX systems and <code>/etc/init.d</code> on Solaris systems.</p> <p>To start the ISEE client on Windows systems, open the Services utility, and start the HP ISEE service.</p>
hpservices stop	<p>Stops the ISEE client. Located in <code>/sbin/init.d</code> on HP-UX systems and <code>/etc/init.d</code> on Solaris systems.</p> <p>To stop the ISEE client on Windows systems, open the Services utility, and stop the HP ISEE service.</p>
hps_diag.sh	Gathers ISEE and Self-Healing Services log files and configuration files, installation status, and patch information for all applications that Self-Healing Services supports. This file is used by recon to gather Self-Healing Services, ISEE, and system diagnostic information.
iseeConnectivityTest.sh	Performs an ISEE connectivity test. Located in <code>/opt/hpservices/RemoteSupport/bin</code>
recon.sh	Runs the Self-Healing Services data collectors for all supported HP OpenView applications that are installed on this system.

B **Log Files**

This appendix contains the names and descriptions of the log files used by HP OpenView Self-Healing Services.

Available Log Files

Unless otherwise noted, the following log files are located in:

HP-UX and Solaris:

`/var/opt/OV/log/shs`

Windows:

`<dataDir>\data\log\shs`

where `<dataDir>` is the data directory that you specified at install time. By default, `<dataDir>` is `C:\Program Files\HP OpenView`.

Table B-1 Self-Healing Services Log Files

File	Description
<code>shs.log</code>	Main log file. Contains all log messages for the Self-Healing Services client.
<code>collector-registration.log</code>	Log file that has an entry each time that a collector for a supported application is registered; used during installation.
<code>swagent.log</code>	Installation error messages on HP-UX. Located in <code>/var/adm/sw</code> .
<code>stdout.log</code> <code>stderr.log</code> <code>shutdownout.log</code> (jetty shutdown logs) <code>shutdownerr.log</code> (jetty error shutdown logs)	Windows only. Contains messages pertaining to the initialization and operation of the Self-Healing Services user interface. Located in the following directory: <code><installDir>/java/shs/jetty/logs</code> where <code><installDir></code> is the default application directory that you specified at installation time. By default, this is <code>C:\Program Files\HP OpenView</code> .
<code>jetty.out</code>	HP-UX or Solaris only: Jetty web server log files, which contains messages pertaining to the initialization and operation of the Self-Healing Services user interface. Located in the following directory: <code><installDir>/java/shs/jetty/logs/</code> where <code><installDir></code> is the default application directory that you specified at installation time. By default, this is <code>/opt/OV</code> .

Table B-2 ISEE Log Files

File	Description
<p>HP-UX and Solaris: /var/opt/hpservices/log/ mad.log</p> <p>Windows: C:\Program Files\ Hewlett-Packard\ISEE\ MotiveChorus\log\mad.log</p>	<p>Motive Chorus log file</p>
<p>HP-UX and Solaris: /var/opt/hpservices/log</p> <p>Windows: C:\Program Files\ Hewlett-Packard\ISEE\logs</p>	<p>Other log files for the ISEE client. One of the most useful files is submitData.log.</p>

C **Data Collected**

This appendix contains a link to detailed descriptions of the data collected when Self-Healing Services detects a fault in a supported software application.

Data Collected by Self-Healing Services

Data is collected by the Self Healing Services client when a fault is detected in a supported HP OpenView software application. The data is then packaged into an incident package that is sent back to HP for automated analysis. Information sent to HP consists of system information as well as application-specific information for the fault.

All the system information listed in “System Information Collected” in this appendix is collected when a fault is detected in a supported application.

NOTE

When a fault is detected in a supported application with *only* Self-Healing Services basic support, the system information listed in “System Information Collected” in this appendix and patch information is the only information collected. For a list of applications with basic support, see the following document:

http://support.openview.hp.com/pdf/selfhealing-supported-apps_ver2-6.pdf

System Information Collected

Hostname

OS name and version

Machine type

Model

Amount of swap space

Amount of physical memory

Amount of total disk space

Amount of available disk space

File system info (using `bdf` on HP-UX, `df` on Solaris)

DCE information (`rpccp show mapping`)

Environment variables

Locale information (`locale`)

Network status (`netstat`)

Uptime info (`uptime`)

Process info (`top` and `sar` on HP-UX, `ps` and `psrinfo` on Solaris)

Configurable kernel parameters

List of installed applications (`swlist` on HP-UX, `pkginfo` on Solaris)

Contents of the following files: `/etc/inetd.conf` and `/etc/nsswitch.conf`