

Open Service Event Manager

Setup Guide

This document provides instructions for installing and configuring Open Service Event Manager 1.4.7.

Rev. September 12, 2008



Hewlett-Packard Company
Technical Publications
3404 East Harmony Road
Fort Collins, Colorado 80528 • U.S.A.

June 2008

© Copyright 1998 - 2008 Hewlett-Packard Development Company, L.P.

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.

The information contained herein is subject to change without notice. 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.

This service tool software, including associated documentation, is the property of and contains confidential technology of Hewlett-Packard Company or its affiliates. Service customer is hereby licensed to use the software only for activities specified in the Exhibit SS5, and HP Terms and Conditions of Sale and Services, HP Business Terms or HP Global Agreement and only during the term of the applicable support delivered by HP or its authorized service provider. Customer may not modify or reverse engineer, remove, or transfer the software or make the software or any resultant diagnosis or system management data available to other parties without HP's or its authorized service provider's consent. Upon termination or expiration of the services, customer will, at HP's or its service provider's option, destroy or return the software and associated documentation in its possession.

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation. UNIX is a registered trademark of The Open Group. Intel and Pentium are trademarks of Intel Corporation in the U.S. and other countries.

Printed in the U.S.

Change Summary

The following table summarizes the changes to this document:

Revision	Description
10/13/06-A	Initial 1.4.3 copy
03/10/08	Minor Updates for OSEM Release 1.4.5
06/18/08	Minor Updates for OSEM Release 1.4.6
09/11/08	Minor Updates for OSEM Release 1.4.7

Contents

Title Page	i
Copyright Statement	ii
Change Summary	iii
List of Figures	ix
List of Tables	xi
1 Introduction to OSEM	1-1
1.1 What is OSEM?	1-2
1.1.1 OSEM for SNMP	1-3
1.1.2 OSEM for HTTP	1-3
1.1.2.1 WEBES Systems	1-4
1.1.2.2 DECEvent Systems	1-4
1.1.2.3 M/Series FC Switches	1-4
1.2 The OSEM Host	1-4
1.2.1 OSEM Host Hardware Platforms	1-5
1.2.2 OSEM Host Operating Systems	1-5
1.2.3 OSEM Host Software	1-5
1.3 Managed Systems	1-6
1.3.1 Managed System Hardware Platforms	1-6
1.3.2 Managed System Operating Systems	1-7
1.3.3 Managed System Software	1-7
1.4 This Guide	1-8
1.5 Related Information	1-8
2 Getting Started	2-1
2.1 Site Survey	2-2
2.2 Installation Overview	2-3
2.3 Kits and Filter File Updates	2-3
2.4 Documentation	2-4

Contents

3 Windows OSEM Host 3-1

3.1 Pre-Installation	3-2
3.2 Installation	3-3
3.3 Post-Installation	3-3
3.3.1 Rerunning the Kit	3-3
3.3.2 Accepting SNMP Packets	3-4
3.3.3 Restricting Access to OSEM	3-4
3.3.4 Sending a Test Notification	3-4
3.3.5 Setting the SNMP Trap Service for Auto Startup	3-4
3.3.6 Configuring SNMP Community Names	3-5
3.3.7 Updating and Registering the MIB File	3-5
3.3.8 How to Change the HP SIM Host Name	3-5
3.4 Uninstallation	3-6
3.5 Multiple OSEM Hosts	3-6
3.6 OSEM and firewalls	3-6

4 Storage Management Appliance OSEM Host 4-1

4.1 Connecting to the SMA	4-2
4.2 Pre-Installation	4-2
4.3 Installation	4-3
4.4 Post-Installation	4-3
4.4.1 Rerunning the Kit	4-3
4.4.2 Restricting Access to OSEM	4-3
4.4.3 Sending a Test Notification	4-4
4.4.4 Setting the SNMP Trap Service for Auto Startup	4-4
4.4.5 Configuring SNMP Community Names	4-4
4.4.6 Automated Notifications	4-4
4.5 Uninstallation	4-5
4.6 Multiple OSEM Hosts	4-5

5 SNMP Managed Systems 5-1

5.1 Overview	5-2
5.2 Supported Notifications	5-2
5.3 A Note About HTTP Notifications	5-5
5.4 Site Survey	5-5
5.5 The OSEM Host	5-6
5.6 Guidelines for SNMP Systems	5-6
5.7 Windows Server 2003 Default Behavior	5-6
5.8 The Storage Management Appliance	5-7
5.8.1 Connecting to the SMA	5-7
5.8.1.1 Windows 2000 Desktop	5-7
5.8.1.2 Open SAN Manager	5-7
5.8.2 Insight Manager	5-8
5.8.3 Storage Software	5-8
5.8.4 SNMP Traps—from IM Agents	5-8
5.8.5 SNMP Traps—from HSV Element Manager	5-10
5.9 SNMP Traps—from B/Series Fibre Channel Switches	5-10
5.10 SNMP Traps – From C/Series Fibre Channel Switches	5-12

6 HTTP Managed Systems 6-1

- 6.1 Overview 6-2
- 6.2 A Note About SNMP Notifications 6-2
- 6.3 Site Survey 6-2
- 6.4 The OSEM Host 6-2
- 6.5 WEBES Systems 6-2
 - 6.5.1 Supported Notifications 6-3
 - 6.5.2 Guidelines for WEBES Systems 6-3
 - 6.5.3 Windows (Non-Appliance) 6-4
 - 6.5.4 The Storage Management Appliance 6-6
 - 6.5.4.1 Connecting to the SMA 6-6
 - 6.5.4.2 Insight Manager 6-7
 - 6.5.4.3 Storage Software 6-7
 - 6.5.4.4 Event Log Size 6-7
- 6.6 DECEvent Systems 6-8
 - 6.6.1 Guidelines for DECEvent Systems 6-8
 - 6.6.2 Tru64 UNIX 6-9
 - 6.6.3 OpenVMS 6-11
- 6.7 M/Series FC Switch Systems 6-13

A The Customer Profile File A-1

- A.1 Overview A-2
- A.2 How the Profile File Works A-2
- A.3 Number of Profile Files A-2
- A.4 Location of the Profile File A-2
- A.5 Calling the Profile File A-3
- A.6 Profile Template A-3
- A.7 Configuration Information A-3
 - A.7.1 Sample Profile 1—Simple A-4
 - A.7.2 Sample Profile 2—MSCS Cluster A-4
 - A.7.3 Sample Profile 3—MSCS Cluster with DRM A-5

B Troubleshooting B-1

- B.1 Verifying WEBES Notifications B-2
- B.2 Verifying SNMP Notifications B-2
 - B.2.1 Generating SNMP Traps from System Management Home Page B-2
 - B.2.2 Generating SNMP Traps from Windows B-3
 - B.2.3 Generating SNMP Traps from UNIX and Linux B-3
 - B.2.4 Generating SNMP Traps from NetWare B-3
- B.3 SNMP GET Failures B-4
- B.4 System Name Issues B-4
- B.5 OSEM Log File B-4
- B.6 TCP/IP Ports Used by OSEM B-4
- B.7 Decompression Message B-5
- B.8 Services B-5
- B.9 Processes B-5
- B.10 Interpreting Copies of Problem Reports B-5

C Products Supported by OSEM

- C.1 ProLiant Support C-2
- C.2 Integrity Support C-2
- C.3 Switch and Tape Support C-3
- C.4 Multivendor Support C-5
- C.5 Storage Products C-5
- C.6 MSADB 1.52.90 Ruleset C-5
- C.7 Additional OSEM Highlights C-6

Glossary

List of Figures

1-1	Open Service Event Manager Site	1-2
1-2	OSEM Reporting	1-3
2-1	Size of Site	2-2
5-1	SNMP Properties	5-9
6-1	Sample LP6NDS35.SYS Product Version	6-6
6-2	Event Log Settings	6-8
B-1	SNMP Test.....	B-3

List of Tables

6-1	Files Revisions Required for SANWorks Secure Path 3.1—Windows 2000	6-4
6-2	File Revisions Required For StorageWorks Platform Solution Kit—Windows 2000	6-5
6-3	ENP Files for Tru64 UNIX	6-9
6-4	ENP Files for OpenVMS	6-11
B-1	Port Numbers Used by OSEM	B-4

Introduction to OSEM

This chapter provides an overview of OSEM, associated service offerings, hardware and software necessary for implementation, and this manual.

What is OSEM?	page 1-2
The OSEM Host	page 1-4
Managed Systems	page 1-6
This Guide.....	page 1-8
Related Information	page 1-8

Introduction to OSEM

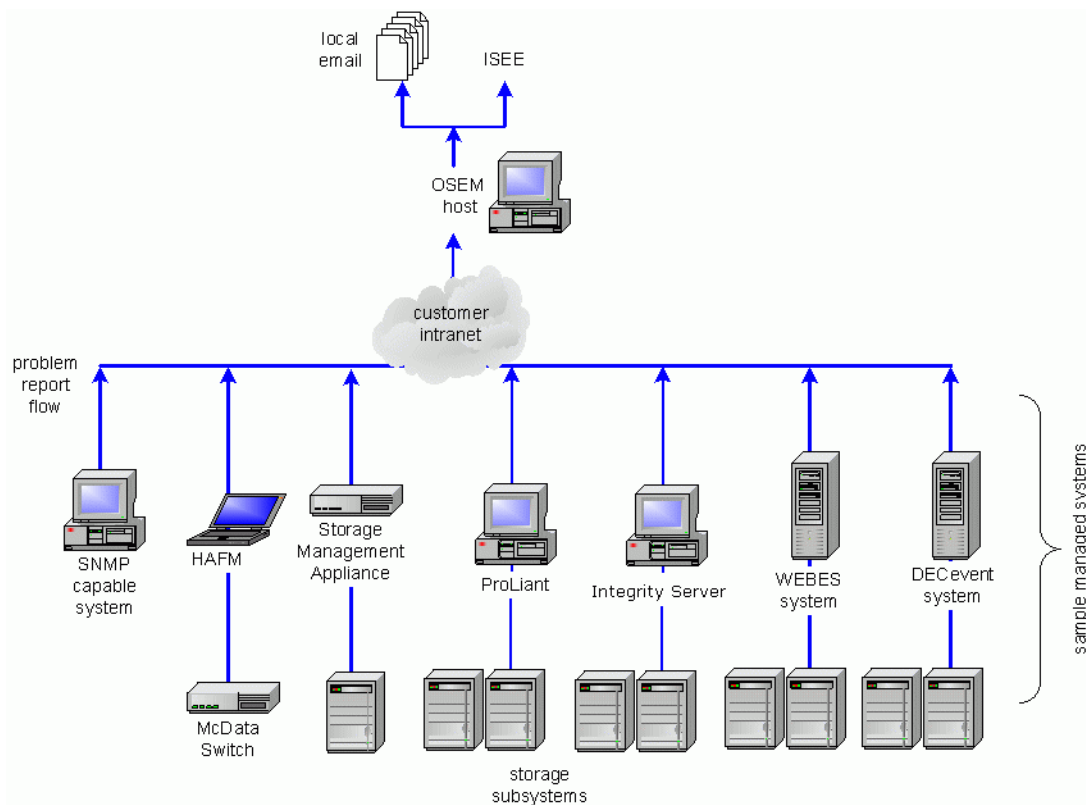
1.1 What is OSEM?

1.1 What is OSEM?

Open Service Event Manager (OSEM) allows customers to collect, filter, and format problem reports for assorted systems. OSEM can automatically send service event notifications as local email messages or as Instant Support Enterprise Edition (ISEE) notifications to HP (see Figure 1-1). OSEM also supports HP Service Essentials Remote Support Pack (RSP) notifications. In addition to 32-bit and 64-bit Intel Windows machines (SMA and ProLiant) OSEM also runs on HP Integrity Servers running Windows.

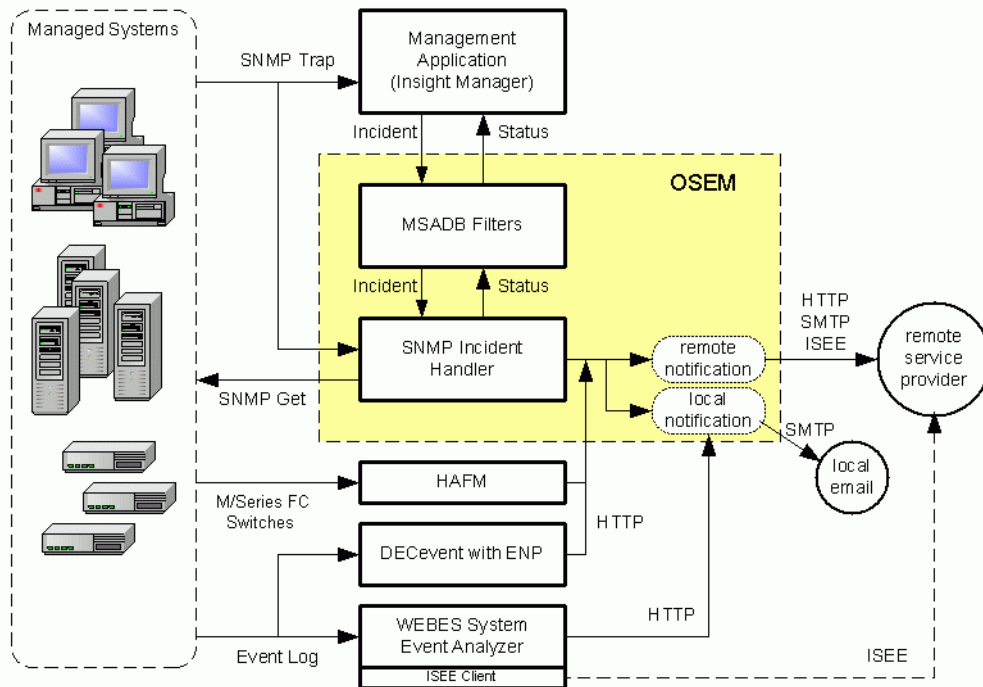
Customer systems self-report by running automated software for the detection and forwarding of incidents to a designated OSEM host.

Figure 1-1 Open Service Event Manager Site



How customers use OSEM depends on what type of managed systems they have and what they want to monitor and maintain. These decisions, in turn, determine what automated reporting functions that a customer participates in.

Figure 1-2 OSEM Reporting



1.1.1 OSEM for SNMP

OSEM provides for detection and auto-reporting of events affecting systems (such as the HP ProLiant, Itanium Processor Family (IPF) server, or OpenView Storage Management Appliance) on SNMP-managed networks. Collection can occur directly, or indirectly through a management application such as HP Systems Insight Manager.

Best results are achieved if the SNMP traps are generated by Insight Manager (IM) agents installed on the system. Other trap-sending configurations are possible but supported on an as-is basis only.

OSEM also provides for the detection and auto-reporting of SNMP events affecting HP B-Series and HP C-Series Fibre Channel (FC) switches. Collection occurs directly from the FC Switch.

1.1.2 OSEM for HTTP

OSEM provides for collection and auto-reporting of events from systems capable of sending event data over hypertext transfer protocol (HTTP). Systems in this category include Web-Based Enterprise Services (WEBES) capable systems, non-WEBES systems that run DECEvent, and the high availability fabric manager (HAFM) attached to M/Series FC switches.

Introduction to OSEM

1.2 The OSEM Host

1.1.2.1 WEBES Systems

OSEM works in conjunction with WEBES to monitor a system's event log, providing detection and auto-reporting of events affecting storage subsystems and hosts:

- Host Based Storage—Windows, Tru64 UNIX®, and OpenVMS host-based storage is supported.
- SAN Based Storage—OSEM supports automated notification for SAN-based storage attached to the HP OpenView Storage Management Appliance (SMA).
- Host Servers—The same WEBES software that allows for auto-reporting of host-based storage events will detect and auto-report events directly affecting Tru64 and OpenVMS servers.

WEBES monitoring is supported only for local email notifications. Remote auto-reporting via ISEE requires that the ISEE Client be installed on each WEBES system.

11.2.2 DECevent Systems

On older, non-WEBES systems, you can add the Event Notification Program (ENP) and register it with DECevent to send notifications to the OSEM host via HTTP. This setup provides an alternative to the previous reporting method of using System Initiated Call Logging (SICL) and DSNLink on these systems. Systems in this category include the following:

- Non WEBES-capable AlphaServers running Tru64 UNIX
- Non WEBES-capable AlphaServers running OpenVMS
- OpenVMS VAX systems

1.1.2.3 M/Series FC Switches

The HAFM appliance provides an interface for operating and managing M/Series FC switches, and can forward events from those switches in HTTP format to the OSEM host.

1.2 The OSEM Host

The OSEM host is the web-enabled central service processor residing at the customer site. As the gateway for managed system notifications, the OSEM host accumulates events from the entire site, filters them, and forwards them onward.

It is worth noting that the OSEM host itself also can be a managed system, simply by installing the necessary software for automatic notifications. This might be desired at a smaller site where resources are limited. Terminology such as “combination” or “dual” system refers to this double-role configuration of OSEM host and managed system.

1.2.1 OSEM Host Hardware Platforms

The OSEM host requires one of the following:

- An HP ProLiant server or HP Integrity server

Note that OSEM usually will operate on any industry standard x86 system. However, because HP does not qualify OSEM on third-party products, functionality on such systems is provided on an as-is basis only.

- An HP OpenView Storage Management Appliance
- An HP Integrity Server

1.2.2 OSEM Host Operating Systems

The OSEM host requires one of the following operating systems:

- Windows 2000, with SP2 or higher
- Windows Server 2003/R2 x86/x64
- Windows 2003 Enterprise Server/R2 x86/x64
- Windows 2003 DataCenter for the 64 bit OSEM kit

Not all operating systems are available for all hardware platforms.

1.2.3 OSEM Host Software

The OSEM host uses the following software:

- Required—OSEM
- Optional—HP Insight Manager

HP Systems Insight Manager can be installed on the OSEM host or a separate system. If HP SIM 5.1 or greater is installed on the OSEM host, OSEM will utilize HP SIM for SNMP configuration, Managed system information and SNMP trap notification.

Note

Do not install Insight Manager on the OSEM host if the OSEM host is a Storage Management Appliance.

- Optional—The ISEE Client/ The RSP Remote Support Client

Introduction to OSEM

1.3 Managed Systems

You also have the option to install the ISEE Client on a separate system. Either configuration is acceptable, provided that you adjust the OSEM Internal Settings and Remote Delivery pages as described in the *OSEM User Guide*.

If OSEM is to be part of a CMS host, both HP SIM and the ISEE Client must reside on the same host along with OSEM.

1.3 Managed Systems

Essentially, managed systems are the customer systems under service—the reason for having the OSEM infrastructure and associated reporting. Managed systems run software to detect and auto-report events to the OSEM host over the customer intranet.

As stated earlier, the OSEM host itself can become a managed system simply by installing additional software for automatic notifications. Terminology such as “combination” or “dual” system refers to this double-role configuration of managed system and OSEM host.

1.3.1 Managed System Hardware Platforms

In general, OSEM supports the following hardware platforms as managed systems:

- HP Servers that are supported by HP IM agents
- HP OpenView Storage Management Appliances
- HP Integrity Servers
- HP AlphaServers
- VAX platforms
- HP B-Series Fibre Channel Switches
- HP C-Series Fibre Channel Switches
- HP M-Series Fibre Channel Switches
- Modular Cooling Systems
- Dynamic Smart Cooling system
- Uninterruptable Power Supply
- Nearline Virtual Tape Library

1.3.2 Managed System Operating Systems

Managed systems that report to OSEM may run any operating system that meets one or more of the following criteria:

- It can send SNMP traps that OSEM knows about.
- It can send WEBES event data over HTTP.
- It can send DECEvent data over HTTP.
- It can send M/Series FC switch event data over HTTP.

SNMP traps—Best results are achieved if the managed system has HP IM agents installed. The IM agents are distributed by HP and are designed to generate traps that contain information that allows for more complete analysis of HP hardware. OSEM supports traps generated by HP B-Series and C-series switches.

The following operating systems are examples of ones that can be used on managed systems:

- Microsoft® Windows 2000, Server 2003
- HP Tru64 UNIX
- HP OpenVMS
- VMware ESX 2.1.x, 2.5.x (on ProLiant servers)
- Red Hat Linux
- Windows 2003 Enterprise Server
- Windows 2003 DataCenter
- SuSE Linux Enterprise Server (on Integrity Servers)

1.3.3 Managed System Software

Managed systems need different software to detect and analyze service events, and forward the events to the OSEM host. These programs can help identify intermittent problems before they become hard failures, and in many cases can match reported problems to a field replaceable unit (FRU). Individual requirements vary depending on the method of reporting:

- SNMP Notifications—IM agents are strongly recommended. The IM agents are distributed by HP and are designed to generate SNMP traps with information that allows for a more complete analysis.

Non-IM agents are supported on an as-is basis only.

- WEBES HTTP Notifications—WEBES System Event Analyzer is required.
- DECEvent HTTP Notifications—DECEvent and ENP are required.
- M/Series FC switch HTTP Notifications—The HAFM application is required.

Introduction to OSEM

1.4 This Guide

1.4 This Guide

This document describes how to install and configure the OSEM host at customer sites. Because of the wide variety of managed systems that can report to OSEM, experience with the setup and administration of your particular systems is assumed. Operational background on Windows, Tru64 UNIX, OpenVMS, SNMP, or other topics already found in the native documentation are generally beyond the scope of this guide.

1 Introduction to OSEM	Introduces OSEM and its role at customer sites
2 Getting Started	Tells how to prepare a customer site for OSEM
3 Windows OSEM Host	Describes the setup of a typical Windows OSEM host
4 Storage Management Appliance OSEM Host	Describes the setup of an HP OpenView Storage Management Appliance as an OSEM host
5 SNMP Managed Systems	Describes SNMP notifications from managed systems to the OSEM host
6 HTTP Managed Systems	Describes the HTTP based notifications that OSEM can support
A The Customer Profile File	Explains the role and content of the WEBES profile file
B Troubleshooting	Describes procedures for problem isolation and correction
Glossary	Contains terminology and definitions

1.5 Related Information

OSEM relies on assorted software to provide input to its reporting function. This guide does not provide comprehensive low-level detail about all of the data-sending software because these components often are available individually, for uses beyond OSEM. See the separate, product-specific documentation for each component to obtain any further information about the installation and extended uses of that component:

- HP Systems Insight Manager (HP SIM)
- WEBES
- System Event Analyzer (SEA, formerly Compaq Analyze)
- DECEvent
- ENP
- HAFM
- B-Series and C-Series FC Switches

Getting Started

This chapter explains how to prepare your site for OSEM and where to find software and documentation.

Site Survey	page 2-2
Installation Overview	page 2-3
Kits and Filter File Updates	page 2-3
Documentation	page 2-4

Getting Started

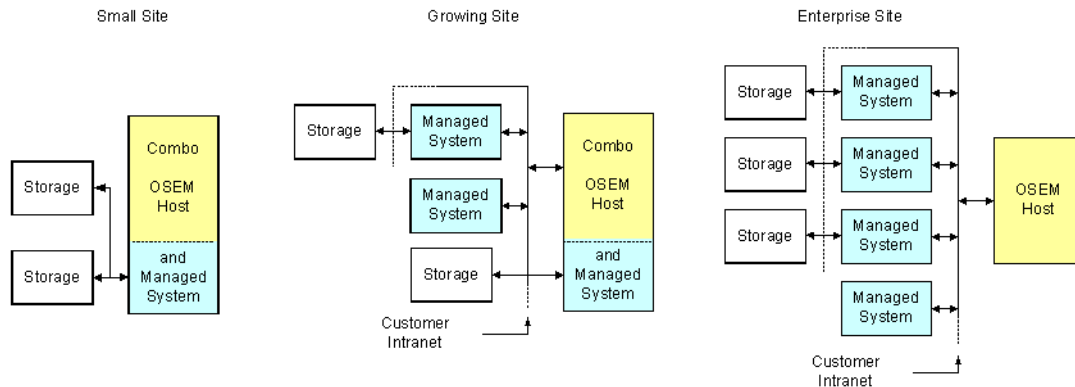
2.1 Site Survey

2.1 Site Survey

Before looking at individual systems or running the OSEM software kit, you need to make decisions about your site and how it will use OSEM.

- If you have a large number of managed systems, you should opt for a separate, dedicated OSEM host (see Figure 2–1).

Figure 2–1 Size of Site



- Choose the systems that will participate in OSEM, and decide what role each system will have: OSEM host, managed system, or combination.

You must configure an OSEM host first. After that, you are free to establish your own timetable for configuring each managed system and pointing it to the OSEM host.

- HP recommends one OSEM host per physical site. For diversification, avoid installing the OSEM host function on top of critical path systems whenever possible (such as Exchange servers, SQL servers, or routers).
- HP Systems Insight Manager

In the past using HP Systems Insight Manager with OSEM was not required. However, if configuring a Central Management System (CMS) as part of the HP Remote Support Pack (RSP), HP SIM 5.1 or better is required. HP SIM provides consolidated management options. For more information, see your HP Systems Insight Manager documentation.

- Locate the IP address or name of your outgoing email SMTP server.
- Address any other issues with the health of the site intranet. The OSEM host port 2069 requires an unrestricted TCP/IP connection to all managed systems, for example.
- Decide on your approach for email notifications. For example, software such as WEBES SEA can email its own copies of event notifications, and these copies would duplicate the OSEM notifications.

In other words, the emails can quickly add up. If you always specify the same address, somebody will receive multiple copies of every event for the entire site. One option might be to specify one central address during OSEM host setup, and individual server administrator addresses for each managed system.

- Decide on what OSEM functions to set up for each managed system. There are different kinds of automated notifications for SNMP or HTTP.

2.2 Installation Overview

Begin working with individual systems after completing the [Site Survey](#) and addressing any outstanding issues.

1. Address OSEM host prerequisites.
2. Install OSEM on the OSEM host.
3. Configure the OSEM host.

You are then free to follow your own implementation timetable for configuring each managed system and pointing it to the OSEM host. The software, setup, and documentation required varies according to platform and the kind of reporting you are implementing.

4. Address managed server prerequisites.
5. Install the software (e.g. IM agents, ENP, WEBES) needed for automated notification.
6. Configure the software to point to the OSEM host.

Note:

OSEM performs SNMP-GETS on port 161. SNMP-Trap runs on port 162. OSEM runs on port 2069.

2.3 Kits and Filter File Updates

Kits and updates for OSEM are available at the following URL:
www.hp.com/services/osem

Users within the HP network can go to the URL:
http://searay-cxo.cxo.hp.com/service_tools/osem/

2.4 Documentation

Documentation for OSEM is available at the following URL:
www.hp.com/services/osem

Users within the HP network can go to the URL:
http://techpubs.cxo.hp.com/doc_osem.html

Windows OSEM Host

This chapter describes how to set up and configure a typical Windows system to serve as the OSEM host. The Storage Management Appliance, which also runs Windows, involves different steps and is covered in Chapter 4.

If you are setting up a system that serves as a combination OSEM host and managed system, add any desired automated notification functions (see Chapters 5 and 6) after completing the instructions in this chapter.

Pre-Installation	page 3-2
Installation	page 3-3
Post-Installation	page 3-3
Uninstallation	page 3-6
Multiple OSEM Hosts	page 3-6

3.1 Pre-Installation

Note

The Storage Management Appliance, which also runs Windows, involves different steps which is covered in Chapter 4.

Be sure to read Chapter 2 [Getting Started](#) before proceeding. OSEM sites require the [Site Survey](#) described in Chapter 2.

Establish these prerequisites before running the installation kit. In most cases, systems already are at least partially configured, so determine what requirements are missing and install them accordingly:

- A system manufactured by HP, such as the ProLiant or HP Integrity Servers.

Note that OSEM usually will operate on any industry standard system running Microsoft Windows. However, because HP does not qualify OSEM on third-party products, functionality on such systems is provided on an as-is basis only.

- Minimum 512 MB RAM (1 GB recommended if the OSEM host runs additional services. A CMS host requires 1 GB minimum, 2GB recommended)
- Minimum 300 MB free disk space on the local hard drive
- Windows 2000, with SP2 or higher, or Windows Server 2003/R2 x86/x64/IPF

(You can check the operating system and service pack level using `C:\> winver`.)

- Working network connection, such as through an ethernet adapter
- TCP/IP installed and working
- Fixed IP address

As a confirmation step, ping the OSEM host at its own fixed IP name or address `C:\>ping osemhost.abc.xyzcompany.com`. If you do not get a response, resolve the issue before continuing.

- SNMP service installed and started (requires the operating system CD)
- SNMP Trap service (requires the operating system CD)

The SNMP Trap service must be installed.

- Microsoft JVM 5.00.3802 or or a suitable SUN JRE installed supporting JAVA in the Internet explorer

To check your JVM version, enter `C:\>jview`. If necessary, install version 5.00.3802 or greater from <http://www.microsoft.com/java/download.htm>.

- ❑ The installation fails if you map a share drive to the OSEM kit files. To avoid this issue, do one of the following:
 - Make sure that the kit files are available locally, such as on a CD or by copying them directly to the system.
 - When installing, enter the full universal naming convention (UNC) path to the kit files, for example: `\\servername\sharename\path_to_files\setup.exe`

3.2 Installation

Follow these steps to install the kit. Be sure you have addressed all [Pre-Installation](#) steps in [Section 3.1](#) before beginning this section.

1. Close other programs that are currently running, and do not start other programs during the installation.
2. Start the master InstallShield program by running the .exe file. You can run it by double-clicking its icon or by choosing Start | Run from the desktop.
3. Follow the prompts. The kit asks you to supply the following:
 - The address of your outgoing email SMTP server
 - The email address that should receive copies of problem reports
 - The email address that should receive alerts about OSEM itself

3.3 Post-Installation

The installation kit completes by opening a readme file and by launching the OSEM Viewer in your web browser. Read and close the readme file. The *OSEM User Guide* contains detailed information about how to use the OSEM Viewer.

Note that you can disable notifications (for example, during site maintenance) by stopping or starting reporting on the OSEM Viewer main page.

3.3.1 Rerunning the Kit

Avoid running the kit .exe program again because it starts the uninstall utility. To properly uninstall, see [Section 3.4](#).

3.3.2 Accepting SNMP Packets

When setting up a Windows 2000 OSEM host it may be desirable to reduce the SNMP data visibility. To do this an administrator needs to configure the SNMP security setting via Start | Programs | Administrative Tools | Services | SNMP Service. Under the Security tab, set the Windows Server 2000 to accept SNMP packets from localhost only. Windows 2003 implements this security setting by default.

3.3.3 Restricting Access to OSEM

OSEM 1.4.7 allows any user to view problem reports but limits configuration to localhost only. Further restriction can be applied by listing the only allowed systems IPS or FQDNS in the Enabled Clients List.

See the OSEM User Guide for details.

3.3.4 Sending a Test Notification

With reporting turned on, you may want to send a test notification using Start | Programs | OSEM V1.4.7 | Test OSEM. Confirm transmission of the test message by checking the email account that you specified for notifications.

3.3.5 Setting the SNMP Trap Service for Auto Startup

This section applies only to OSEM hosts that accept incoming SNMP traps.

Follow these steps to ensure that the SNMP Trap Service is set to start automatically:

1. Open the Services Manager (for example, choose Start | Programs | Administrative Tools | Services on Windows 2000).
2. Double-click the SNMP Trap Service.
3. In the box next to Startup type, verify or choose Automatic.
4. Press Apply and then OK.
5. Right Click on the SNMP Trap Service and Press Restart.
6. Press Restart.
7. Click Yes on the Restart Other Services box.

3.3.6 Configuring SNMP Community Names

This section applies only to OSEM hosts that accept incoming SNMP traps.

If you have set up SNMP community names (other than the default community), you must provide OSEM with the community name of each managed system it must access. The community name allows OSEM to get MIB data for each SNMP trap it receives from a given managed system. This can be configured by name/ip or subnet basis.

1. Start OSEM (Start | Programs | OSEM V1.4.7 | OSEM Viewer).
2. Stop reporting.
3. Specify addresses using the Communities option. See the *OSEM User Guide* for details.
4. Restart reporting.

If you do not configure the Communities option, all IP addresses are assumed to be in the default community. In addition, any IP address that you do not specify also is assumed to be in the default community.

3.3.7 Updating and Registering the MIB File

See the HP Insight Manager User Guide for information related to updating and registering the MIBs.

3.3.8 How to Change the HP SIM Host Name

The HP SIM host name/ip is required for OSEM to send service trap data to HP SIM. Although designed for HP SIM, any third party application can listen for a service trap. In OSEM 1.4.2 this internal setting name was changed to Service Trap Destination. Also OSEM 1.4.2 provides this service trap data to HP SIM 5.1 or greater using a SOAP connection. This will cause duplicate Service traps in HP SIM 5.1 or greater.

Follow these steps to change the HP SIM/Service trap destination host name:

- Open OSEM viewer (Http://Localhost:2069)
- Select Internal Settings from the left hand pane.
- In box next to Service Trap Destination host name or IP number replace localhost with the name or IP address of the system with HP SIM. To stop sending the SNMP service trap enter none as the destination address.
- Click Apply Changes Button.

3.4 Uninstallation

Uninstallation completely removes all the files under the OSEM directories. If desired, you can manually back up configuration files such as `working.props`, `hosts.txt`, or `communities.txt`. You also may want to back up the notifications folder to preserve copies of all your problem reports. OSEM 1.3.7 or greater makes a copy of all configuration and state information during the uninstall process. During the next installation OSEM will ask the installer if the previously saved data is to be reinstalled. During a silent installation the previous information is always installed.

Otherwise, follow these steps to uninstall OSEM:

1. Close OSEM if it is running.
2. Choose Start | Settings | Control Panel.
3. Select Add/Remove Programs.
4. Highlight the OSEM entry.
5. Press the button for removing the program.
6. Follow the prompts.

The first Cancel button is your only opportunity to cleanly exit the uninstall routine. Afterwards, do not cancel or stop the uninstall, even if a cancel or quit option becomes available.

3.5 Multiple OSEM Hosts

You can configure multiple OSEM hosts at a site, but be aware that unwanted copies of problem reports can quickly accumulate, especially when the same email addresses are repeatedly specified or when the same managed system reports to several OSEM hosts.

3.6 OSEM and firewalls

OSEM uses port 2069 to communicate with a browser or 3rd party problem report generators such as HAFM, WEBES and ENP. If a local firewall is installed (Windows XP service pack 2) and access to OSEM is desired, this port must be opened.

See <http://support.microsoft.com/default.aspx?scid=kb;en-us;308127>

The Microsoft SNMP services also needs port 162 open to receive traps.

Storage Management Appliance OSEM Host

This chapter describes how to set up and configure the HP OpenView Storage Management Appliance as the OSEM host.

The Storage Management Appliance OSEM host also acts as a managed system that reports to itself, so add SNMP (see Section 5.8) and WEBES (see Section 6.5) notifications after completing the instructions in this chapter.

Connecting to the SMA.	page 4-2
Pre-Installation	page 4-2
Installation.	page 4-3
Post-Installation	page 4-3
Uninstallation	page 4-5
Multiple OSEM Hosts.	page 4-5

4.1 Connecting to the SMA

The SMA is a “headless” server, meaning it is designed to be configured and allowed to run with minimal direct user interaction—without a physical monitor, keyboard, or mouse attached.

You can connect to the Windows 2000 desktop on the SMA using two methods:

- By directly connecting a monitor, keyboard, and mouse
- By running the Microsoft Terminal Services client

Every SMA is preconfigured to accept Terminal Services client connections because the Terminal Services server is preinstalled. Users who do not already have a copy of the Terminal Services client can download it from the following URL:

<http://www.microsoft.com/windows2000/downloads/recommended/TSAC/tsmsi.asp?Lang>

Desktop connections also require the account username and password for the SMA. The factory-set defaults are username **administrator** and password **admin#####**, where ##### is the last six characters of the serial number in reverse order. The password is case sensitive, and you are advised to change it (if you have not already done so) for better system security.

4.2 Pre-Installation

Caution

Even though the SMA can be your OSEM host, do not install Insight Manager on the SMA. Insight Manager installation is not supported and can prevent browser access to the SMA. This implies that you cannot make an SMA a CMS host.

Be sure to read Chapter 2, [Getting Started](#), before running individual installations. OSEM sites require the [Site Survey](#) described in Chapter 2.

Unlike the Windows OSEM host described in Chapter 3, which may have to be configured from scratch, the SMA is preconfigured with most hardware and software prerequisites. The only remaining pre-installation requirements for the OSEM host functions are as follows.

- Obtain a fixed IP address for the SMA. Do not use DHCP.
- If a previous copy of OSEM was installed, uninstall it by following the instructions in Section 4.5. Otherwise, OSEM does not reinstall.
- The installation fails if you map a share drive to the OSEM kit files. To avoid this issue, do one of the following:

- Make sure that the kit files are available locally, such as on a CD or by copying them directly to the system.
- When installing, enter the full universal naming convention (UNC) path to the kit files, for example: \\servername\sharename\path_to_files\setup.exe

4.3 Installation

Follow these steps to install the kit. Be sure you have addressed all [Pre-Installation](#) steps in Section 4.2 before beginning this section.

1. Close other programs that are currently running, and do not start other programs during the installation.
2. Start the master InstallShield program by running the .exe file. You can run it by double-clicking its icon or by choosing Start | Run from the desktop.
3. Follow the prompts. The kit asks you to supply the following:
 - The address of your outgoing email SMTP server
 - The email address that should receive copies of problem reports
 - The email address that should receive alerts about OSEM itself

4.4 Post-Installation

The installation kit completes by opening a readme file and by launching the OSEM Viewer in your web browser. Read and close the readme file. The *OSEM User Guide* contains detailed information about how to use the OSEM Viewer.

Note that you can disable notifications (for example, during site maintenance) by stopping or starting reporting on the OSEM Viewer main page.

4.4.1 Rerunning the Kit

Avoid running the kit .exe program again because it starts the uninstall utility. To properly uninstall, see Section 4.5.

4.4.2 Restricting Access to OSEM

OSEM 1.4.7 allows any user to view problem reports but limits configuration to localhost only. Further restriction can be applied by listing the only allowed systems IPS or FQDNS in the Enabled Clients List.

See the OSEM User Guide for details.

4.4.3 Sending a Test Notification

With reporting turned on, you may want to send a test notification using Start | Programs | OSEM V1.4.7 | Test OSEM. Confirm transmission of the test message by checking the email account that you specified for notifications.

4.4.4 Setting the SNMP Trap Service for Auto Startup

Follow these steps to ensure that the SNMP Trap Service is set to start automatically:

1. Go to Start | Programs | Administrative Tools | Services.
2. Double-click the SNMP Trap Service.
3. In the box next to Startup type, verify or choose Automatic.
4. Press Apply and then OK.
5. Right Click on the SNMP Trap Service and Press Restart.
6. Press Restart.
7. Click Yes on the Restart Other Services box.

4.4.5 Configuring SNMP Community Names

This section applies only to OSEM hosts that accept incoming SNMP traps.

OSEM provides for default community name configuration. Initially this setting is “public”. If you have set up SNMP community names (other than the default community), you must provide OSEM with the community name of each managed system it must access. The community name allows OSEM to get MIB data for each SNMP trap it receives from a given managed system. This can be configured by name/ip or subnet basis.

1. Start OSEM (Start | Programs | OSEM V1.4.7 | OSEM Viewer).
2. Stop reporting.
3. Specify addresses using the Communities option. See the *OSEM User Guide* for details.
4. Restart reporting.

If you do not configure the Communities option, all IP addresses are assumed to be in the default community. In addition, any IP address that you do not specify also is assumed to be in the default community.

4.4.6 Automated Notifications

To finish configuring the SMA so that it sends automated notifications about its own state, add SNMP (see Section 5.8) and WEBES (see Section 6.5) notifications.

4.5 Uninstallation

Uninstallation completely removes all the files under the OSEM directories. If desired, you can manually back up configuration files such as `working.props`, `hosts.txt`, or `communities.txt`. You also may want to back up the notifications folder to preserve copies of all your problem reports. OSEM 1.3.7 or better makes a copy of all configuration and state information during the uninstall process. During the next installation OSEM will ask the installer if the previously saved data is to be reinstalled. During a silent installation the previous information is always installed.

Otherwise, follow these steps to uninstall OSEM:

1. Close OSEM if it is running.
2. Choose Start | Settings | Control Panel.
3. Select Add/Remove Programs.
4. Highlight the OSEM entry.
5. Press the button for removing the program.
6. Follow the prompts.

The first Cancel button is your only opportunity to cleanly exit the uninstall routine. Afterwards, do not cancel or stop the uninstall, even if a cancel or quit option becomes available.

4.6 Multiple OSEM Hosts

You can configure multiple OSEM hosts at a site, but be aware that unwanted copies of problem reports can quickly accumulate, especially when the same email addresses are repeatedly specified or when the same managed system reports to several OSEM hosts.

SNMP Managed Systems

This chapter describes SNMP notifications from managed systems to the OSEM host.

Overview	page 5-2
Supported Notifications	page 5-2
A Note About HTTP Notifications	page 5-5
Site Survey	page 5-5
The OSEM Host	page 5-6
Guidelines for SNMP Systems	page 5-6
Windows Server 2003 Default Behavior	page 5-6
The Storage Management Appliance	page 5-7
SNMP Traps—from B-Series Fibre Channel Switches	page 5-10

SNMP Managed Systems

5.1 Overview

5.1 Overview

Any system capable of sending SNMP traps can direct those traps to the OSEM host for notification purposes, but best results are achieved if the system uses IM agents distributed by HP. Other trap-sending configurations are supported on an as-is basis only.

Trap-sending systems can include, but are not limited to, the following:

- HP ProLiant Servers that are supported by HP IM agents
- HP OpenView Storage Management Appliances
- HP Integrity Servers
- HP AlphaServers
- VAX platforms
- HP B-Series Fibre Channel Switches
- HP C-Series Fibre Channel Switches
- HP M-Series Fibre Channel Switches
- Modular Cooling Systems
- Dynamic Smart Cooling system
- Uninterruptible Power Supply
- Nearline virtual tape library
- Other Industry Standard Servers

It is beyond the scope of this manual to detail the specific SNMP configuration procedure for every combination of operating system and hardware that is capable of sending traps. This is especially true for platforms that are developed and distributed outside of HP.

However, this chapter makes an effort to clarify known configuration issues that have come up in the course of OSEM development and testing. Ultimately, though, it is the responsibility of the administrator of any given managed system to understand and configure SNMP functions on that system.

5.2 Supported Notifications

This release includes SNMP notification support through IM agents in the following areas:

- CL380 CR3500 controller failures
- CL380 EMU fan failures
- CL380 EMU power supply failures
- CL380 CR3500 external cabinet fan failures
- CL380 CR3500 external cabinet Power supply failures
- CL380 CR3500 attached drive failures
- Smart array accelerator battery failures

SNMP Managed Systems

5.2 Supported Notifications

- Smart array accelerator ECC error threshold exceeded notifications
- Smart array accelerator memory read errors
- Smart array accelerator memory write errors
- Smart array controller failures
- Smart array attached drive failures
- Smart array attached drive SMART pre-failures
- Fibre channel array accelerator battery failures
- Fibre channel array accelerator ECC error threshold exceeded notifications
- Fibre channel array accelerator memory read errors
- Fibre channel array accelerator memory write errors
- Fibre channel array host controller failures
- Fibre channel array attached drive failures
- Fibre channel array attached drive SMART pre-failures
- Tag RAM parity errors
- ECC correctable error threshold exceeded notifications
- Server fan failures
- Server fault tolerant power supply failures
- Server VRM failed or degraded notifications
- Server agent test traps
- IDE drive failures
- Server standard SCSI attached drive failures
- Server standard SCSI attached drive SMART pre-failures
- Server standard SCSI controller failures
- Server CPU pre-failures
- RILOE battery failures
- RILOE controller failures
- External SCSI storage cabinet fan failures
- External SCSI storage cabinet power supply failures
- Integrity Server fabric and crossbar errors
- Integrity Server Core Electronic Component errors
- Integrity Server System Bus Adapter and Lower Bus Adapter errors

The following FC Switches (Brocade and McData) are supported:

B/Series (Brocade) Switches

B/Series (Brocade) Switches	Model (Number)
Brocade 4gb SAN Cube Switch	A7533A

SNMP Managed Systems

5.2 Supported Notifications

Brocade 4GB SAN Cube Switch Full Fabric	A7534A
Brocade 4gb SAN Cube Switch Power Pack	A7535A
2/128 (32-port) Base	AA981A
2/128 (32-port) Power Pack	AA982A
4/32 Full SAN Switch	A7393A
4Gb, 32 port model SAN Switch, with 32 ports activated and power pack software bundle	A7394A
4/32 Base SAN Switch	A7537A
2/16N Power Pack	AA977A
GSA 2/16N Power Pack	AD514A
2/16V Base	AA978A
GSA 2/16V Base	AD512A
2/16N Full Fabric	AA990A
GSA 2/16N Full Fabric	AD513A
2/8V Base	AA979A
GSA 2/8V Base	AD515A
2/8V Power Pack	AA980A
GSA 2/8V Power Pack	AD516A
4/256 SAN Director	A7988A
4/8 SAN Switch	A7984A
4/16 SAN Switch	A7985A

M-Series (McData) Switches

M-Series (McData) Switches	Model (Number)
McData Cube Switch	N/A
Director 2/140 (32 port)	316093-B22
Draco IV - Edge Switch 2/24	DS-DMGGE-BD / 316095-B21
Draco V - Edge Switch 2/12	None / 348406-B21
HA Fabric Manager Server	A7489A

C-Series (Cisco MDS) Switches

SNMP Managed Systems

5.3 A Note About HTTP Notifications

C/Series (Cisco MDS) Switches	Model (Number)
9509 Multilayer Director Switch	A7462A
9506 Multilayer Director Switch	A7471A
9216 Multilayer Fabric Switch	A7473A

C/Series (Cisco MDS) Switches	Model (Number)
9216A Multilayer Fabric Switch	A7558A
9216i Multilayer Fabric Switch	A7557A
9140 Multilayer Fabric Switch	A7427A
9120 Multilayer Fabric Switch	A7426A

There is no support in the following areas:

- Secondary storage, including:
tape drives, libraries, changers, and external CD towers
- Network adapters
- POST and ASR conditions
- Cluster and software conditions

5.3 A Note About HTTP Notifications

Be aware that sometimes, such as with some SMA systems, both SNMP and [HTTP Managed Systems](#) can be set up on the same system, so you may want to look through [Chapter 6](#) to see whether a system can support additional coverage.

5.4 Site Survey

In general, you should review [Chapter 2, Getting Started](#), before identifying managed systems and running kits. It is important to make the decisions described in the [Site Survey](#) before configuring reporting.

5.5 The OSEM Host

You must have an OSEM host configured and available for two-way communication before pointing managed systems to it. To check, you can ping the OSEM host from the managed system and vice versa. If you do not get the right responses, resolve the issue before continuing.

In addition, it is okay to have a combination system that performs the role of OSEM host but is also a managed system that “reports to itself” at the address **localhost** or **127.0.0.1**. Remember that the OSEM host functions must be set up first on such combination systems.

5.6 Guidelines for SNMP Systems

Managed systems that participate in SNMP notifications must include the following:

- ❑ All managed systems must have a working intranet connection, such as through an ethernet adapter, with TCP/IP installed and running. Managed systems must have two-way communication with the OSEM host over this connection.
- ❑ Managed systems need agent software for problem detection and trap generation.

IM agents are strongly recommended. The IM agents are distributed by HP and are designed to generate SNMP traps with information that allows for a more complete analysis.

Non-IM agents are supported on an as-is basis only.

- ❑ Finally, all managed systems need to have the address of the OSEM host defined as a trap destination.

The remaining sections in this chapter detail some specific, known configuration issues that have come up in the course of OSEM development and testing. These sections should not be considered a comprehensive guide to everything that might apply to your environment, however.

5.7 Windows Server 2003 Default Behavior

The OSEM host must communicate back to the managed system, but by default, Windows Server 2003 only accepts SNMP packets from the localhost. To configure Windows Server 2003 to send traps to the OSEM Server, go to Start | Programs | Administrative Tools | Services | SNMP Service. Under the Security tab, you have two options:

- Set the Windows Server 2003 to accept SNMP packets from any host.
- Individually add the OSEM host to the list.

5.8 The Storage Management Appliance

This remaining sections in this chapter describe known configuration issues for the HP OpenView Storage Management Appliance (SMA).

- [5.8.1 Connecting to the SMA](#)
- [5.8.2 Insight Manager](#)
- [5.8.3 Storage Software](#)
- [5.8.4 SNMP Traps—from IM Agents](#)
- [5.8.5 SNMP Traps—from HSV Element Manager](#)

5.8.1 Connecting to the SMA

The SMA is a “headless” Windows 2000 server, meaning it is designed to be configured and allowed to run with minimal direct user interaction—without a physical monitor, keyboard, or mouse attached.

However, some steps in this guide require access to the [Windows 2000 Desktop](#) on the SMA. Other steps require a remote browser interface pointed to the [Open SAN Manager](#) software on the SMA.

5.8.1.1 Windows 2000 Desktop

You can connect to the Windows 2000 desktop on the SMA using two methods:

- By directly connecting a monitor, keyboard, and mouse
- By running the Microsoft Terminal Services client

Every SMA is preconfigured to accept Terminal Services client connections because the Terminal Services server is preinstalled. Users who do not already have a copy of the Terminal Services client can download it from the following URL:

<http://www.microsoft.com/windows2000/downloads/recommended/TSAC/tsmsi.asp?Lang>

Desktop connections also require the account username and password for the SMA. The factory-set defaults are username **administrator** and password **admin#####**, where ##### is the last six characters of the serial number in reverse order. The password is case sensitive, and you are advised to change it (if you have not already done so) for better system security.

5.8.1.2 Open SAN Manager

You can connect to the Open SAN Manager (OSM) on the SMA by pointing your browser to the following URL. A working network connection is assumed:

SNMP Managed Systems

5.8 The Storage Management Appliance

`http://hostname-or-IP-address-of-appliance:2301/OpenSanManager/home`

Browser connections require the OSM username and password. The factory-set defaults are username **administrator** and password **administrator**.

The OSM browser display contains three sections:

- Session pane—top of the window
- Navigation pane—left portion of the window
- Content pane—right portion of the window

For more information about OSM content and use, see the *HP OpenView Storage Management Appliance Getting Started Guide*, Part Number 234873–110. (Chapter 3, Using Open SAN Manager, can familiarize you with window displays and terms that appear in this chapter.)

5.8.2 Insight Manager

Never install Insight Manager on the SMA. Insight Manager installation is not supported and can prevent browser access to the SMA.

5.8.3 Storage Software

Normally, the SMA is preconfigured to work with OSEM. However, if you have an older SMA, you must check for the following minimum software versions:

- Upgrade the SMA to Open SAN Manager (OSM) 1.0 B or greater. See the Management Appliance Update documentation for specifics.
- Install the June 2001 OSM update or greater.
- Installing all the latest SMA patches is recommended.
- To maximize reporting, ACS 8.6 or greater is recommended (applies to HSG controllers only).

5.8.4 SNMP Traps—from IM Agents

IM agents notify OSEM about events affecting the SMA itself. Configure the SNMP traps as follows:

1. Access the OSEM host. If an SMA is the OSEM host, you must connect to its SMA [Windows 2000 Desktop](#).
2. Open Start | Programs | OSEM V1.4.1 | OSEM Viewer, and press Stop Reporting.
3. Access the desired SMA. Connect to its SMA [Windows 2000 Desktop](#), if it is not already connected.
4. Go to Start | Programs | Administrative Tools | Services.

SNMP Managed Systems

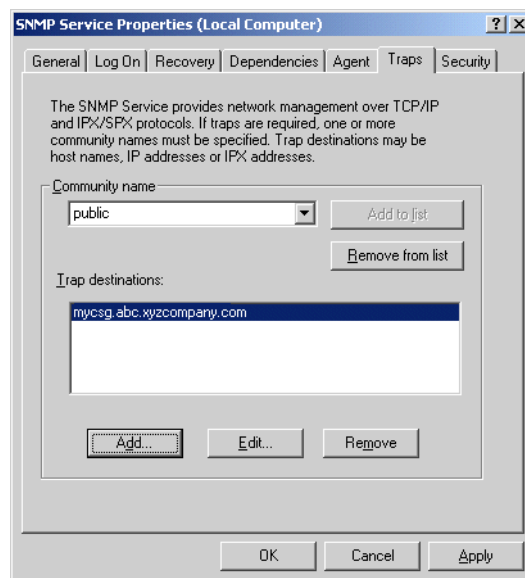
5.8 The Storage Management Appliance

5. Double-click the SNMP Service.
6. Choose the Traps tab.
7. In the Community Names field, enter a community name string. If a community name already exists, select it. If one does not exist, type **public** in the Community Names field box and press the button to add it to the list. See Figure 5–1.

The default community string is “public.” If you enter a different community string here, you also must enter it on the HP Systems Insight Manager management console that is responsible for the system. To change the community string (community strings are case-sensitive) in HP Systems Insight Manager, see the *Insight Manager User Guide* section on “Setting Up SNMP Community Strings.”

In addition, if you enter a community name other than public, you must specify communities as described in Chapter 4, Section 4.4.5, [Configuring SNMP Community Names](#).

Figure 5–1 SNMP Properties



8. Under the Trap Destinations list, press the Add button.
9. In the Host name, IP or IPX address box, type one of the following:
 - **localhost** or **127.0.0.1** if the SMA itself is the OSEM host
 - The IP address or full domain name of the separate OSEM host
10. Click Add and Apply.
11. If using a community name other than public, choose the Security tab:
 - a. Press the Add button under “Accepted community names.”

SNMP Managed Systems

5.9 SNMP Traps—from B-Series Fibre Channel Switches

- b. Set Community Rights to Read Only.
 - c. Enter the community name.
 - d. Press Add and then OK.
12. Right Click on the SNMP Service and select Restart.
 13. If prompted, click Yes on the Restart Other Services box.
 14. Press OK.
 15. Access the OSEM host. If an SMA is the OSEM host, connect to its SMA [Windows 2000 Desktop](#) if not already connected.
 16. Open Start | Programs | OSEM V1.4.1 | OSEM Viewer, and press Start Reporting.

5.8.5 SNMP Traps—from HSV Element Manager

HSV event notification is now supported by WEBES SEA.

5.9 SNMP Traps—from B-Series Fibre Channel Switches

HP B-Series Fibre Channel (FC) Switches notify OSEM of critical and serious conditions on the switch. Configure the B-Series switches as follows:

1. Add the B-Series switch the OSEM Managed Systems page. Be careful while entering the product number and serial number and other entitlement information correctly.
2. Telnet to the FC switch and login with the administrator user and password.
3. Run the `agtCfGSet` command to configure the SNMP Trap destinations. Press the Enter key by taking the default values until you see the following prompts:

```
switch:admin> agtCfGset
...
swEventTrapLevel: (0..5) [0] 3
...
```

Enter at least the value 3 for the `swEventTrapLevel`.

Note

Some firmwares allow `swEventTrapLevel` to be managed on a per trap destination basis. The prompting for the `swEventTrapLevel` may come after the trap destination is entered.

...

5.9 SNMP Traps—from B-Series Fibre Channel Switches

```
SNMP community and trap recipient configuration:
Community (rw): [Secret C0de]
Trap Recipient's IP address in dot notation: [12.87.56.162]
Community (rw): [OrigEquipMfr]
Trap Recipient's IP address in dot notation: [12.1.195.139]
Community (rw): [private]
Trap Recipient's IP address in dot notation: [0.0.0.0]
...
```

When an empty trap recipient entry (0.0.0.0) is found, enter the IP address of the OSEM host. If all the trap recipient entries appear to be used, determine if one of the entries can be replaced with the OSEM host.

If SNMP read access is limited to specific subnet areas, ensure that the switch is configured to allow access to the OSEM host. If necessary, enter the subnet area of the OSEM host at one of the the following empty (0.0.0.0) prompts:

```
SNMP access list configuration:
Access host subnet area in dot notation: [0.0.0.0]
Read/Write? (true, t, false, f): [true]
Access host subnet area in dot notation: [0.0.0.0]
Read/Write? (true, t, false, f): [true]
```

In addition to setting up the SNMP trap destinations, some firmwares allow precise MIB and trap functionality enablement FC Switch using the `snmpmibcapset` command. If your firmware supports the `snmpmibcapset` command, run the command configuring at least the settings displayed in **underlined-bold** below.

Note

Not setting up your FC switch in the way identified below may cause OSEM to not receive all the trap events.

```
switch:admin> snmpmibcapset
The SNMP Mib/Trap Capability has been set to support:
FE-MIB
SW-MIB
FA-MIB
SW-TRAP
FA-TRAP
SW-EXTTRAP
FA-MIB (yes, y, no, n): [no]
FICON-MIB (yes, y, no, n): [no]
HA-MIB (yes, y, no, n): [no] yes
SW-TRAP (yes, y, no, n): [no] yes
  swFCPortScn (yes, y, no, n): [no] yes
  swEventTrap (yes, y, no, n): [no] yes
  swFabricWatchTrap (yes, y, no, n): [no]
  swTrackChangesTrap (yes, y, no, n): [no]
FA-TRAP (yes, y, no, n): [no]
SW-EXTTRAP (yes, y, no, n): [no] yes
HA-TRAP (yes, y, no, n): [no] yes
  fruStatusChanged (yes, y, no, n): [no] yes
  cpStatusChanged (yes, y, no, n): [no] yes
  fruHistoryTrap (yes, y, no, n): [no]
```

5.10 SNMP Traps – From C/Series Fibre Channel Switches

HP C/Series Fibre Channel Switches notify OSEM of error conditions on the switch. Configure the C/Series switches as follows:

1. Add the C/Series switch to the OSEM Managed Systems page. Take caution to enter the product number and serial number and other entitlement information correctly.
2. Access the switch CLI (telnet or SSH).
3. Run the following commands (in **bold**) to allow the OSEM host to communicate with the switch (the example below uses `public` as the read-only community name, any valid community name can be used):

```
switch# config  
switch(config) # snmp community public ro
```

4. Run the following commands (in **bold**) to configure the switch to send traps to the OSEM host (use the IP address of the OSEM host for *ipaddress*):

```
switch# config  
switch(config) # snmp host ipaddress traps v1 udp-port 162
```

HTTP Managed Systems

This chapter describes HTTP based notifications from managed systems to the OSEM host.

Overview	page 6-2
A Note About SNMP Notifications	page 6-2
Site Survey	page 6-2
The OSEM Host	page 6-2
WEBES Systems	page 6-2
Windows (Non-Appliance)	page 6-4
The Storage Management Appliance	page 6-6
DECevent Systems	page 6-8
Tru64 UNIX	page 6-9
OpenVMS	page 6-11

HTTP Managed Systems

6.1 Overview

6.1 Overview

OSEM provides for collection and auto-reporting of events from systems capable of sending event data over HTTP. Systems in this category include WEBES capable systems, non-WEBES systems that run DECEvent, and the HAFM server attached to M/Series FC switches.

6.2 A Note About SNMP Notifications

Be aware that sometimes, such as with some SMA systems, both HTTP and [SNMP Managed Systems](#) can be set up on the same system, so you may want to look through [Chapter 5](#) to see whether a system can support additional coverage.

6.3 Site Survey

In general, you should review [Chapter 2, Getting Started](#), before identifying managed systems and running kits. It is important to make the decisions described in the [Site Survey](#) before configuring reporting.

6.4 The OSEM Host

You must have an OSEM host configured and available before pointing managed systems to it. To check, you can ping the OSEM host from the managed system and vice versa. If you do not get the right responses, resolve the issue before continuing.

In addition, it is okay to have a combination system that performs the role of OSEM host but is also a managed system that “reports to itself” at the address **localhost** or **127.0.0.1**. Remember that the OSEM host functions must be set up first on such combination systems.

6.5 WEBES Systems

OSEM works in conjunction with WEBES to monitor the event log, providing detection and auto-reporting of events affecting storage subsystems and hosts:

- **Host Based Storage**—Windows, Tru64 UNIX, and OpenVMS host-based storage is supported.
- **SAN Based Storage**—OSEM supports automated notification for SAN-based storage attached to the HP OpenView Storage Management Appliance (SMA).
- **Host Servers**—The same WEBES software that allows for auto-reporting of host-based storage events will detect and auto-report events directly affecting Tru64 and OpenVMS servers.

This chapter does not repeat the information already available in the WEBES installation manual, user guides, and release notes. However, it makes an effort to clarify known configuration issues that have come up in the course of OSEM development and testing. Refer to your WEBES documentation as the first resource for WEBES configuration and usage.

6.5.1 Supported Notifications

WEBES notifications are supported only on OSEM hosts that are configured for local email only (without remote notification). In the OSEM Viewer, you must set the outbound protocol to “None” on the Internal Settings page if you are pointing WEBES systems to the OSEM host. See the *OSEM User Guide* or help if you need additional details.

Remote WEBES notification via ISEE requires that the ISEE Client be installed directly on the WEBES system (see Figure 1–2). Remote WEBES notifications are not supported by the ISEE Client that forwards remote notifications on behalf of the OSEM host.

The specific notifications that WEBES will send are derived from the WEBES Supported Products List. Be sure to check the list shown in the WEBES documentation for your version of WEBES.

6.5.2 Guidelines for WEBES Systems

Managed systems need to have WEBES installed according to the instructions in the *WEBES Installation Guide*, with the following considerations. You may want to print these notes, and keep them on hand while installing WEBES.

- ❑ All managed systems must have a working intranet connection, such as through an Ethernet adapter, with TCP/IP installed and running. Managed systems must be able to communicate with the OSEM host over this connection.
- ❑ SEA is required. The other WEBES tools are optional.
- ❑ Before installing, purge the event log as described in the *WEBES Installation Guide*. SEA scans the existing log after installation, so this prevents a large number of unwanted reports from older log entries.

Caution: Purging the log during an active scan can result in lost or scrambled event data. If you forget to purge before SEA begins scanning, stop the Director process, purge the log, and restart the Director.

- ❑ WEBES may warn you that DSNLink is not installed. DSNLink is not required, so any references to DSNLink can safely be ignored.
- ❑ If needed, see Appendix A in this manual for more information about filling in the profile.txt file.
- ❑ After installing, enter **desta qsap on** from the command prompt. For QSAP, enter or confirm the address of the OSEM host. Enter or confirm **2069** as the port number that the host is listening on.

HTTP Managed Systems

6.5 WEBES Systems

- ❑ Optional test message—After installing, you may want to verify notification by sending a test event as described in Section B.1, [Verifying WEBES Notifications](#).

The remaining sections in this chapter detail some specific, known configuration issues that have come up in the course of OSEM development and testing. These sections should not be considered a comprehensive guide to everything that might apply to your environment, however.

6.5.3 Windows (Non-Appliance)

Note

SAN-based storage attached to the HP OpenView Storage Management Appliance, which also runs Windows, is a unique configuration and is covered in Section 6.5.4.

Storage event log notifications require that you configure your Windows storage environment and host with the following:

- ❑ Working storage subsystem (e.g. HSG80)
- ❑ Supported host bus adapter for fiber optic (copper not supported)
- ❑ HSG80 storage subsystems ACS V8.5 or higher
- ❑ Fiber kit from SecurePath 3.1

If installing SANWorks SecurePath: Install the fiber kit from the SecurePath 3.1 distribution (from the Fiberchannel Software Setup folders). Do not install the fiber kit from the StorageWorks Platform Solution Kit. This step installs the proper drivers such as raidisk.sys for Windows 2000.

- ❑ SANWorks SecurePath for Windows

If installing SANWorks SecurePath: Install SecurePath and see Table 6–1 to verify necessary files revisions before continuing.

Table 6–1 Files Revisions Required for SANWorks Secure Path 3.1—Windows 2000

Driver	Description	Minimum Revision
Windows 2000 Directory location: Winnt\system32\drivers		
Raidisk.sys	Compaq multipath driver	3.1.11
Compaq KGPSA-xx PCI-Fibre Channel HBA	Compaq driver not digitally signed	5.4.41.0

Table 6–1 Files Revisions Required for SANWorks Secure Path 3.1—Windows 2000 (continued)

Driver	Description	Minimum Revision
Windows 2000 Directory location: \Program Files\Compaq\StorageWorks FC-Switch\ or \Program Files\Compaq\StorageWorks FC-AL\		
HS_Service.exe	logging service	minimum date 2/2/2000
HSZservicecontrol.dll	logging service	minimum date 2/2/2000

SWCC agent

If installing SWCC: Install the StorageWorks Command Console (SWCC) agent.

StorageWorks Platform Solution Kit

Install the fiber kit from the StorageWorks Platform Solution Kit only if you are not installing SANWorks SecurePath.

There are platform solutions kits on the software CD that have V245al (arbitrated loop) and V245sw (switch based) kits for the HSG80. The kits install the necessary drivers and services required for event logging to function properly. Before installing OSEM, check to ensure that these correct drivers have been installed.

While newer StorageWorks Platform Solution Kits may become available, the system must conform to at least the minimums described in Table 6–2.

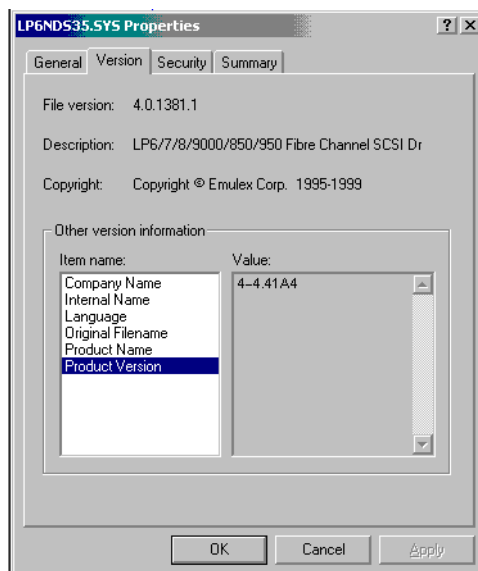
Table 6–2 File Revisions Required For StorageWorks Platform Solution Kit—Windows 2000

File	Minimum Revision
StorageWorks 8.5A Platform Solution Kit on Windows 2000 Check the following files:	
In the directory matching your configuration: \Program Files\Compaq\StorageWorks FC-Switch\ or \Program Files\Compaq\StorageWorks FC-AL\	
HS_Service.exe	Minimum date 2/2/2000
HszServiceControl.dll	Minimum date 2/02/2000
CPQKGPSA.sys	Minimum product version 5–4.41A4 (Open the file properties and look at the product version as shown in Figure 6–1.)

HTTP Managed Systems

6.5 WEBES Systems

Figure 6–1 Sample LP6NDS35.SYS Product Version



6.5.4 The Storage Management Appliance

This section describes known configuration issues for the HP OpenView Storage Management Appliance (SMA).

- [6.5.4.1 Connecting to the SMA](#)
- [6.5.4.2 Insight Manager](#)
- [6.5.4.3 Storage Software](#)
- [6.5.4.4 Event Log Size](#)

6.5.4.1 Connecting to the SMA

The SMA is a “headless” Windows 2000 server, meaning it is designed to be configured and allowed to run with minimal direct user interaction—without a physical monitor, keyboard, or mouse attached.

You can connect to the Windows 2000 desktop on the SMA using two methods:

- By directly connecting a monitor, keyboard, and mouse
- By running the Microsoft Terminal Services client

Every SMA is preconfigured to accept Terminal Services client connections because the Terminal Services server is preinstalled. Users who do not already have a copy of the Terminal Services client can download it from the following URL:

<http://www.microsoft.com/windows2000/downloads/recommended/TSAC/tsmsi.asp?Lang>

Desktop connections also require the account username and password for the SMA. The factory-set defaults are username **administrator** and password **admin#####**, where ##### is the last six characters of the serial number in reverse order. The password is case sensitive, and you are advised to change it (if you have not already done so) for better system security.

6.5.4.2 Insight Manager

Never install Insight Manager on the SMA. Insight Manager installation is not supported and can prevent browser access to the SMA.

6.5.4.3 Storage Software

Normally, the SMA is preconfigured to work with OSEM. However, if you have an older SMA, you must check for the following minimum software versions:

- Upgrade the SMA to Open SAN Manager (OSM) 1.0 B or greater. See the Management Appliance Update documentation for specifics.
- Install the June 2001 OSM update or greater.
- Installing all the latest SMA patches is recommended.
- To maximize reporting, ACS 8.6 or greater is recommended (applies to HSG controllers only).

6.5.4.4 Event Log Size

If the SMA also is the OSEM host, follow these steps to modify the default application log settings to ensure that the event log has sufficient room to store incoming events.

1. Connect to the SMA Windows 2000 desktop.
2. Go to Start | Settings | Control Panel | Administrative Tools | Event Viewer | Application Log | Properties.

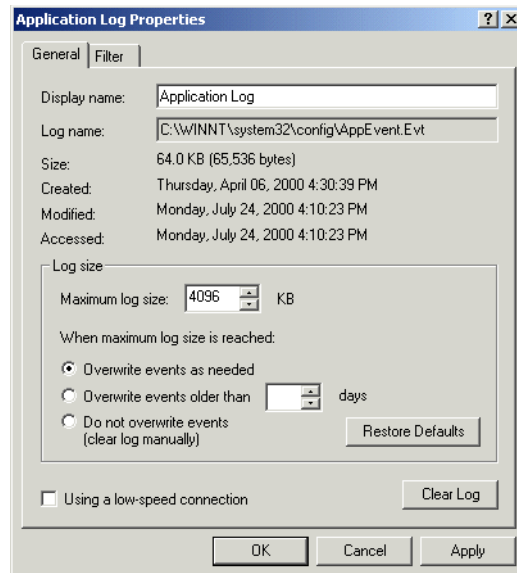
Increase the maximum log size to 4096 KB, and set the Event Log Wrapping to overwrite events as needed (see Figure 6-2). Click OK.

These settings supersede the ones from the *SEA User Guide*, if they are different.

HTTP Managed Systems

6.6 DECEvent Systems

Figure 6–2 Event Log Settings



6.6 DECEvent Systems

DECEvent systems traditionally used SICL reporting to the service provider over DSNLink. By adding the Event Notification Program (ENP) and registering it with DECEvent, you send notifications to the OSEM host via HTTP instead. These systems include:

- Non WEBES-capable AlphaServers running Tru64 UNIX
- Non WEBES-capable AlphaServers running OpenVMS
- OpenVMS VAX systems

Be aware that DECEvent does not provide the same level of coverage and support as WEBES. For example, there is no automated notification for VAX/VMS, and there is very limited storage coverage.

6.6.1 Guidelines for DECEvent Systems

The DECEvent managed systems described in this section require the following:

- DECEvent 3.4 for event analysis
- ENP—a small executable and script
- A working network connection over which they can communicate with the OSEM host

The remaining sections in this chapter detail some specifics regarding ENP, because ENP lets DECEvent send its data over HTTP to the OSEM host. Users should refer to their DECEvent documentation for information about installing, configuring, and using DECEvent.

6.6.2 Tru64 UNIX

After DECEvent 3.4 is installed and configured, follow these steps to install and configure ENP on non-WEBES AlphaServers running Tru64 UNIX:

1. Log in as super user (root).
2. Extract the ENP kit contents:

```
# tar -xvf DECEvent_ENP.tar
```

3. Copy the three files to the appropriate directories:

```
# cp enp /usr/bin
# cp enp.config /etc
# cp csgnotify /usr/opt/DIA340/sbin
```

Table 6-3 ENP Files for Tru64 UNIX

File	Target Directory	Description
enp	/usr/bin	Event Notification Program
enp.config	/etc	Configuration file
csgnotify	/usr/opt/DIA340/sbin	Notification script file

4. Change the permissions on the executable and script files:

```
# chmod +x /usr/bin/enp
# chmod +x /usr/opt/DIA340/sbin/csgnotify
```

5. Edit two environment variables in the enp.config file and save the file. Set the CSG_SERVER variable to the fully qualified name of the OSEM host. Set the PORT variable to the receiving port on the OSEM host (2069 by default).

```
CSG_SERVER=osemhost.abc.xyzcompany.com
PORT=2069
```

6. Invoke DECEvent:

```
# /usr/sbin/dia -int
```

7. Show external registered scripts, and look for the old WorldWire wwnotify script:

```
dia>shw ext
```

8. Remove the wwnotify script:

```
dia>rm ext -f /usr/opt/DIA340/sbin/wwnotify -l customer
```

9. Add the new csgnotify script:

HTTP Managed Systems

6.6 DECEvent Systems

```
dia>ad ext -f /usr/opt/DIA340/sbin/csgnotify -l customer
```

10. Exit DECEvent:

```
dia>exit
```

11. Verify the existence of the file /usr/opt/DIA340/tmp/WWNotify_SysInfo.txt. If the file does not exist, enter the following command to create it:

```
# /usr/sbin/diasetup
```

Clusters—You must run the diasetup command on each node of a cluster to ensure the proper reporting of node-specific information.

12. Configure a DECEvent customer profile text file if you have not already done so (see below).
13. Show DECEvent external registered scripts, and look for the new csgnotify script:

```
# /usr/sbin/dia shw ext
```

14. Verify the ENP script installation by running a DECEvent test command:

```
# /usr/sbin/dia tst -e customer
```

15. Open the OSEM Viewer in a web browser (http://<osem_host>:2069/default.htm) and click the Notifications link. The Notifications page should display the test notification generated by DECEvent.

DECEvent Profile File

The customer profile text file contains system and contact information as explained in Appendix A. Although Appendix A deals primarily with WEBES profile files, the overall reasons for having the file and what it should contain are the same. For DECEvent on Tru64 UNIX, follow these specific steps when configuring the profile file:

1. Copy the text file containing the customer profile to /var/DIA/FMGPROFILE.
2. See if the DECEvent system setting FMG__CUST_PROFILE contains the correct path and filename:

```
# /usr/sbin/dia shw set FMG__CUST_PROFILE
```

3. If necessary, correct the path and filename:

```
# /usr/sbin/dia -int
dia>set sys FMG__CUST_PROFILE /var/DIA/FMGPROFILE
dia>sav sys
dia>exit
```

6.6.3 OpenVMS

After DECEvent 3.4 is installed and configured, follow these steps to install and configure ENP on non-WEBES AlphaServers or VAX systems running OpenVMS:

1. Log in as the system manager or set `proc/priv=all`.
2. Extract the ENP kit contents:

For Alpha systems:

```
$ RUN DECEVENT_ENP_ALPHA.EXE
$ BACKUP DECEVENT_ENP_ALPHA.BCK/SAVE_SET *
```

For VAX systems:

```
$ RUN DECEVENT_ENP_VAX.EXE
$ BACKUP DECEVENT_ENP_VAX.BCK/SAVE_SET *
```

3. Copy the two files to the appropriate directories:

```
$ COPY /LOG ENP_DECEVENT.EXE SYS$SYSTEM:
$ COPY /LOG CSGNOTIFY.COM SYS$MANAGER:
```

Table 6–4 ENP Files for OpenVMS

File	Target Directory	Description
ENP_DECEVENT.EXE	SYS\$SYSTEM	Event Notification Program
CSGNOTIFY.COM	SYS\$MANAGER	Notification script file

Clusters—Copy the two files to `SYS$COMMON:[SYSEXE]` and `SYS$COMMON:[SYSMGR]`, respectively, if you do not want to put copies on every node in the cluster.

4. In your system startup file, define the following logical names:

```
$ DEFINE/SYSTEM/EXEC CS_GATEWAY$NODE_DECEVENT "<OSEM_HOST>"
$ DEFINE/SYSTEM/EXEC CS_GATEWAY$NOTIFY_DECEVENT SYS$MANAGER:CSGNOTIFY.COM
```

Where `<OSEM_HOST>` is the fully qualified name of the OSEM host, for example:

```
$ DEFINE/SYSTEM/EXEC CS_GATEWAY$NODE_DECEVENT "osem.abc.xyzcompany.com"
```

5. If the receiving port on the OSEM host is other than the default 2069, also define the following logical name within the startup file:

```
$ DEFINE/SYSTEM/EXEC CS_GATEWAY$PORT_DECEVENT "<Port_Number>"
```

6. Invoke DECEvent:

```
$ DIA /INT
```

HTTP Managed Systems

6.6 DECEvent Systems

7. Show external registered scripts, and look for the old WorldWire wwnotify script:

```
DIA>SHOW EXTERNAL
```

8. Remove the old WorldWire wwnotify script.

Removing the WorldWire notification script may require you to open another window and translate logical names that are registered. Remove the logical that translates to the wwnotify.com file. (To translate a logical, enter the command SHOW LOGICAL <logical_name>.)

```
DIA>REMOVE EXTERNAL <logical_name> CUSTOMER
```

9. Add the new CSGNOTIFY script:

```
DIA>ADD EXTERNAL CS_GATEWAY$NOTIFY_DECEVENT CUSTOMER
```

10. Exit DECEvent:

```
DIA>EXIT
```

11. Configure a DECEvent customer profile text file if you have not already done so (see below).
12. Show DECEvent external registered scripts, and look for the new CSGNOTIFY script:

```
$ DIA SHOW EXTERNAL
```

13. Verify the ENP script installation by running a DECEvent test command:

```
$ DIA TEST EXTERNAL CUSTOMER
```

14. Open the OSEM Viewer in a web browser (http://<osem_host>:2069/default.htm) and click the Notifications link. The Notifications page should display the test notification generated by DECEvent.

DECEvent Profile File

The customer profile text file contains system and contact information as explained in Appendix A. Although Appendix A deals primarily with WEBES profile files, the overall reasons for having the file and what it should contain are the same. For DECEvent on OpenVMS, follow this specific step when configuring the profile file:

Edit the DECEvent startup file (SYSS\$STARTUP:DECEVENT\$STARTUP.COM) to define a logical name identifying your profile:

```
$ DEFINE/SYS/EXEC FMGPROFILE disk:[path]your_filename.txt
```

Where disk:[path]your_filename.txt is the full path and filename of the profile file.

6.7 M/Series FC Switch Systems

The HAFM server is a notebook PC with the HAFM application installed. The application provides an interface for operating and managing the M/Series FC switch, and can forward switch event data to OSEM via HTTP.

Follow these steps to point the HAFM server to the OSEM host. The procedure includes a restart of the HAFM server.

1. Add the HAFM server name or IP to the enabled clients list.
2. Create a managed system page entry for HAFM using its name or IP as a key and provide serial and product number information along with entitlement information if required.
3. From the HAFM server, ensure that there is a working network connection to the OSEM host.
4. Open the properties file to configure the HAFM phone-home.

On HAFM 7.X open the following file:

```
C:\Program Files\HAFM\rns.properties
```

On HAFM 8.X open the following file:

```
C:\Program Files\HAFM 8.2\CallHome\Config\hp-lan.properties
```

5. Look for the lines shown below:

```
RnsDataDir=c:\HAFMData\RnsData  
RnsEventDir=c:\HAFMData\RnsData  
RnsLogDir=c:\HAFMData\Rnsdata  
CSGIpAddress=  
CSGPort=2069  
CSGExePath=/ms/eventAsync
```

6. Make the following changes:

CSGIpAddress—Enter the name or IP address of the OSEM host, for example:
osemhost.abc.xyzcompany.com.

CSGPort—Leave the default of 2069, unless you know that the OSEM host has been reconfigured to receive messages on another port.

7. Save and close the properties file.
8. To apply the changes, restart the HAFM server. Restarting the HAFM server does not adversely affect the operation of the director or fabric.

The Customer Profile File

This appendix provides additional detail about the customer profile file, including what it is, how it works, and examples of how to set up typical profile files.

Overview	page A-2
How the Profile File Works	page A-2
Number of Profile Files	page A-2
Location of the Profile File	page A-2
Calling the Profile File	page A-3
Profile Template	page A-3
Configuration Information	page A-3

The Customer Profile File

A.1 Overview

A.1 Overview

Automatic WEBES notifications let you dispatch the appropriate corrective actions at your site. An important part of these notifications includes matching system information to the fault and failure messages from WEBES. Your customer profile file is the key to this task.

A.2 How the Profile File Works

When serviceable events are identified on a managed system, WEBES assembles a text message about the failure, including summary analysis, and attaches your profile text file to the message. Then, the entire message gets securely routed to the OSEM host within your enterprise. The OSEM host forwards the message as email to recipients of your choosing.

The profile file helps the message accurately identify the following:

- The department, location, phone number, and contact person
- The managed system from which the message originated, including address, physical location, contact person for that managed system, and so on

In instances where the managed system includes attached Enterprise Array Controllers or SAN storage, the profile file becomes very important in indicating storage configuration, exact FRUs, and physical location of any failing component (see Section [A.7](#)).

A.3 Number of Profile Files

A managed system must have access to at least one profile text file. One suggested setup is to have a profile file on each managed system. However, in a cluster environment it might be more efficient to create a single profile file and store it in a suitable directory on a common, shared disk that all nodes in the cluster have read access to. Provided that you reference the correct file path (see Section [A.5](#)), there is no reason you cannot edit, update, and maintain a profile file in a different location than the suggested default.

A.4 Location of the Profile File

Even after installing WEBES, you can manually update the profile file using any text editor. The default name and location for the profile file is in the \config subdirectory under your WEBES (svctools) installation, as shown.

```
C:\Program Files\hp\svctools\specific\desta\config\profile.txt
```

You can, however, locate and name the profile file as desired, provided that the managed system always has access to it.

A.5 Calling the Profile File

So that WEBES can detect the profile file, its path is specified in the following file:

```
C:\Program Files\hp\svctools\specific\desta\config\desta.reg
```

If you move the profile file from its default location, update the following line in the `desta.reg` file. You can edit `desta.reg` with any text editor.

```
CA.ACHSProfile=filename
```

Filename is the path and name of the profile file. Be aware that backslash characters must be doubled for the path to be interpreted correctly. For example:

```
CA.ACHSProfile=C:\\Program  
Files\\hp\\svctools\\specific\\desta\\config\\profile.txt
```

A.6 Profile Template

The WEBES kit (on Windows) prompts you with a template `profile.txt` file during installation. You then edit and use this template as a model. It includes the following headings, which you must fill in, add to, or modify as necessary to create a complete profile.

```
Customer:  
Address:  
System Type:  
Serial number:  
Primary Contact:  
Secondary Contact:  
Phone number:  
Special Instructions:  
  
CONFIGURATION INFORMATION:  
  
SYSTEM:                Model:  
System S/N:            System Name:  
System IP address:    Fixed ( ) DHCP Served ( )  
  
<other configuration information>  
Storage:
```

A.7 Configuration Information

Adding storage configuration information to the profile file is very important. For example, when your storage is part of a storage area network (SAN), event detection occurs within the SAN itself, but the event information gets logged to all the hosts attached to the SAN environment. As such, multiple managed systems may in fact receive event information indicating the same potential failure because of the shared/redundant resource nature of the SAN.

The Customer Profile File

A.7 Configuration Information

Ultimately, this one event may be reported as multiple events. With accompanying configuration information, however, your administrator is able to build a true picture of where the fault is and more accurately direct resources to the physical location of the problem.

If your system is well bounded (i.e. all storage is directly attached to SmartArray Controllers on the servers), simpler configuration information is usually enough.

A.7.1 Sample Profile 1—Simple

The following is a simple profile.txt depicting:

- ProLiant server
- No attached ESA12000/RA8000 Storage Array Subsystem

```
Customer: Acme Stonecutting, Inc.
System Type: ProLiant Model 5500
System S/N: V907-BY43-1972 System Name: ARGOSS
System IP address: 123.4.567.89 Fixed(X) DHCP Served ( )
Primary Contact: Fred Flintstone
Secondary Contact: Barney Rubble
Phone number: (xxx) 555-5555
Special Instructions:
Check with customer prior to dispatching services. Prior notification to
security is necessary for service access to site.
Remote call back to system permissible w/prior notification to customer so
that account may be enabled.
CONFIGURATION INFORMATION:
Qty 2 - KZPAC array controllers on PCI bus #1 attached to qty 6 StorageWorks
I shelves w/disks.
```

A.7.2 Sample Profile 2—MSCS Cluster

The following shows configuration information from a profile.txt depicting:

- 2 ProLiant servers
- Attached to ESA12000/RA8000 Storage Array Subsystem
- The servers are in an MSCS configuration.

```
CONFIGURATION INFORMATION:
MS Cluster Systems
SYSTEM: ProLiant Model: 5500
System S/N: V907-BY43-1972 System Name: SNOBAL
System IP address: 192.7.100.99 Fixed(X) DHCP Served ( )
SYSTEM: ProLiant Model: 5500
System S/N: V903-BW43-1972 System Name: QUEBAL
System IP address: 192.7.100.98 Fixed(X) DHCP Served ( )
Compaq FC Switch 16 Serial # 3G944001233
TCPIP 192.7.100.100
Compaq FC Switch 16 Serial # 3G944001235
TCPIP 192.7.100.101
ESA12000 Array Controller
Subsystem Name: Joiner
joiner-Top >> HSG80 ZG91416110 Software S056P-0, Hardware E06
joiner-Bottom>> HSG80 ZG83502157 Software S056P-0, Hardware E03
```

The Customer Profile File

A.7 Configuration Information

```
ESA12000 Array Controller
Subsystem Name: Partn
partnr-Top >> HSG80 ZG91516230 Software S056P-0, Hardware E06
partnr-Bottom>> HSG80 ZG91516231 Software S056P-0, Hardware E03
```

A.7.3 Sample Profile 3—MSCS Cluster with DRM

The following shows configuration information from a profile.txt depicting:

- Data Replicator Storage Solution
- Two (initiator and target) sites
- 2 ProLiant servers on each site
- ESA12000/RA8000 Storage Array Subsystems interconnected by FC Switches between the sites.
- FC SAN is linked between Initiator/Target sites by Compaq FC Gateway ATM interfaces and a leased ATM circuit.
- The servers are in an MSCS configuration.

```
CONFIGURATION INFORMATION:
INITIATOR SITE: DENVER
Denver, CO., US
1244 E. McGuire Way, Floor 2, Room CR1
MS Cluster Systems
SYSTEM: ProLiant Model: 8500
System S/N: Q762-BHET-AE43-1305 System Name: FSTBAL
System IP address: 192.7.100.99 Fixed(X) DHCP Served ( )
SYSTEM: ProLiant Model: 8500
System S/N: Q761-BHET-AE44-0900 System Name: CRVBAL
System IP address: 192.7.100.98 Fixed(X) DHCP Served ( )
ESA12000 Storage ARRAY CONTROLLER
Subsystem Name: Denver
denver-Top >> HSG80 ZG91416110 Software S056P-0, Hardware E06
denver-Bottom>> HSG80 ZG83502157 Software S056P-0, Hardware E03
Compaq FC Switch 16 Serial # 3G944001233
TCPIP 192.7.100.100 Fixed(X) DHCP Served ( )
Compaq FC Switch 16 Serial # 3G944001235
TCPIP 192.7.100.101 Fixed(X) DHCP Served ( )
FC GATEWAY Serial # 52623434
TCPIP 192.7.100.102 Fixed(X) DHCP Served ( )
Dial-in Phone Number to FC Gateway Asynchronous Switch
Ph. 303-555-xxxx
-----
TARGET SITE: CHICAGO
Chicago, Ill, CO., US
1245 Times Blvd.
Floor 7, CR200
MS Cluster Systems
SYSTEM: ProLiant Model: 5500
System S/N: xxxxxxxxxxxxxx System Name: SNKBAL
System IP address: 192.7.100.79 Fixed(X) DHCP Served ( )
SYSTEM: ProLiant Model: 5500
System S/N: xxxxxxxxxxxxxx System Name: SLDBAL
System IP address: 192.7.100.78 Fixed(X) DHCP Served ( )
ESA12000 Array Controller
Subsystem Name: Chicago
chicago-Top >> HSG80 ZG91416110 Software S056P-0, Hardware E06
chicago-Bottom>> HSG80 ZG83502157 Software S056P-0, Hardware E03
Compaq Switch 16 Serial # 3G012000435
```

The Customer Profile File

A.7 Configuration Information

```
TCPIP 192.7.100.200 Fixed (X) ) DHCP Served ( )
Compaq Switch 16 Serial # 3G9012000422
TCPIP 192.7.100.201 Fixed (X) ) DHCP Served ( )
FC GATEWAY Serial # 526538653
TCPIP 192.7.100.202 FIXED ) DHCP Served ( )
Dial-in Phone Number to FC Gateway Asynchronous Switch
Ph. 312-222-xxxx
```

B

Troubleshooting

This guidelines in this appendix may help in troubleshooting your OSEM installation.

Verifying WEBES Notifications	page B-2
Verifying SNMP Notifications	page B-2
SNMP GET Failures	page B-4
System Name Issues	page B-4
System Name Issues	page B-4
OSEM Log File	page B-4
TCP/IP Ports Used by OSEM	page B-4
Decompression Message	page B-5
Services	page B-5
Processes	page B-5
Interpreting Copies of Problem Reports	page B-5

Troubleshooting

B.1 Verifying WEBES Notifications

B.1 Verifying WEBES Notifications

You can verify that SEA is transmitting messages from the managed system by sending a test message at the command prompt of the managed system:

```
C:\> wsea test
```

Successful test message receipt to the specified email addresses indicates that the managed system is communicating properly.

Additional troubleshooting can include opening a web browser and pointing it to SEA on the managed system (http://managed_server_address:7902). Then, check the event log on the managed system for the test event and the callout.

Also, if the OSEM host is properly enabled, a notify message should be found in the OSEM host application event log.

Testing by Creating a Fault

During verification of proper fault handling, you might decide to manually induce a test fault. In some of these cases, the test event could be written to the Windows event log but not get correctly analyzed by SEA. If you suspect this is happening, check your StorageWorks Platform Solution Kit installation, and ensure that the file dates and versions conform to the minimum prerequisites.

B.2 Verifying SNMP Notifications

B.2.1 Generating SNMP Traps from System Management Home Page

The following steps allow the user to send a test trap from the managed system to the OSEM host to verify the SNMP setup. These steps work for both MS Windows and Linux systems.

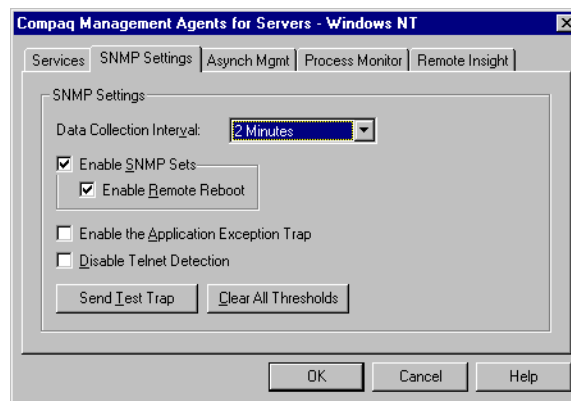
1. Connect to the managed system with a browser on port 2381.
(https://managed_system:2381)
2. Login with administrator or root privilege
3. Select the Settings tab.
4. Select SNMP and Agent Settings
5. Push the Test Trap Button

B.2.2 Generating SNMP Traps from Windows

Follow these steps on the managed system to verify that IM agents are sending traps.

1. Verify the SNMP configuration as described under [SNMP Managed Systems](#) in Chapter 5.
2. Open the Insight Agents icon under Start | Settings | Control Panel.
3. Under the SNMP Settings tab, press the Send Test Trap button (see Figure B-1). Not all tabs shown in Figure B-1 will be available on all servers.

Figure B-1 SNMP Test



B.2.3 Generating SNMP Traps from UNIX and Linux

```
Linux> snmpset -v 1 -c public <ip address> enterprises.232.11.2.8.1.0 s "Test Trap"
Linux> snmpset -v 1 -c public <ip address> enterprises.232.11.2.8.1.0 s " "
```

The IP address would be the one for the managed system that is to send the trap. The OSEM server address would be specified by the `snmpd.conf` file on the managed system.

The command is in `/usr/sbin` and needs to be executed from there if the path for that is not set on that particular UNIX system.

B.2.4 Generating SNMP Traps from NetWare

To send test traps from NetWare:

- Log into the System Management Homepage.
- Go to the Settings tab.
- Click the Send Test Trap button - you need to make sure the destination IP address is in the `SYS:\ETC\traptarg.cfg` file.

B.3 SNMP GET Failures

To complete a problem report, OSEM must be able to connect back to the system that generated the trap. If the OSEM log reveals a GET failure, check for these possible explanations:

- A community string mismatch
- Host restrictions listed in the SNMP service applet
- An agent not running on the managed system

B.4 System Name Issues

When OSEM receives a trap, it sees the IP address and performs a reverse lookup to find the system name. In some environments, WINS servers and DNS servers do not provide the same system name. Furthermore, name resolution seen from two different systems can differ depending on location in the network and the timing associated with response messages.

Address any name space configuration issues in your environment to correct this kind of problem.

B.5 OSEM Log File

During installation, OSEM generates a log file in the defined TEMP directory called OSEMInfo.txt that may be of use in troubleshooting installation problems. The kit writes text entries to OSEMInfo.txt that include product names, versions, build numbers, install start and finish timestamps, and operating system information.

B.6 TCP/IP Ports Used by OSEM

OSEM and its member components use system port numbers as described in Table B-1.

Table B-1 Port Numbers Used by OSEM

Port	Machine Type	Use
2301	OSEM host	Web GUI port for Insight Manager Web Agents. When authorized, it is used by HP Service for remote troubleshooting access.

Table B-1 Port Numbers Used by OSEM (continued)

Port	Machine Type	Use
2381	OSEM host	Secure System Management Homepage
7902	Managed System	Web GUI port for SEA. When authorized, it is used by HP Service for remote troubleshooting access.
2069	OSEM host	Web port used by OSEM service to receive events from managed systems

B.7 Decompression Message

If the installation drive does not have enough space to unpack the OSEM installation files from the software CD or stored location, the following message appears:

```
Error 1926 - could not set security for file "c:\config.msi\  
Error 5: verify that you have sufficient privileges to modify security for  
this file.
```

Be sure that the system has the necessary free space available as described in the prerequisites.

B.8 Services

The following service gets installed with OSEM:

Display Name: Open Service Event Manager
Name: CRSMInvoker

B.9 Processes

OSEM installs the process CRSM5Invoker.exe as a wrapper executable, plus java.exe, which is the central process.

B.10 Interpreting Copies of Problem Reports

When OSEM generates an email copy of a problem report, it lists all of the possible fields in an end-to-end OSEM reporting scenario. Depending on service offering and where the copy is viewed, users may see some unpopulated fields. This is because certain values are provided by the managed system while others are provided by the OSEM host.

For example, if you read the email copy of a problem report generated on a managed system and mailed from that managed system, you see empty fields—ones that eventually get populated by the OSEM host once the report travels through that system.

Another scenario occurs when problem report fields are populated only by certain OSEM agents. For example, an SNMP trap from OSEM for SNMP populates the SNMP_OIDS field, but an event log entry does not. Likewise, a problem report from SEA in OSEM for Event Log populates its own subset of the fields.

Note that the detailed portion of any email copies of problem reports is intended for OSEM debugging.

Products Supported by OSEM

This appendix provides a cumulative list of products that are supported by OSEM. The list of products is not exhaustive and currently only includes products since OSEM Version 1.4.4.

ProLiant Support	page C-2
Integrity Support	page C-2
Switch and Tape Support	page C-3
Multivendor Support	page C-5
MSADB 1.52.90 Ruleset	page C-5

Products Supported by OSEM

C.1 ProLiant Support

C.1 ProLiant Support

At OSEM 1.4.7, support for ProLiant servers includes the following:

- The MSADB ruleset version 1.52.90 supports HP Insight Management Agents v6.0 to v8.0
- The ruleset enhances call-out information by including c-class blade location information for managed devices running supported Linux operating systems. Previously OSEM 1.4.4 provided this functionality for Windows-based devices.
- The ruleset enhances part callout support for the HP ProLiant DL385-G2, the ProLiant DL580-G5 and the ProLiant DL585-G2 servers.
- The ruleset also enhances part callout support for the E200i, P800 and P700m raid controllers.
- Also included are SML videos for ProLiant G3 and G4 servers, as well as StorageWorks devices.
- Support in Insight Management Agents v8.1.1 for the following HP ProLiant server models:
 - HP ProLiant DL785 G5 server
 - HP ProLiant DL365 G5 server
 - HP ProLiant DL385 G5 server
 - HP ProLiant DL320 G5p server
 - HP ProLiant ML310 G5 server
 - HP ProLiant DL385 G5 server
 - HP ProLiant BL495c G5 server
- OSEM 1.4.7 includes updated analysis rules for the following HP ProLiant server models:
 - HP ProLiant DL785 G5 server
 - HP ProLiant BL2x220c G5 server
 - HP ProLiant BL260c G5 server
 - HP ProLiant BL465c G5 server
 - HP ProLiant DL585 G5 server

C.2 Integrity Support

Rules release supports the following HP Integrity servers running RedHat or SUSE IA-64 Linux:

- BL860c, rx1600, rx1620, rx2600, rx2620, rx2660, rx3600, rx4640, rx5760, rx6600, rx7620, rx7640, rx8620, rx8640
- HP Integrity Superdome with sx2000 chipset—16/32/64 Intel Itanium 2 processors
- HP Integrity Superdome with sx1000 chipset—16 processor/32 core server Intel Itanium 2 processor or mx2 dual-processor modules (32 CPUs)

- HP Integrity Superdome with sx1000 chipset—32 processor/64 core server Intel Itanium 2 processor or mx2 dual-processor modules (64 CPUs)
- HP Integrity Superdome with sx1000 chipset—64 processor/128 core server Intel Itanium 2 processor or mx2 dual-processor modules (128 CPUs)

For information on HP server systems and supported operating systems, go to:
<http://www.hp.com>

For information on Linux and to download Linux manageability SNMP agents, go to:
<http://www.hp.com/go/integritylinuxessentials>

- Support for the Ultrium 448c Tape Blade server

C.3 Switch and Tape Support

This release of OSEM has event rules for the following models of Fibre Channel switches and Directors:

- HP StorageWorks 2000 Modular Smart Array (MSA2000) series
- HP B-Series, HP C-Series & HP M-Series Fibre Channel Switches
- HP C-Series Fibre Channel Switches
- HP Enterprise Vaulting Service (EVS) Storage Disaster recovery service
- Brocade Fibre Channel Switches (up to Brocade Fabric Operating System (FOS) v5.3.0):
 - Brocade SilkWorm 1000 family (Type 1)
 - Brocade SilkWorm 2800 (16 port, 1 Gbit/sec) (Type 2)
 - Brocade SilkWorm 2400, 2100 (8 port, 1 Gbit/sec) (Type 3)
 - Brocade SilkWorm 2010, 2040, 2050 (20X0) (8 port, 1 Gbit/sec) (Type 4)
 - Brocade SilkWorm 2210, 2240, 2250 (22X0) (16 port, 1 Gbit/sec) (Type 5)
 - Brocade SilkWorm 2800 (16 port, 1 Gbit/sec) (Type 6)
 - Spider card (SilkWorm 2800) (Type 7)
 - Brocade SilkWorm 3800 (16 port, 1/2 Gbit/sec) (Type 9)
 - Brocade SilkWorm 12000 (64/128 port, 1/2 Gbit/sec) (Type 10)
 - Brocade SilkWorm 3900 (32 port, 1/2 Gbit/sec) (Type 12)
 - Brocade SilkWorm 3200 (8 port, 1/2 Gbit/sec) (Type 16)
 - HP StorageWorks SAN Switch 2/16-EL (16 port, 1/2Gbps based on 3600) (Type 17)
 - HP StorageWorks SAN Switch 2/8 (Bladerunner, SilkWorm 3000, in MSA1000, 1/2 Gbps) (Type 18)
 - Brocade SilkWorm 24000 (128 port, single domain director) (Type 21)
 - IBM Blade Center Switch Module 3016 (Blazer, 14/2 port, 1/2Gbit/sec, based on SW3900) (Type 22)
 - Brocade SilkWorm 3250 (8 port, 1/2 Gbit/sec) (Type 26)

Products Supported by OSEM

C.3 Switch and Tape Support

- Brocade SilkWorm 3850 (16 port, 1/2 Gbit/sec) (Type 27)
- HP Blade Center Switch Module 4012 (8/4 port, 1/2/4 Gbit/sec, based on SW4100) (Type 29)
- Brocade SilkWorm 4100 (32 port, 1/2/4 Gbit/sec) (Type 32)
- Dell Blade Center Switch Module 3014 (10/4 port, 1/2 Gbit/sec, based on SW3900) (Type 33)
- Brocade SilkWorm 200E (8/12/16 port, 1/2/4 Gbit/sec, based on SW4100) (Type 34)
- Brocade SilkWorm AP7420 (16 port) (Type 38)
- Brocade SilkWorm 48000 (256 port, 1/2/4 Gbit/sec, single Domain director, 16- or 32-ports blades) (Type 42)
- Brocade SilkWorm 24 port C-class Blade Switch module (Type 43)
- Brocade SilkWorm 4900 (4/64) (Type 44)
- Brocade SilkWorm 7500 (400 MPR) (Type 46)
- Brocade SilkWorm 5000 (4/32b) (Type 58)
- Brocade 8/24c SAN switch for BladeSystem c-Class
- HP DCX Director Switch support
- Cisco Fibre Channel switches (up to SAN-OS v3.2):
 - MDS 9506 (A7471A 2GB Director)
 - MDS 9509 (A7462A 2GB Director)
 - MDS 9513 (A????A Multilayer director)
 - MDS 9216 (A7473A 2GB Switch)
 - MDS 9140 (A7427A 2GB Switch)
 - MDS 9120 (A7426A 2GB Switch)
 - MDS 9020 (AE377A 4GB Fabric Switch from QLogic)
 - MDS 9216A (A7758A 2GB Switch)
 - MDS 9216i (A7557A 2GB Switch)
 - MDS 9132 (Old Cisco switch chassis)
 - MDS 9116 (Old Cisco switch chassis)
 - MDS 9124e (AG641A 4GB) C-Class Blade FC switch
 - MDS 9222i C-Class Blade switch 4/66
 - MDS 9134 C-Class Blade switch 4/32
- McData Fibre channel switches
 - All McData switches that are supported by EFCM v9.6 are supported in OSEM 1.4.5
- QLogic Fibre Channel switches
 - HP StorageWorks 8/20q FC Switch
- Virtual Connect Fibre Channel modules
 - HP 4Gb Virtual Connect Fibre Channel Module for c-Class
- HP Nearline Storage products (including Virtual Library Systems)

- HP StorageWorks Extended Tape Library Architecture (ETLA):
 - ESL and EML series Tape libraries
- VLS6000, VLS12000 series and VLS300 series Gateways
- HP 9000 Virtual Library System (VLS9000)
- HP M-Series FC switches are supported through EFCM v9.6 only
- MSL Tape Library support
 - MSL 2024
 - MSL 4048
 - MSL 8096
 - 1/8 G2 Tape Autoloader

C.4 Multivendor Support

- Dell PowerEdge server support

C.5 Storage Products

- HP StorageWorks 2000 Modular Smart Array (MSA2000) series
- HP SC08e HBA (LSI) SAS 8 external ports for MSA 2xxx

C.6 MSADB 1.52.90 Ruleset

The 1.52.90 ruleset includes:

- ProLiant
 - filtermap.cpq.xml version 1.52.90
 - cpq_snmpMsg.properties
- Fiber Channel Switches
 - filtermap.fcs.xml version 1.52.90
 - fcs_snmpMsg.properties
- HP Nearline Storage products
 - filtermap.nl.xml version 1.52.90
 - nl_snmpMsg.properties
- IBM X-series
 - filtermap.ibm.xml version 1.52.90
 - ibm_snmpMsg.properties
- Integrity Server
 - filtermap.ipf.xml version 1.52.90

Products Supported by OSEM

C.7 Additional OSEM Highlights

- ipf_snmpMsg.properties
- Individual service rev files

C.7 Additional OSEM Highlights

- OSEM status for No Location and Configuration - Business Unknown conditions
- OSEM Managed System Page system type dropdown for Network-Attached Storage (NAS)
- HP SIM 5.2.2 support addressing additional managed entity data fields (site country code, entered product number, customDeliveryId)
- Support for Modular Cooling System G2
- OSEM 1.4.7 offers updated Service Media Library links
- OSEM 1.4.7 includes enhanced hard drive service events to prevent noise events when a user removes a hard disk drive
- IM Agents v8.1.1 support
 - Red Hat Enterprise Linux 5.2
 - SUSE Linux Enterprise Server 10 SP2
 - Windows Small Business Server 2008

Glossary

A

ACHS

Automatic Call Handling System. Within the service provider's customer service center, ACHS accepts incoming event analysis messages that were initiated by [SICL](#).

agent

An agent is an event detection program residing on a managed system. For example, the IM agents generate SNMP traps that OSEM can receive and interpret.

automated notification

Automated notification lets customer managed systems self-report by automatically detecting and sending service event reports to specified email recipients or to remote service providers. See also [problem report](#).

Automatic Call Handling System

See [ACHS](#).

C

CADC

Crash Analysis Data Collector. On Windows systems, CADC is required before the system can collect operating system failure information and format it into a footprint that [CCAT](#) can then analyze. The Tru64 UNIX and OpenVMS operating systems come with built-in utilities that create such footprints.

CCAT

Computer Crash Analysis Tool. CCAT is a remote operating system failure analysis tool and is a [WEBES](#) component.

Glossary

D

Common Remote Support Module

See [CRSM](#).

Computer Crash Analysis Tool

See [CCAT](#).

Crash Analysis Data Collector

See [CADC](#).

CRSM

Common Remote Support Module. CRSM is the event-delivery application installed on the OSEM host. CRSM includes a browser-based GUI that allows a user to manage [automated notification](#) and individual problem reports.

customer service gateway

The PRS counterpart to the OSEM host.

D

DECEvent

A system event monitoring tool for HP Tru64 UNIX and HP OpenVMS systems. DECEvent is the predecessor of [SEA](#).

DESTA

Distributed Enterprise Service Tools Architecture. DESTA is the engineering code name for the [WEBES](#) software suite architecture. Consider any references to DESTA to be roughly synonymous with WEBES itself.

DHCP

Dynamic Host Configuration Protocol. DHCP is a protocol for automatic TCP/IP configuration that provides dynamic and static address allocation and management.

Distributed Enterprise Service Tools Architecture

See [DESTA](#).

downstream

Downstream describes the [automated notification](#) relationship between systems and the OSEM host. A managed system is downstream from the OSEM host. See also [upstream](#).

DSNLink

A service tool that allows two-way [SICL](#) communications between a customer system and a service provider system.

Dynamic Host Configuration Protocol

See [DHCP](#).

H

HP Systems Insight Manager

HP Systems Insight Manager is a web-based enterprise management application that lets users manage networked devices singly or in logical groups. When installed on the OSEM host, HP Insight Manager 5.1 receives SNMP traps from IM agents, creates problem reports, and forwards those problem reports as part of [automated notification](#).

HTTP

Hypertext Transfer Protocol. HTTP is the protocol used by web servers and client browsers to move web content over a network. HTTP is one of the two protocols that OSEM can use to communicate with managed systems. The other is [SNMP](#).

Hypertext Transfer Protocol

See [HTTP](#).

I

Instant Support Enterprise Edition

See [ISEE](#).

Intel based

In this document, Intel based refers to the industry standard x86 processor architecture available originally from Intel and, subsequently, from other manufacturers. The Pentium family of chips are examples of Intel based processors.

ISEE

Instant Support Enterprise Edition. HP ISEE automates remote support over the Internet by using electronic notifications similar to those from [SICL](#) or PRS. ISEE also includes remote diagnostic scripts to analyze supported systems and devices.

Glossary

M

ISEE Client

The portion of the ISEE application that must be installed on any system that will participate in [automated notification](#) to HP. When used with [OSEM](#), one ISEE Client can send notifications for multiple systems.

M

managed system

A managed system is a customer computing system that is being monitored and serviced. Managed systems generate problem reports that get transmitted to the OSEM host, which in turn sends the reports as [automated notification](#) messages.

Management and Service Access Database

See [MSADB](#).

MIB Rev files

Files used to update a Management Information Base (MIB). In general, a MIB is a collection of managed objects and their attributes, such as the object's names, their permissible behavior, and the operations that can be performed on them. The MIB Rev files provided with CRSM contain the rules used by Insight Manager to do first-level filtering of SNMP traps.

MSADB

Management and Service Access Database. The MSADB is a set of database files containing filter criteria and related information used to determine which system events should trigger problem reports. There are no MSADB files on managed systems that do not contain CRSM, so problem reports or SNMP traps sent from these systems to the OSEM host are not filtered. MSADB filtering is applied on the OSEM host before the problem reports are sent to the email recipients.

O

Open Service Event Manager

See [OSEM](#).

OSEM

Open Service Event Manager. OSEM collects and formats problem reports from assorted customer systems, and allows those systems to send [automated notification](#) messages to local email recipients or to HP through [ISEE](#).

OSEM host

The OSEM host acts as a gateway for managed systems to connect with the outside world. Events from the managed systems are accumulated to a single OSEM host, formatted, and forwarded onward as [automated notification](#) reports.

P

problem report

Strictly speaking, a problem report may not always indicate a hard failure. Instead, problem report in the context of OSEM is a generic term that describes any serviceable event reported. Problem reports are viewable in the web browser. They sometimes also may be referred to as dial-outs or incident reports.

Q

QSAP

Qualified Service Access Point. QSAP is an older name for the OSEM host.

Qualified Service Access Point

See [QSAP](#).

R

RCM

Revision and Configuration Management. In versions prior to [WEBES 4.2](#), RCM was a WEBES component that collected configuration, revision, and patch data from supported systems.

Revision and Configuration Management

See [RCM](#).

S

SEA

System Event Analyzer. SEA is a remote system event monitoring tool and is a [WEBES](#) component.

Glossary

T

SICL

System Initiated Call Logging. SICL uses [DSNLink](#) to send fault and failure messages to the service provider's customer service center. The messages are then received by [ACHS](#), analyzed, and acted upon as appropriate. The follow-up service offering to SICL is PRS.

Simple Mail Transfer Protocol

See [SMTP](#).

Simple Network Management Protocol

See [SNMP](#).

SMTP

Simple Mail Transfer Protocol. SMTP is a TCP/IP protocol governing email transmission and reception.

SNMP

Simple Network Management Protocol. Although not limited to TCP/IP, SNMP is widely deployed in TCP/IP networks. SNMP operates on top of the Internet Protocol (IP) and is a management architecture designed to meet the needs of the average network. SNMP is one of the two protocols that OSEM can use to communicate with managed systems. The other is [HTTP](#).

System Event Analyzer

See [SEA](#).

System Initiated Call Logging

See [SICL](#).

T

TCP/IP

Transmission Control Protocol/Internet Protocol. TCP/IP provides communication between computers across interconnected networks, even when the computers have different hardware architectures and operating systems.

Transmission Control Protocol/Internet Protocol

See [TCP/IP](#).

U

upstream

Upstream describes the [automated notification](#) relationship between systems and the OSEM host. The OSEM host is upstream from its managed systems. In turn, the [ISEE Client](#) is upstream from the OSEM host when remote automated notifications are sent to the service provider. See also [downstream](#).

W

WCC

WEBES Common Components. The WCC are required portions of WEBES that allow the tool suite to function as an integrated installation. The WCC are separate from the individual tools in the WEBES suite ([SEA](#) and [CCAT](#)) and are almost always transparent to the user. See also [WCCProxy](#).

WCCProxy

Like the [WCC](#), the WCCProxy is another required part of WEBES. (The WCCProxy also is a required part of the [ISEE Client](#).) After WEBES installation, the WCCProxy appears as a separately installed kit and represents WEBES functionality not developed in the Java™ environment. The WCCProxy contains functions that allow WEBES to interact properly with the operating system.

Web-Based Enterprise Services

See [WEBES](#).

WEBES

Web-Based Enterprise Services. WEBES is an integrated set of web-enabled service tools that includes the System Event Analyzer ([SEA](#)) and Computer Crash Analysis Tool ([CCAT](#)), as well as the required components [WCC](#) and [WCCProxy](#). See also [DESTA](#).

WEBES Common Components

See [WCC](#).

WorldWire

A service tool that allows for secure two-way PRS communication between a customer system and a service provider system.

