

# **HP Instant Support Enterprise Edition SPOP Users' Guide**



**Manufacturing Part Number: 5991-0762**  
**March, 2005**

**A.03.90**

© Copyright 2003 - 2005 Hewlett-Packard Development Company, L.P.

---

## Legal Notices

This document contains information that is protected by copyright. All rights are reserved. Reproduction, adaptation, or translation without prior written permission is prohibited, except as allowed under the copyright laws.

The information contained in this document is subject to change without notice.

### Copyright Notices

HP Instant Support Enterprise Edition (ISEE) is an HP-owned and operated technology supporting servers, Mission Critical Proactive Services, Solaris, storage, networking, and digital press devices as covered by Hewlett-Packard hardware or software support agreements.

Copyright © Hewlett-Packard Development Company, L.P. 2003-2005

### Trademark Notices

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

Java™ is a trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape and HP.

Microsoft® Windows, NT®, and Internet Explorer are registered trademarks of Microsoft Corp.

Motive™ is a registered trademark of Motive Communications, Inc.

Netscape is a registered trademark of Netscape Communications Corporation.

Pentium® is a U.S. registered trademark of Intel Corporation.

Symantec® is a registered trademark of Symantec Corporation.

Spirian® is a registered trademark of Spirian Technologies, Inc.

*Hewlett-Packard makes no warranty of any kind with regard to this manual, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.*

## **Revision History**

July 2003	Edition ISEE A.03.00
March 2004	Edition ISEE A.03.50
April 2004	Revision ISEE A.03.50
March 2005	Edition ISEE A.03.90

New editions are complete revisions of the manual, incorporating extensive technical changes. Intermediate revisions include minor corrections and updates and do not change the edition number.

Provided by:

HEWLETT-PACKARD COMPANY  
3404 E. Harmony Road  
Fort Collins, CO 80528  
U.S.A.

---

## Conventions

The typeface conventions used within this document follow:

**Body Text:** NewCenturySchlbk 10 pt is used as the main body text in this document.

*Emphasis:* Italicized NewCenturySchlbk 10 pt is used to indicate words that are emphasized and *document\_names*.

*Italics:* Italicized Courier New 10 pt is used to indicate *<variable\_information>* the user must enter and *[Soft Buttons]*.

**ComputerOutput:** Courier New 10 pt indicates text output from a computer, text, soft buttons, or user interface.

**[Button]:** Courier New 10 pt indicates the use of a keyboard button (**[Hard Buttons]**).

**UserInput:** Bold Courier New 10 pt indicates text the user must enter into the system. Italicized words within the text indicate *<variable\_information>*.

**http or https://...:** Bold Courier New 10 pt indicates Web addresses (URLs).

---

## HP ISEE Documentation

HP ISEE documentation includes the following:

*Client Installation Guide* (part number 5991-0761)

This installation and configuration guide, used by a customer or customer's HP support engineer, provides instructions for acquiring the HP ISEE software from the HP software distribution portal. It is used for installing and configuring the software for the Monitored Clients. This guide is available at:

<http://www.hp.com/learn/isee>.

*SPOP User Guide* (part number 5991-0762)

This SPOP guide, used by a customer or customer's HP support engineer, provides instructions for using the Enterprise Service Console on the SPOP. This guide is available at:

<http://www.hp.com/learn/isee>.

*HP Instant Support Enterprise Edition Remote Connectivity Implementation Guide* (part number 5990-7254)

The HP Instant Support Enterprise Edition Remote Connectivity Implementation Guide is used by HP Support Engineers to deploy and configure the Cisco Remote Connectivity solution, including the Customer Access System, at the customer's site. It is also used by customers to control access in their networks. This guide will be available upon product release at:

<http://www.hp.com/learn/isee>.



**1. Understanding ISEE and the SPOP**

Using this Guide .....	10
Understanding ISEE .....	11
Understanding Scheduled Collections .....	11
Understanding the SPOP .....	13

**2. Understanding the Enterprise Service Console Utilities**

Understanding the Enterprise Service Console .....	16
Understanding the Enterprise View Features .....	17
Understanding Incident Management .....	17
Understanding Contact and User Management .....	18
Understanding Company Contact Information Management .....	19
Understanding Password Management .....	19
Understanding Device Management .....	19
Understanding Device Group Management .....	20
Understanding the Scheduler .....	21
Understanding when to Schedule Collections .....	22
Understanding when to View Scheduler Results .....	22
Understanding when to Alter a Schedule .....	22
Understanding the Servers and Status Utility .....	23
Understanding when to Change E-mail Notification for Client Polling Failure .....	23
Understanding when to Change your SMTP Mail Server .....	23
Understanding HP Tools .....	24
Understanding Content Version Management .....	24
Understanding Unreachable Device Notification .....	24

**3. Using the Enterprise Service Console**

Using the Enterprise Service Console .....	26
Using the Enterprise View .....	27
Viewing Open Incidents in the Enterprise View .....	28
Viewing Closed Incidents in the Enterprise View .....	29
Managing Contacts and Users in the Enterprise View .....	30
Managing Company Contact Information in the Enterprise View .....	33
Changing the Default Administrator Password in the Enterprise View .....	34
Managing Devices in the Enterprise View .....	36
Managing Device Groups in the Enterprise View .....	40
Using the Scheduler .....	42
Scheduling Collections in the Enterprise Service Console .....	43
Viewing Scheduler Results .....	47
Altering a Scheduled Collection .....	49
Using Servers & Status .....	51
Changing E-mail Notification for Failed Client Polling .....	51
Changing your SMTP Mail Server .....	53
Disabling Notifications to Your SMTP Mail Server .....	55
Using HP Tools: Managing Content Versions .....	57
Downloading New Content Bundles .....	57

---

# Contents

Managing Content Web Targets. . . . .	58
Using HP Tools: Unreachable Device Notification . . . . .	60
Accessing the Unreachable Device Notification Application . . . . .	60
Enabling the Device Unreachable Monitoring Service. . . . .	61
Managing Devices. . . . .	61
Configuring Device Monitoring Features . . . . .	63
Managing Maintenance Windows . . . . .	64
Managing the E-mail Notification Address List . . . . .	65
Managing Global Default Settings . . . . .	66
Managing Device Settings . . . . .	67

## 4. Using Software Management

Anti-Virus Protection on the SPOP. . . . .	70
Virus Protection Process. . . . .	70
Symantec LiveUpdate Options. . . . .	70
Updating Symantec Anti Virus Definitions . . . . .	71
Troubleshooting. . . . .	73
Enabling and Scheduling Symantec LiveUpdate . . . . .	73
Security Patching Process . . . . .	76
Controlling Automatic Downloads with the Software Management Application . . . . .	77

## Glossary



---

# **1            Understanding ISEE and the SPOP**

## Using this Guide

This document covers SPOP processes such as monitoring the Enterprise, managing scheduled collections, and using the Software Management Application. These features are addressed in the subsequent chapters. Please read the following to better understand how this guide is structured.

- Chapter 1, “Understanding ISEE and the SPOP,” on page 9, introduces ISEE Support, the Advanced Configuration, and the Support Point of Presence (SPOP).
- Chapter 2, “Understanding the Enterprise Service Console Utilities,” on page 15, provides context for the Enterprise Service Console features. It explains the Enterprise Service Console (ESC) utilities and use models and references corresponding tasks in Chapter 3. This chapter enables *learning* about the Enterprise Service Console.
- Chapter 3, “Using the Enterprise Service Console,” on page 25, details Enterprise Service Console (ESC) tasks. This chapter provides directions for completing routine tasks in the ESC based on the context in Chapter 2. This chapter enables *usage* of the Enterprise Service Console.
- Chapter 4, “Using Software Management,” on page 69, covers the Software Management application. Software Management updates Symantec Antivirus definitions and select HP software on the SPOP. This chapter explains how the Software Management applications works and outlines the processes necessary to acknowledge and accept software updates.

## Understanding ISEE

HP Instant Support Enterprise Edition (ISEE) integrates proven, secure, remote solutions for IT environments covered by support agreements. HP ISEE is available in Standard and Advanced configurations. In both configurations supported devices are monitored with HP ISEE Client software. The client software is also installed by default on the SPOP so that it can be monitored for hardware events and failure.

The ISEE Standard Configuration provides remote monitoring and data collection. In the Standard Configuration Monitored Clients report directly to the HP Support Center. The Standard Configuration does not include an SPOP.

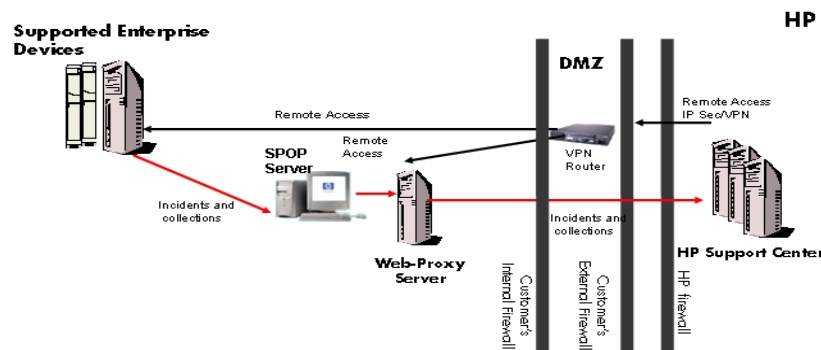
The ISEE Advanced Configuration provides remote monitoring and data collection, centralized enterprise incident viewing, and remote support. In the Advanced Configuration Monitored Clients report events and system collections to a Support Point of Presence (SPOP), and the SPOP reports to the HP Support Center. The SPOP enables the customer to manage enterprise information from a central location.

The Advanced Configuration also includes remote connectivity through a VPN router for trouble shooting customer enterprises. For more information on ISEE Remote Connectivity features and capabilities see the *HP Instant Support Enterprise Edition Remote Connectivity Implementation Guide*.

**NOTE**

Figure 1-1 provides an overview of the Advanced Configuration, including the flow of data across firewalls.

**Figure 1-1 The Advanced Configuration Implementation**



## Understanding Scheduled Collections

Scheduling configuration collections enables HP to provide more robust troubleshooting and support. Scheduled collections provide data that your HP support engineer can access to run Contract Compare assessments for you. Contract Compare Assessments are done inside of HP and ensure that HP customers receive the support levels they have purchased. Additionally, Contract Compare assessments offer an organized and accurate

**Understanding ISEE**

overview of customer contracts and simplifies the contract management process. For the ISEE A.03.90 release, scheduled collections are supported on HP-UX, Linux, and Windows operating systems.

After completing the initial ISEE configuration for your Advanced Configuration ISEE client as described in the *Instant Support Enterprise Edition Client Installation and Upgrade Guide*, you can schedule system configuration collections by completing “Using the Scheduler” on page 42.

---

**NOTE**

The first scheduled collection must run before a Contract Compare assessment can be run. If your scheduled collection runs on a Monday at 10:00 PM, for instance, the assessment cannot be run until the first collection is complete.

---

---

## Understanding the SPOP

The ISEE SPOP provides the following features:

- Centralized management of the enterprise through a consolidated view of HP ISEE incidents, control over device, contact, and scheduled collection information, and notification of the status of Monitored Clients from the Enterprise Service Console.
- Remote software management for efficient distribution of ISEE software and antivirus definition updates.
- Select Mission Critical features such as Network Support and Storage services for customers, based on the their support agreements.

---

### NOTE

These Mission Critical features are implemented and supported by your HP Support Engineers.

---

Due to the complexity of software licensing, the SPOP is HP-owned. However, the SPOP is deployed to the customer site and enables centralized management of ISEE support. The HP ISEE SPOP is installed and, when necessary, upgraded by your HP Support Engineer. You can add ISEE Monitored Clients at any time, but the deployment of the SPOP is coordinated by HP.

The SPOP functions as an ISEE Monitored Client and can function as a central client to handle submission of incidents from other ISEE Monitored Clients. To better understand the functionality and use models of ISEE Monitored Clients, please reference the *Instant Support Enterprise Edition Client Installation and Configuration Guide*.

---

### NOTE

For a complete list of ISEE-supported operating systems and hardware devices, please view the ISEE supported products web page at:

[http://www.hp.com/hps/hardware/hw\\_products.html](http://www.hp.com/hps/hardware/hw_products.html).



---

## **2      Understanding the Enterprise Service Console Utilities**

## Understanding the Enterprise Service Console

The Enterprise Service Console (ESC) is a Web-based user interface on the Support Point of Presence (SPOP). The ESC enables centralized enterprise management, scheduled collections, and Device Unreachable Notification. The ESC is used to manage your Enterprise information and preferences.

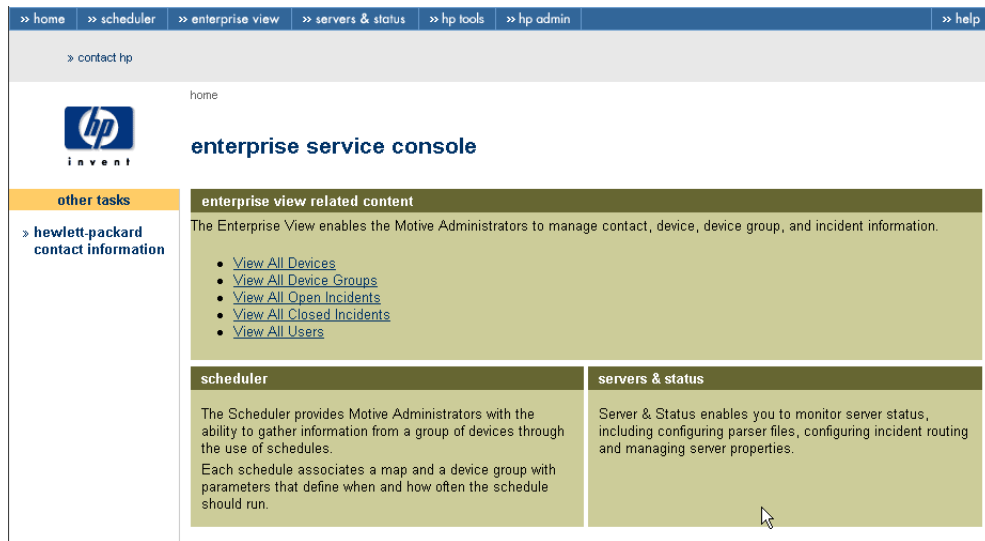
ISEE Enterprise Service Console requires Microsoft Internet Explorer 5.0+. If a customer-provided system connects to the SPOP using Terminal Services, the customer-provided system must run Windows 2000 or greater, or the customer must obtain a Terminal Services Client license for that machine. HP does not provide Terminal Services licenses to customers.

The Enterprise Service Console includes the following utilities:

- Enterprise View
- Scheduler
- Servers & Status
- HP Tools

Each of these utilities enables functional control over an ISEE component. Reference the following sections to better understand why and when to use each feature of the Enterprise Service Console. Each section in this chapter has a corresponding usage section in Chapter 3 that details the steps required for the specified tasks.

**Figure 2-1** The Enterprise Service Console





## Understanding the Enterprise View Features

The Enterprise View enables centralized management of incident information, contacts, users, devices, and device groups. The following subsections correspond to tasks outlined in Chapter 3 under the section “Using the Enterprise View” on page 27. Read the “When” explanations to understand the circumstances for completing the task. Then, complete the steps referenced in the corresponding “How” section for the specified task.

### Understanding Incident Management

All incidents submitted by your ISEE Monitored Clients are managed by the SPOP. With the Enterprise View, you can view open incidents to determine whether or not the incident was actionable, who was assigned to work on an incident, and what device submitted incidents.

When viewing incidents, you can sort by any of the following attributes:

- `incident ID` (the numerical identifier of each incident)
- `wfm ID` (the identifier assigned to an incident when the ISEE Support center has deemed it actionable)
- `opened` (the date the incident was logged by the SPOP database)
- `device name` (the name of the ISEE Monitored Client that submitted the incident from inside of your enterprise)
- `status` (either open or closed)
- `queue` (the type of operating system running on the Monitored Client)
- `problem area` (the type of data addressed by the incident; similar to description)
- `description` (the type of incident that was submitted)

### Understanding when to View Open Incidents

**When:** The following are examples in which you would review open incidents:

- To verify that new installation and entitlement incidents were received after installing your ISEE Monitored Clients. To do this, you can sort by `device name` to group incidents submitted from the newly installed ISEE Monitored Client, or you can sort by `description` to group a particular type of incident, such as entitlement incidents.
- To review all open incidents submitted from a specific Monitored Client. To do this, you can sort by `device name` to group incidents submitted by a specific device. Then you can compare the volume and frequency of incident submissions from a particular Monitored Client.
- To review incidents submitted from a specific operating system type. To do this you can sort by `queue` and compare the volume and frequency of incidents from a specific operating system type in your enterprise.
- To monitor incident volume in general. To do this you can simply review the quantity of incidents in the Enterprise View.

**How:** To view open incidents reference “Viewing Open Incidents in the Enterprise View” on page 28.

**Understanding when to View Closed Incidents** Closed incidents are purged from the SPOP database after 180 days.

**When:** You would view closed incidents if you have a recurring problem with a specific ISEE Monitored Client and want to view the incident history of that client. You can do this by sorting by `device name` to group incidents submitted by an individual Monitored Client.

**How:** To view closed incidents reference “Viewing Closed Incidents in the Enterprise View” on page 29.

### Understanding Contact and User Management

This feature enables you to create individual device contacts for your professionals dedicated to the support of a specific ISEE Monitored Client. Creating device contacts enables HP to inform your designated contact(s) of incident status for specific ISEE monitored devices. Contacts are associated with devices, so when following up on incidents associated with a device, you can identify the contact(s) responsible for that device.

There are two types of SPOP users:

1. A contact is a customer representative designated to be contacted by HP in case of a problem with a specific ISEE Monitored Client.
2. A user is a contact who also has an SPOP administrative account.

User roles are a collection of privileges associated with an HP ISEE account. Privileges represent an HP ISEE operation. Privileges define what support Analysts and engineers can view and access.

The following roles are available when creating a contact:

**Table 2-1**

#### SPOP Account Roles

Role	Privileges
Operator	Allows Server Management from the Enterprise Service Console.
Administrator	Allows User Management from the Enterprise Service Console.
Support Manager	Provides unlimited support privileges.
Senior Support Analyst	Provides broad support privileges.
Support Analyst	Allows limited support privileges.

To create an administrative account, select the Administrator, Support Manager, and Operator roles.

**When:** You manage contacts and users in the Enterprise View to reflect a change of employment in your company. For example, if an employee leaves or is terminated, his/her account is deleted. Likewise, if a new employee is hired, an account is created. If an employee assumes additional responsibilities or changes his/her hours of availability, his/her account can be updated to reflect those changes. Passwords are also managed with this functionality.

**How:** To Manage Contacts reference “Managing Contacts and Users in the Enterprise View” on page 30.

### Understanding Company Contact Information Management

Your Company Contact information is unlikely to change. However, the SPOP enables updates as necessary. This information is associated with incidents submitted by the SPOP.

**When:** You would manage your company contacts information in the Enterprise View to reflect a change of your primary company contact. Additionally, if you experience a corporate name change, change in location, or change of phone number, that information is updated in your company contacts.

**How:** To Manage Company Contact information reference “Managing Company Contact Information in the Enterprise View” on page 33.

---

#### NOTE

If you need to change the default contact for e-mail notification, please reference “Changing E-mail Notification for Failed Client Polling” on page 51.

---

### Understanding Password Management

All ISEE SPOPs are issued the same default administrative password for the Enterprise Service Console. For your own security, it is strongly advised that you customize your password.

The characteristics of a secure password include seven or more characters comprised of alpha and numeric characters, upper and lower case characters, and special characters (non alphanumeric, such as punctuation marks) and should not include dictionary words or simple combinations of such words.

**When:** Your HP Support Engineer requests a new password from you before the SPOP is installed. However, if you choose to change the password yourself, or if you choose to change it again later, you can do so in the Enterprise Service Console.

**How:** To Manage Company Contact information reference “Managing Company Contact Information in the Enterprise View” on page 33.

### Understanding Device Management

The Enterprise View enables you to edit device details, assign contacts, and add device notes for your ISEE Monitored Clients. These features provide more context and improved support of incidents submitted from your Monitored clients.

**When:** The following are examples in which you would manage devices:

- To add or remove a contact for a specific Monitored Client. For example, if a different employee is now responsible for a Monitored Client, you can change the contact for that client.
- To modify or correct the details associated with a Monitored Client. For example, if you relocate a Monitored Client, you can modify the location information in the device details. This provides more accurate details about incidents submitted from that device.
- To add or edit device notes that are associated with incidents submitted by a specific Monitored Client. This feature enables you to enter relevant information through a free text field.

**How:** To Manage Device information reference “Managing Devices in the Enterprise View” on page 36.

### **Understanding Device Group Management**

Device Groups are required to configure Scheduled Collections. You must create device groups before you can schedule configuration collections for your ISEE Monitored Clients. Whenever you add a new ISEE Monitored Client, you must add it to a Device Group to enable scheduled collections for the new device. The same ISEE Monitored Client can be added to multiple device groups.

**When:** The following are examples in which you would manage Device Groups:

- To add a Monitored Client to a device group. For example, if you install a new ISEE Monitored client, you can add it to a device group to enable scheduled collections. To do this you would edit an existing device group and choose the new Monitored Client from the list of available devices and add it to the selected device group.
- To add or remove a Monitored Client from a device group. For example, if you want to stop scheduled collections on a specific monitored client, you would remove it from its device group. To do this you would edit an existing device group and remove the specific Monitored Client from that device group.
- To create or edit a device group to address specific needs in your enterprise. To do this you would add a new group or edit an existing group and customize your options as you create/edit the group.
- To delete a device group that you no longer want or need.

**How:** To Manage Device Groups reference “Managing Device Groups in the Enterprise View” on page 40.

## Understanding the Scheduler

The Scheduler utility in the Enterprise Service Console enables scheduled collections of configuration information from your Enterprise. Scheduling configuration collections enables HP to provide more robust troubleshooting and support practices. Scheduled collections are supported on HP-UX, Linux, and Windows operating systems. By default system collections are not enabled during the installation of ISEE Monitored Clients.

The scheduler in the Enterprise Service Console gathers information from a preselected group of devices. Each schedule associates a MAP and a device group with parameters that define when and how often the schedule will run. Only one MAP can be assigned to each scheduled collection. Scheduled collections are sent to the HP Support Center for faster troubleshooting.

Device Groups must be created before collections can be scheduled; for more information about device groups see “Understanding Device Group Management” on page 20. When scheduling a collection, verify that the MAP selected corresponds appropriately with the attributes of the Device Group. For example, you could not run a Windows Comprehensive System Information MAP against a device group comprised of HP-UX systems.

HP recommends scheduling your configuration collections at a time that will not conflict with peak system usage, regularly scheduled business processes, or other scheduled maintenance tasks.

The following scheduled collections are currently available. New MAPs are occasionally available. For more information about how new MAPs/Content are deployed, see “Understanding Content Version Management” on page 24. For more information about a specific MAP, please use the online MAP Browser at:

<http://isee.<region>.hp.com/isee/MapScriptsBrowser/index.html>

Regions include: europe, americas, and asiapac

---

### NOTE

The scheduled collections may require 15 minutes or more to complete on each scheduled system.

- **Additional HP-UX Comprehensive Information MAP:** This is an HP-UX comprehensive MAP. It runs five HP-UX diagnostic MAPs.
- **Comprehensive HP-UX System Information MAP:** This is an HP-UX comprehensive MAP. It runs eight HP-UX diagnostic MAPs (for example: GeneralSystemInfo).
- **Linux Comprehensive System Information MAP:** This is a comprehensive MAP. It runs eight Linux diagnostic MAPs (or example: LinuxHardwareInformation, LinuxGeneralSystemInfo).
- **Solaris Comprehensive System Information MAP:** This is a comprehensive MAP. It runs eight Solaris diagnostic MAPs.
- **Windows Comprehensive System Information MAP:** This is a comprehensive MAP. It runs eight Windows diagnostic MAPs (WindowsGeneralSystemInfo, etc.).
- **WinGetConfig Comprehensive System Information MAP:** This is a comprehensive MAP. It collects diagnostic information on the Windows client. Requires GetConfig installation on client.

### Understanding when to Schedule Collections

**When:** You would create a new collection schedule for a new device group or to run multiple scheduled collections on the same device group. You would also change a collection schedule if your business requirements dictate running the collections during a different time or interval.

**How:** To Schedule Collections reference “Scheduling Collections in the Enterprise Service Console” on page 43.

### Understanding when to View Scheduler Results

**When:** You would view scheduler results when you want to compare collection information gathered at different time periods an/or from different devices. You can use this information to compare and view system configuration information and to see what type of information is being collected from your systems.

---

**NOTE**

Scheduled system collection data is purged from the SPOP database after 180 days.

**How:** To view scheduler results reference “Viewing Scheduler Results” on page 47.

### Understanding when to Alter a Schedule

**When:** You would change suspend a schedule for maintenance on a system and resume the schedule when the maintenance tasks are complete. You would delete a schedule when it is superseded by another schedule or no longer needed.

**How:** To alter a schedule reference “Altering a Scheduled Collection” on page 49.

## **Understanding the Servers and Status Utility**

The Servers and Status option in the Enterprise Service Console enables you to configure notifications for Client Polling failures and to customize your SMTP server. Client Polling occurs between the SPOP and your ISEE Monitored Clients. If one or more of your Monitored Clients fails to communicate with the SPOP during the polling interval, the SPOP will generate a notification and send it to the person(s) designated to be notified of polling failures.

### **Understanding when to Change E-mail Notification for Client Polling Failure**

While it would be rare for you to need to change the notification for polling failures, this situation would arise due to staff changes. You would change notifications to be sent to the person responsible to act if clients fail to communicate regularly with the SPOP.

To change E-mail notifications see “Changing E-mail Notification for Failed Client Polling” on page 51.

### **Understanding when to Change your SMTP Mail Server**

Changes to your SMTP mail server would facilitate the need to change the listing in the Enterprise Service Console. The correct SMTP information allows notifications regarding requests to run MAPs, status of closed incidents, and if the client polling fails.

To change E-mail notifications see “Changing your SMTP Mail Server” on page 53. To disable all notifications through the SMTP server see “Disabling Notifications to Your SMTP Mail Server” on page 55.

## Understanding HP Tools

HP Tools enable content version management and Unreachable Device Notification.

### Understanding Content Version Management

Periodically, new HP ISEE software content is developed and released by HP. This content is published to an HP repository. Your ISEE SPOP polls this repository for updates. There are three supported web targets on the SPOP to store and manage this content. These web targets are the source of MAPs used by scheduled collections.

**Default:** This web target always contains the latest available MAPs on the SPOP. Reactive MAP executions requested by HP support engineers use this default repository.

**SDC\_test:** The customer uses this web target to verify the content bundle on test systems before allowing MAPs to be run on production servers. Customers promote content bundles to this web target.

**SDC\_production:** This web target is used for scheduled data collections on production servers. Customers promote content bundles to this repository if they have validated the bundle and trust its content.

When new content becomes available, you will be notified. To manage content on the SPOP check the `Content Version Management` feature of the Enterprise Service Console see “Using HP Tools: Managing Content Versions” on page 57.

### Understanding Unreachable Device Notification

Unreachable Device Notification performs reachability monitoring of HP customers’ devices in the ISEE Advanced Configuration and provides notifications of unreachable systems to HP Support Center and appropriate personnel at the customer site.

To change E-mail notifications see “Using HP Tools: Unreachable Device Notification” on page 60.



---

## **3 Using the Enterprise Service Console**

## Using the Enterprise Service Console

If you are unfamiliar with the Enterprise Service Console, please see “Understanding the Enterprise Service Console” on page 16.

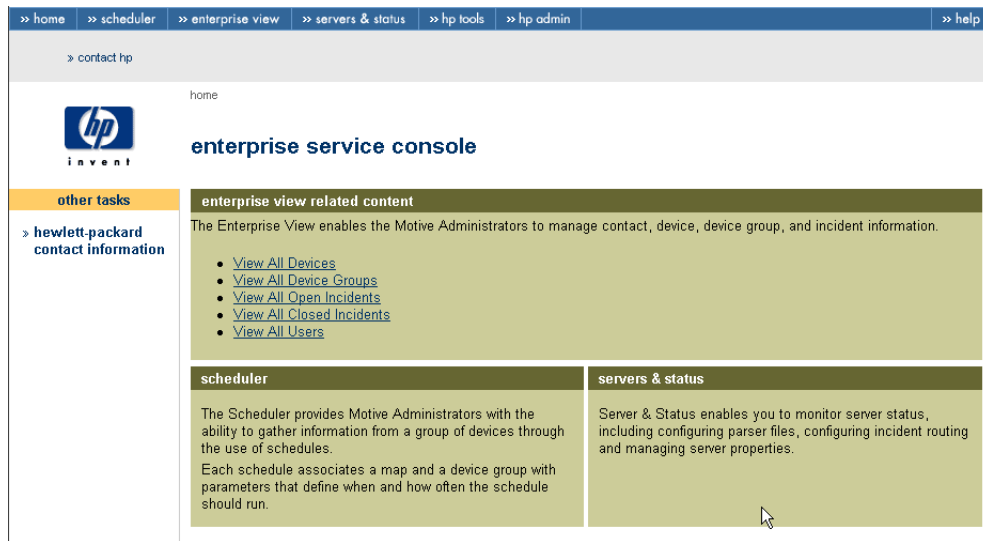
1. Choose the appropriate method, based on your Enterprise configuration, to access the Enterprise Service Console.

- If you are working directly on the SPOP system, start the Enterprise Service Console by double clicking the Enterprise Service Console Icon on the SPOP desktop.
- If you are accessing the SPOP remotely, access the Enterprise Service Console through Microsoft Internet Explorer 5.0+ at the following URL:

`https://<spop_hostname>:8080/console/`

Where *<spop\_hostname>* is the fully qualified name of the SPOP.

**Figure 3-1 Starting the Enterprise Service Console**



2. Enter your user name and password.

### NOTE

For directions on changing your password see “Changing the Default Administrator Password in the Enterprise View” on page 34.

If you forgot your password, contact your HP Support Representative for assistance.

## Using the Enterprise View

If you are unfamiliar with the Enterprise View, please see “Understanding the Enterprise View Features” on page 17

To access the Enterprise View:

1. Select `enterprise view` in the horizontal blue navigation bar at the top of the Enterprise Service Console page (see Figure 3-2).

**Figure 3-2** Enterprise View



## Viewing Open Incidents in the Enterprise View

If you are unfamiliar with the incident management, please see “Understanding Incident Management” on page 17.

To view open incidents reported by your ISEE monitored systems:

1. Select `enterprise view` in the horizontal blue navigation bar.
2. Select `view open incidents` from the left navigation list, (see Figure 3-2).
3. Click the appropriate incident under the `incident_id` heading to access a specific incident (see Figure 3-3).

**Figure 3-3** View Open Incidents

incident_id	wfm_id	opened	device_name	status	queue	problem_area	description
Incident 41		1 30 2004, 9:00	example	open	Win2000	New_Installation	New_Installation
Incident 42		1 30 2004, 12:36	example	open	Win2000	New_Installation	New_Installation
Incident 43		1 30 2004, 12:36	example	open	Win2000	Entitlement_Check	Entitlement_Check
Incident 44		1 30 2004, 12:36	example	open	Win2000	TEST incident	cpqHo2GenericTrap

The review this incident screen (Figure 3-4) displays incident status.

**Figure 3-4** Review This Incident

**incident details**

id	44
external key	
problem area	TEST incident
description	cpqHo2GenericTrap
opened	12:36 (MST)
status	open

**messages needing attention**

type	sent date	sender
Or, <a href="#">view all messages.</a>		

**device and contact details**

device name	example
ip address	15.6.37.93
endpoint	Example;37a2b8c5401a7ef6000ec540
contact	<a href="#">example contact</a>

**analyst details**

analyst name	<a href="#">HP Guest</a>
email	example email

**telemetry details**

collection date	map results	attachments
1 30 2004, 12:36	583464684.5@Example0/motive.mf	s2qc.7.txt

## Viewing Closed Incidents in the Enterprise View

If you are unfamiliar with the incident management, please see “Understanding Incident Management” on page 17.

To view closed incidents reported by your ISEE monitored systems:

1. Select enterprise view in the horizontal blue navigation bar.
2. Select view closed incidents from the left navigation list (see Figure 3-5).
3. Click the incident number under the incident\_id heading to access a specific incident (see Figure 3-5).

**Figure 3-5** View Closed Incidents

The screenshot shows the HP Enterprise View interface. At the top, there is a navigation bar with links: >> home, >> scheduler, >> enterprise view, >> servers & status, >> hp tools, >> hp admin, and >> help. Below the navigation bar, there is a breadcrumb trail: > contact hp. The main content area features the HP logo and the text "view closed incidents". A table lists several incidents with columns: incident\_id, wfm id, closed, device name, status, queue, problem area, and description. The table contains four rows of incident data. On the left side, there is a sidebar menu with "enterprise view" selected, and other options like "hewlett-packard contact information", "review company details", "view all devices", "view all device groups", "view open incidents", "view closed incidents", and "view all users". At the bottom, there are links for "privacy statement", "using this site means you accept its terms", and "feedback to webmaster".

incident_id	wfm id	closed	device name	status	queue	problem area	description
Incident 24	1 30 2004, 9:00	example	closed confirmed	Win2000	ISEE_Connectivity	ISEE_Connectivity	
Incident 29	1 30 2004, 9:00	example	closed confirmed	Win2000	Entitlement_Check	Entitlement_Check	
Incident 36	1 30 2004, 12:14	example	closed confirmed	Win2000	ISEE_Connectivity	ISEE_Connectivity	
Incident 39	1 30 2004, 12:18	example	closed confirmed	Win2000	Entitlement_Check	Entitlement_Check	

The review this incident screen (Figure 3-6) displays closed incident status.

**Figure 3-6** Review This Incident

The screenshot shows the HP Enterprise View interface for reviewing a specific incident. At the top, there is a navigation bar with links: >> home, >> scheduler, >> enterprise view, >> servers & status, >> hp tools, >> hp admin, and >> help. Below the navigation bar, there is a breadcrumb trail: > contact hp. The main content area features the HP logo and the text "review this incident". The incident details are displayed in a structured format, including fields for id, external key, problem area, description, opened, and status. Below the incident details, there is a section for "messages needing attention" with a table showing type, sent date, and sender. There is also a link to "view all messages". Further down, there is a section for "device and contact details" with fields for device name, ip address, endpoint, and contact. Below that, there is a section for "analyst details" with fields for analyst name and email. At the bottom, there is a section for "telemetry details" with a table showing collection date, map results, and attachments. The table contains one row of telemetry data.

type	sent date	sender

collection date	map results	attachments
1 30 2004, 8:59	ISEE_Entitlement_Check	linksFile.html

## Managing Contacts and Users in the Enterprise View

If you are unfamiliar with contact and user management, please see “Understanding Contact and User Management” on page 18.

To manage a device contact:

1. From the enterprise view, select `view all users` from the left navigation list.
2. Click `Add New User` (see Figure 3-7).

**Figure 3-7** View All Users

The screenshot shows the 'View All Users' page. At the top, there is a navigation bar with links: home, scheduler, enterprise view, servers & status, hp tools, hp admin, and help. Below the navigation bar, there is a breadcrumb trail: > contact hp. The main content area features the HP logo and the text 'view all users'. On the left, there is a sidebar with the 'enterprise view' menu, including options like 'hewlett-packard contact information', 'view company details', 'view all devices', 'view all device groups', 'view open incidents', 'view closed incidents', and 'view all users'. The main content area has an 'Add New User' button and a table of users:

name	email	login name	phone number	actions
example1	example@hp.com		(555)555-5551	<a href="#">delete &gt;&gt;</a>
example2	example@hp.com	admin	(555)555-5552	<a href="#">delete &gt;&gt;</a>
example3	example@hp.com		(555)555-5553	<a href="#">delete &gt;&gt;</a>
example4	example@hp.com		(555)555-5554	<a href="#">delete &gt;&gt;</a>

At the bottom of the page, there are links for 'privacy statement', 'using this site means you accept its terms', and 'feedback to webmaster'. The footer includes the 'motive smart' logo and copyright information: © 2003 Hewlett-Packard Company, © 2003 Motive Communications.

3. Enter your contact information (see Figure 3-8).

**Figure 3-8** Enter Contact Information

The screenshot shows the 'Enter Contact Information' page. At the top, there is a navigation bar with links: home, scheduler, enterprise view, servers & status, hp tools, hp admin, and help. Below the navigation bar, there is a breadcrumb trail: > contact hp. The main content area features the HP logo and the text 'enter contact information'. On the left, there is a sidebar with the 'enterprise view' menu, including options like 'hewlett-packard contact information', 'view company details', 'view all devices', 'view all device groups', 'view open incidents', 'view closed incidents', and 'view all users'. The main content area has a form with the following fields:

- \*full name
- title
- phone
- cell phone
- pager
- \*email (example: name@example.com)
- work hours
- global contact (checkbox: This contact should be notified about issues related to any of this company's devices)

At the bottom of the form, there are buttons: << previous, next >>, finish >>, and cancel >>. At the bottom of the page, there are links for 'privacy statement', 'using this site means you accept its terms', and 'feedback to webmaster'. The footer includes the 'motive smart' logo and copyright information: © 2003 Hewlett-Packard Company, © 2003 Motive Communications.

4. Click [next].

5. Enter an account name and password for the new user, confirm the password (see Figure 3-9).

**Figure 3-9 Enter Password Information**

The screenshot shows the 'enter account information' page. At the top, there is a breadcrumb trail: >> home >> scheduler >> enterprise view >> servers & status >> hp tools >> hp admin >> help. Below this is a sub-breadcrumb: > contact hp. The main heading is 'enter account information' with the HP logo. A sidebar on the left lists navigation options under 'enterprise view': hewlett-packard, contact information, review company details, view all users, view all devices, view all device groups, and view all incidents. The main form area has a section titled '\* Indicates Required Fields' with the following fields: '\*user provider' (a dropdown menu with 'Motive' selected), '\*account name' (a text input field), '\*password' (a text input field), and '\*confirm' (a text input field). At the bottom right of the form are four buttons: '<< previous', 'next >>', 'finish >>', and 'cancel >>'.

6. Click [next].
7. Select the account roles for this account (see Figure 3-10).

**Figure 3-10 Select User Account Roles**

The screenshot shows the 'select account roles' page. The main heading is 'select account roles'. Below the heading is a table with two columns: 'role' and 'description'. The table contains the following rows:

role	description
<input type="checkbox"/> Device Contact	Performs server-side map and closeout approval
<input type="checkbox"/> AnswerWeb Section Editor	Limited authority to manage answers in some AnswerWeb audiences
<input type="checkbox"/> Guest	Limited guest access to the system
<input type="checkbox"/> AnswerWeb Editor Manager	Full authority to manage answers in AnswerWeb
<input type="checkbox"/> AnswerWeb Editor	Limited authority to manage answers in all AnswerWeb audiences
<input type="checkbox"/> Operator	Server Management FROM the Management Console
<input type="checkbox"/> Administrator	User Management FROM the Management Console
<input type="checkbox"/> Support Manager	Unlimited support privileges
<input type="checkbox"/> Senior Support Analyst	Broad support privileges
<input type="checkbox"/> Support Analyst	Limited support privileges

Below the table are two links: 'Check All' and 'Clear All'. At the bottom right of the page are four buttons: '<< previous', 'next >>', 'finish >>', and 'cancel >>'.

8. Click [next].

9. Select the queues you want associated with this account (see Figure 3-11).

**Figure 3-11** Select User Queues

**select account queues**

queue	description
<input type="checkbox"/> Motive	Motive Queue
<input type="checkbox"/> Solaris	Solaris Problems
<input type="checkbox"/> Linux	Linux Problems
<input type="checkbox"/> AIX	AIX Problems
<input type="checkbox"/> HP-UX	HP-UX Problems
<input type="checkbox"/> WinMe	Windows Millennium Problems
<input type="checkbox"/> WinXP	WinXP Problems
<input type="checkbox"/> Win2000	Windows 2000 Problems
<input type="checkbox"/> WinNT	Windows NT Problems
<input type="checkbox"/> Win98	Windows 98 Problems
<input type="checkbox"/> Win95	Windows 95 Problems
<input type="checkbox"/> Default	Default Queue

[Check All](#) | [Clear All](#)

10. Click [*next*].

11. Select the analyst details for this account (see Figure 3-12).

**Figure 3-12** Select Analyst Details

**enter analyst details**

available

notify by e-mail when

- an incident is assigned
- an incident is withdrawn
- a message arrives

studio audience

12. Click [*finish*].



## Managing Company Contact Information in the Enterprise View

If you are unfamiliar with company contact management, please see “Understanding Company Contact Information Management” on page 19.

Change the company information for all ISEE Monitored Clients by completing the following steps:

1. In the Enterprise View, select review company details.
2. Click edit on the company details header (see Figure 3-13).

**Figure 3-13 Review Company Details**

» home » scheduler » enterprise view » servers & status » hp tools » hp admin » help

» contact hp

home | enterprise view | review company details

**review company details** edit >>

**enterprise view**

- » hewlett-packard contact information
- » review company details
- » view all devices
- » view all device groups
- » view open incidents
- » view closed incidents
- » view all users

**company details**

company name	example
business unit	
phone number	(555)555-5555
fax number	
address	1234 5th Avenue Suite 678 New York, NY 00125
time zone	
country	UNITED STATES
technical contact	<a href="mailto:example@hp.com">example@hp.com</a>
key	B70DECAA-A0D5-4C7A-A6AF-86CAFDA14E33-27

privacy statement      using this site means you accept its terms      feedback to webmaster

© 2003 Hewlett-Packard Company, © 2003 Motive Communications.

3. Update your company or contact information (see Figure 3-14).

**Figure 3-14 Edit Company Details**

» home » scheduler » enterprise view » servers & status » hp tools » hp admin » help

» contact hp

home | enterprise view | edit company details

**edit company details**

**enterprise view**

- » hewlett-packard contact information
- » review company details
- » view all devices
- » view all device groups
- » view open incidents
- » view closed incidents
- » view all users

**\* Indicates Required Fields**

*company name	<input type="text" value="example"/>
*business unit	<input type="text"/>
*phone number	<input type="text" value="(555)555-5555"/>
fax number	<input type="text"/>
*address	<input type="text" value="1234 5th Avenue"/> <input type="text" value="Suite 678"/> <input type="text" value="New York"/> <input type="text" value="NY"/> <input type="text" value="00125"/> example: 12345 or 12345-6789
*time zone	<input type="text" value="(GMT-05:00) Eastern Standard Time (America/Indianapolis)"/>
*country	<input type="text" value="UNITED STATES"/>
technical contact	<input type="text" value="--None--"/>
key	B70DECAA-A0D5-4C7A-A6AF-86CAFDA14E33

save >>

4. Click [save] to save your changes.

## Changing the Default Administrator Password in the Enterprise View

If you are unfamiliar with password management, please see “Understanding Password Management” on page 19.

To change the default administrator account password with the Enterprise Service Console, complete the following steps:

1. From the Enterprise View select view all users from the left navigation list.
2. Click the admin account link in the name column (see Figure 3-15).

**Figure 3-15 View All Users**

The screenshot shows the 'View All Users' page in the Enterprise View. The navigation menu on the left includes 'hewlett-packard contact information', 'view company details', 'view all devices', 'view all device groups', 'view open incidents', 'view closed incidents', and 'view all users'. The main content area features a table of users:

name	email	login name	phone number	actions
example1	example@hp.com		(555)555-5551	delete >>
example2	example@hp.com	admin	(555)555-5552	delete >>
example3	example@hp.com		(555)555-5553	delete >>
example4	example@hp.com		(555)555-5554	delete >>

The 'admin' user row is highlighted, and the 'edit >>' link in the actions column is circled in red. The page also includes a footer with 'privacy statement', 'using this site means you accept its terms', 'feedback to webmaster', and 'motive smart' logo.

3. Click [edit] on the account details row (see Figure 3-16).

**Figure 3-16 Review User Details**

The screenshot shows the 'Review User Details' page. The page is divided into several sections:

- contact details:** Includes fields for full name (Example 1), company name, title, phone (555-5555), cell phone, pager, email (Example1@hp.com), work hours (08:00 - 16:00 EST), and global contact (Yes).
- contact notes:** Includes a text area for notes and a 'Save Notes' button.
- account details:** Includes fields for login name (example) and authorization (Motive). This section is highlighted with a red box.
- roles:** Includes a table with columns for role and description. The role 'Support Manager' has the description 'Unlimited support privileges'.
- queues:** Includes a table with columns for queue and description. The queue 'Win98' has the description 'Windows 98 Problems'.
- support analyst details:** Includes fields for status (available) and studio audience (Default Audience).

4. Enter and confirm the new password (see Figure 3-17).

**Figure 3-17** Enter Password Information

The screenshot shows the HP Enterprise View interface for editing an account password. The breadcrumb trail at the top reads: >> home >> scheduler >> enterprise view >> servers & status >> hp tools >> hp admin. Below this, there is a link to > contact hp. The main content area features the HP logo and the title "edit account password". A navigation sidebar on the left includes "enterprise view" (highlighted) and "hewlett-packard contact information" with sub-links for "review company details", "view all users", "view all devices", "view all device groups", and "view all incidents". The form fields are as follows: "account name" with the value "admin"; "\*password" (required field) with an empty input box; and "\*confirm" (required field) with an empty input box. At the bottom right of the form are two buttons: "update >>" and "cancel >>".

5. Click [update].

## Managing Devices in the Enterprise View

If you are unfamiliar with device management, please see “Understanding Device Management” on page 19.

To manage devices in the Enterprise View:

1. From the Enterprise View, select **view all devices**.
2. Click on the name of the device to edit on the **view all devices** page (see Figure 3-18).

**Figure 3-18 View All Devices**

The screenshot shows the HP Enterprise View interface. At the top is a navigation bar with links: >> home, >> scheduler, >> enterprise view, >> servers & status, >> hp tools, >> hp admin, >> help. Below this is a search bar with '> contact hp'. The main content area has a breadcrumb: home | enterprise view | view all devices. The HP logo and 'invent' tagline are visible. A sidebar on the left under 'enterprise view' lists: > hewlett-packard contact information, > review company details, > view all devices, > view all device groups, > view open incidents, > view closed incidents, > view all users. The main content area features a yellow banner: 'There are [devices pending approval](#)'. Below is a 'device polling status totals' table:

polling	not-polling	marked-offline
1	0	0

Below that is a 'devices' table:

polling status	device name	open incidents	support handle	device type	os	ip address	actions
available	<a href="#">bagend</a>	4	not_available		Windows 2000	15.6.37.93	<a href="#">delete &gt;&gt;</a>

At the bottom, there are links for 'privacy statement', 'using this site means you accept its terms', and 'feedback to webmaster'. The Motive Smart logo and copyright information '© 2003 Hewlett-Packard Company, © 2003 Motive Communications' are also present.

From the review device details page, (see Figure 3-20), you can:

- Edit Device Details:
  - a. Click *[edit]* in the device details row on the review device details page to edit device details.
  - b. Make your changes to the device details (see Figure 3-19).

**Figure 3-19 Edit This Device—Device Details**

edit this device

device details	
name	bagend
key	BAGEND;37a2b8c5401a7e6000ec540
company name	□ □□
device type	--None-- <a href="#">Add to this list</a>
service type	--None-- <a href="#">Add to this list</a>
model type	Intel Pentium <a href="#">Add to this list</a>
operating system	Windows 2000 <a href="#">Add to this list</a>
location	--None-- <a href="#">Add to this list</a>
domain	fc.hp.com
status	available
time zone	(GMT-07:00) Mountain Daylight Time (MST)
support handle	not_available
ip address	15.6.37.93

[update >>](#)

- c. Click *[update]*.
- Edit contacts:

- a. From the `contacts` heading on the review device details page and click `[edit]`.

**Figure 3-20 Review Device Details**

**review device details** edit >>

---

**device details**

name	bagend
key	BAGEND;37a2b8c5401a7e6000ec540
company name	□ □ □
device type	
service type	
model type	Intel Pentium
operating system	Windows 2000
location	
domain	fc.hp.com
status	available
time zone	(GMT-07:00) Mountain Daylight Time (MST)
support handle	not_available
ip address	15.6.37.93

---

**contacts** edit >>

name	email
Kevin □	nobody@hp.com
Kevin □	nobody@hp.com

---

**groups**

group name	number of devices
There are no groups that contain this device.	

---

**open incidents**

opened	incident id	wfm id	queue	problem area	description	status
1 30 2004, 9:00	<a href="#">Incident 32</a>		Win2000	New_Installation	New_Installation	open
1 30 2004, 12:36	<a href="#">Incident 42</a>		Win2000	New_Installation	New_Installation	open
1 30 2004, 12:36	<a href="#">Incident 43</a>		Win2000	Entitlement_Check	Entitlement_Check	open
1 30 2004, 12:36	<a href="#">Incident 49</a>		Win2000	TEST incident	cpqHo2GenericTrap	open

---

**collected data**

collection date	map results	attachments
There is no collected data for this device.		

---

**attached devices**

device name	primary service type	status
There are no attached devices for this device.		

---

**device notes**

notes

**Figure 3-21 Edit This Device—Contacts**

**edit this device**

Selected Company:

---

**contacts**

name	email
<input type="checkbox"/> example1	example@hp.com
<input checked="" type="checkbox"/> example2	example@hp.com
<input checked="" type="checkbox"/> example3	example@hp.com
<input type="checkbox"/> example4	example@hp.com

Check All | Clear All

---

update >>

- b. Add or remove contacts for this device by selecting or unselecting each contact's name (only marked contacts are associated with the device).
  - c. Click `[update]`.
- Add notes:

- a. Scroll to the bottom of the review device details page and the device notes heading.

**Figure 3-22 Review Device Details—Device Notes**



The screenshot shows a web interface element for entering device notes. At the top, there is a header bar with the text "device notes" in blue. Below this, the word "notes" is written in a smaller font. The main area is a large, empty text input field with a vertical scrollbar on the right side. To the right of the input field, there is a button labeled "Save Notes".

- b. Enter the text for your device notes, and click [*Save Notes*] to associate your comments with the selected device.

## Managing Device Groups in the Enterprise View

If you are unfamiliar with device group management, please see “Understanding Device Group Management” on page 20.

To manage device groups in the Enterprise Service Console, complete the following steps:

1. From the enterprise view, select view all device groups from the left navigation list.

**Figure 3-23 View All Device Groups**

view all device groups

group name	description	# of devices	actions
<a href="#">All Devices</a>	All devices belonging to a company	1	
<a href="#">Unassigned Devices</a>	All devices belonging to a company that aren't in any group	1	

[Add a New Group](#)

From the view all device groups page you can:

- Add a new device group
  - a. Select Add a New Group on the view all device groups page.
  - b. Select the appropriate list of devices for monitoring from the select group devices page. Use the attributes on the left side of the page to specify common features of your new device group.

**Figure 3-24 Select Group Devices**

home | enterprise view | view all device groups | select group devices

select group devices

Operating System  
Any  
AIX  
HPUX  
Linux

Service Type  
Any

Device Type  
Any

Contact  
Any  
Example

Location  
Any

Select filtering criteria from the lists above.

device name	device	service type	location	company name
<input type="checkbox"/>	example			
0 Selected Devices ( <a href="#">Check All</a>   <a href="#">Clear All</a> )				

<<previous next>> finish>> cancel>>

- c. Add devices to your new device group by checking the device name box for the selected device.



- d. Click *[next]* when you are finished subscribing devices to your new device group.

The enter device group title screen (Figure 3-25) displays.

**Figure 3-25 Enter Device Group Title**

home | [enterprise view](#) | [view all device groups](#) | enter device group title

### enter device group title

\* Indicates Required Fields

\*title

\*description

<<previous next>> finish>> cancel>>

- e. Enter the title of your new device group and a brief description in the text box.
  - f. Click *[finish]* to save your new device group.
- Edit an existing device group
    - a. Select the device group name you want to edit from the view all device groups page.

**Figure 3-26 Review This Group—Devices**

home | [enterprise view](#) | [view all device groups](#) | review this group

### review this group

**identification** edit>>

title test group  
description new group

**devices** edit>>

device name	support handle	device type	os	ip address	status
example	not_available	Windows 2000	37.6.37.93	available	

- b. Select the device name you want to edit.
  - c. Change the identification and subscription list for the selected device group by clicking *edit* on either heading from the review this group page. Review step 3, Adding a New Device Group, for more detail about these processes.
- Delete an existing device group

Click *[delete]* on the same line as the device group that you want to remove.

This process only deletes the device group, the actual devices are still being monitored on the SPOP by ISEE. However, if you have created scheduled collections for this device group, the collections are no longer performed after the group is deleted.

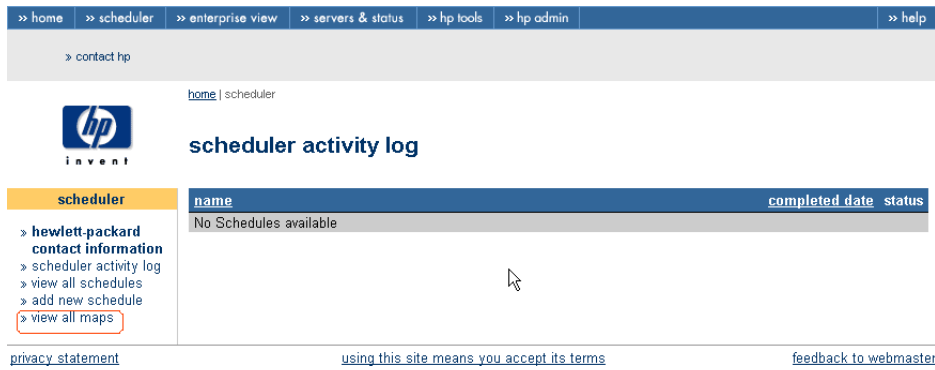
## Using the Scheduler

If you are unfamiliar with the ESC Scheduler, please see “Understanding the Scheduler” on page 21.

To see which the information requested/collected during a system collection, perform the following steps:

1. Select `scheduler` in the horizontal blue navigation bar of the Enterprise Service Console.
2. From the left navigation panel, select the `view all maps` link (see Figure 3-27).

**Figure 3-27 Scheduler Window**



3. Select a MAP in the `view all maps` window (see Figure 3-28).

**Figure 3-28 View All MAPs Window**

### view all maps

name	map type	os platform
<a href="#">Additional HP-UX Comprehensive Information MAP</a>		HPUX
<a href="#">Comprehensive HP-UX System Information MAP</a>		HPUX
<a href="#">Linux Comprehensive System Information MAP</a>		Linux
<a href="#">Solaris Comprehensive System Information MAP</a>		Solaris
<a href="#">Windows Comprehensive System Information MAP</a>		Windows 2000
		Windows 2003
<a href="#">WinGetConfig Comprehensive System Information MAP</a>		Windows 2000
		Windows 2003

Or, select a Map Repository:

- [default](#)
- **[SDC\\_production](#)**
- [SDC\\_test](#)

4. From the review map detail window, (see Figure 3-29), click the show map source link.

**Figure 3-29 Review MAP Detail Window**

review map detail

identification	
title	Additional HP-UX Comprehensive Information MAP
description	NOTICE: This is an HP-UX comprehensive MAP- it runs the 5 other additional HP-UX diagnostic MAPs. This MAP may take 15 or more minutes to complete.
os platform	HPUX
actions	
<a href="#">schedule this map&gt;&gt;</a>	
map parameters	
parameter	default value notes
Enter a timeout multiplication factor	1 Enter a timeout multiplication factor
map source	
<a href="#">Show Map Source</a>	

5. Review the MAP details in map source section of the review map detail window, (see Figure 3-30).

**Figure 3-30 MAP Source**

[Hide Map Source](#)

```
//Additional Comprehensive HP-UX System Information MAP
/*
This HP-UX Comprehensive MAP runs all of the following MAPs in sequence:
Addl_SoftwareConfigurationInformation
Addl_HPUXConfigurationInformation
Addl_HardwareConfigurationInformation
Addl_NetworkInformation
Addl_FileSystemInformation
MAP_VERSION = "A.03.00"
*/
```

To set or change the parameters of the system configuration collections use the directions in the following section.

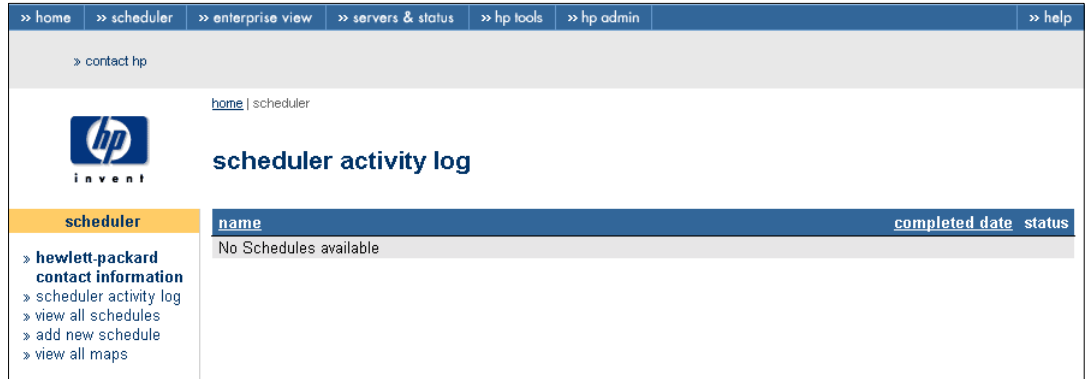
## Scheduling Collections in the Enterprise Service Console

To schedule collections for your enterprise:

1. Select scheduler in the horizontal blue navigation bar.

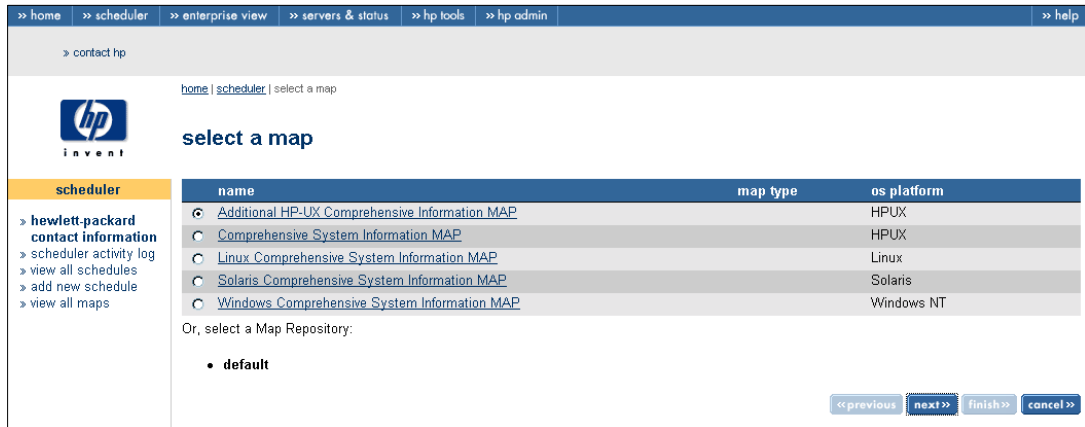
2. Select add new schedule in the left navigation list.

**Figure 3-31 Scheduler Activity Log**



3. Select the Map Repository you want to use. The default MAP repository is used for Support Engineer MAP requests.

**Figure 3-32 Select a MAP**



4. Select the Motive Assistant Program (MAP) you want to schedule.

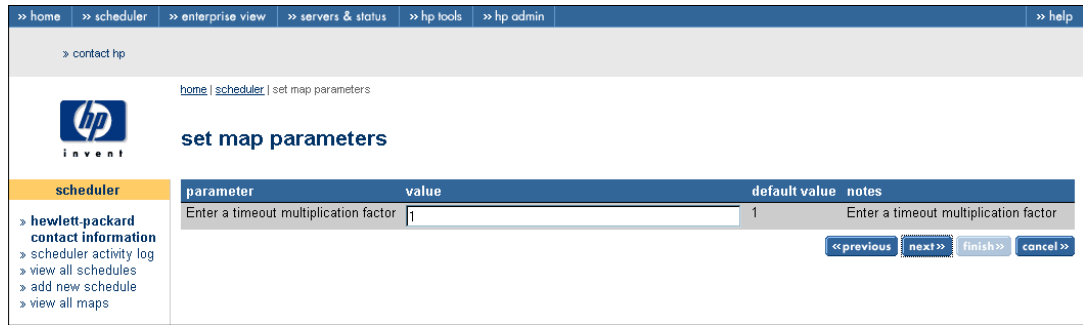
**NOTE**

To enable Contract Compare assessments, choose both the Comprehensive System Map *and* Additional Mission Critical Collectibles.

5. Click [next].

The set map parameters screen (Figure 3-33) displays.

**Figure 3-33 Set MAP Parameters**



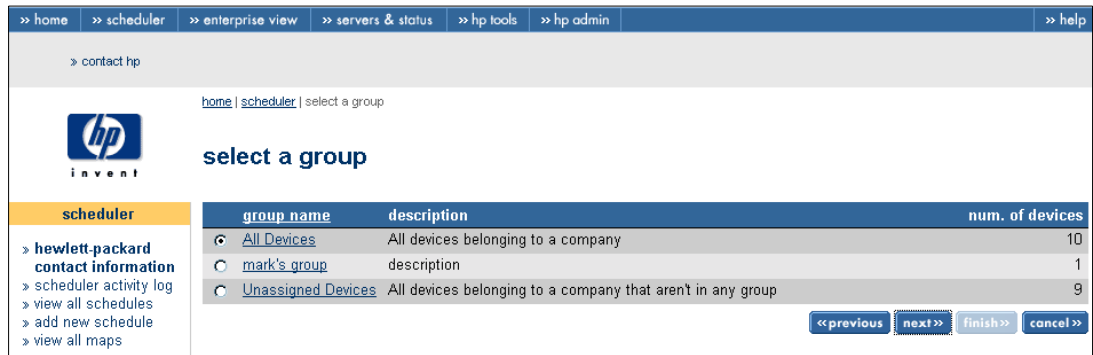
6. Set your map parameters.

The MAP parameters consist of a time-out multiplier.

7. Click [next].

The select a group screen (Figure 3-34) displays.

**Figure 3-34 Select a Group**



8. Select a device group to which this schedule will be assigned.

**NOTE**

Make sure the selected MAP is compatible with the devices in the group you have chosen.

9. Click [next].

The select schedule parameters screen (Figure 3-35) displays.

10. Set your schedule parameters.

**NOTE**

The first scheduled collection must run before a Contract Compare assessment can be run. If your scheduled collection runs on a Monday at 10:00 PM, for instance, the assessment cannot be run until the first collection is complete.

If a device does not complete a collection by the defined deadline, an error is logged. If a schedule does not complete by the defined time-out, pending collections are cancelled and an error is logged for each collection running. To send collection data to Hewlett-Packard, select the checkbox in the escalation section.

**NOTE**

If you want to run a test schedule, create a run once schedule by selecting End after <1> occurrences.

**Figure 3-35 Select Schedule Parameters**

The screenshot shows a web interface for configuring a schedule. The breadcrumb trail is: >> home >> scheduler >> enterprise view >> servers & status >> hp tools >> hp admin >> help. The page title is 'select schedule parameters'. The HP logo is visible. A sidebar on the left contains a 'scheduler' menu with options: hewlett-packard, contact information, scheduler activity log, view all schedules, add new schedule, and view all maps. The main form fields are: 'starting date/time' (Starts: 2-1-2003, 1 PM, 30 MDT); 'recurrence' (radio buttons for Once, Hourly, Daily, Weekly, Monthly; 'Every 1 day(s)' is selected); 'ends' (radio buttons for 'No End Date' and 'End after: 10 occurrences'); 'deadline' (120 minutes); 'timeout' (60 minutes); and 'escalation' (checkbox for 'escalate incident' is checked). Navigation buttons at the bottom right are '<<previous', 'next>>', 'finish>>', and 'cancel>>'.

- 11. Click [next].
- 12. Enter a title and a description for your schedule.

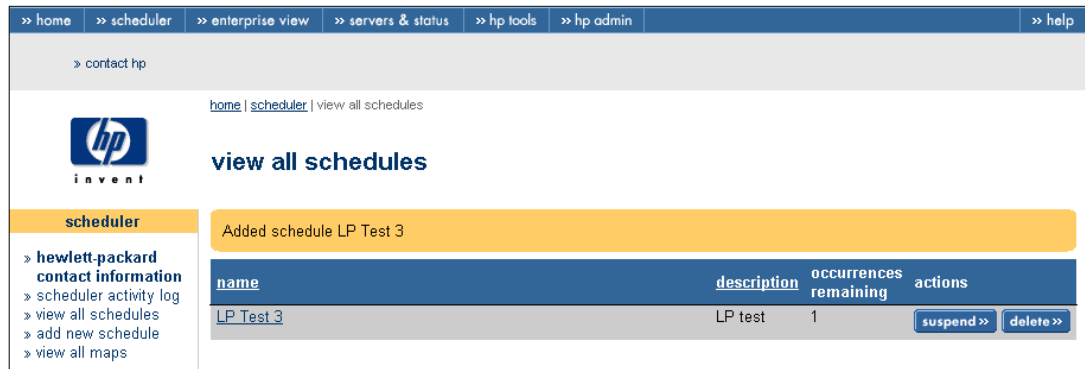
**Figure 3-36 Enter Schedule Title**

The screenshot shows the 'enter schedule title' web form. The breadcrumb trail is: >> home >> scheduler >> enterprise view >> servers & status >> hp tools >> hp admin >> help. The page title is 'enter schedule title'. The HP logo is visible. The sidebar is the same as in Figure 3-35. The main form has a legend: '\* Indicates Required Fields'. There are two input fields: '\*title' and '\*description'. Navigation buttons at the bottom right are '<<previous', 'next>>', 'finish>>', and 'cancel>>'. The footer contains links for 'privacy statement', 'using this site means you accept its terms', and 'feedback to webmaster', along with the 'motive smart' logo and copyright information: © 1994-2002 Hewlett-Packard Company, © 2002 Motive Communications.

- 13. Click [finish].

The view all schedules screen (Figure 3-37) displays showing the schedule you created.

**Figure 3-37 View All Schedules**

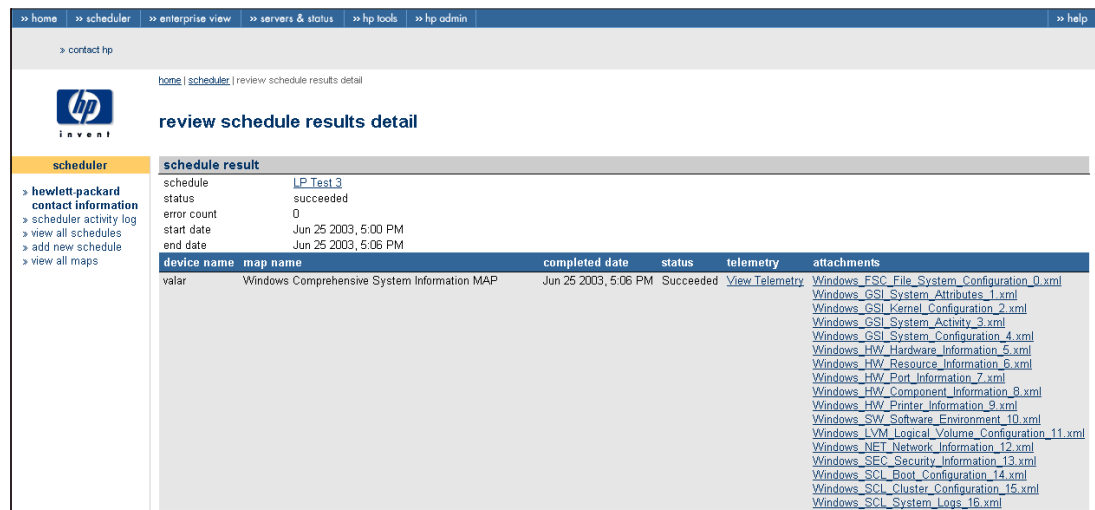


## Viewing Scheduler Results

To view Scheduler results:

1. Select scheduler in the horizontal blue navigation bar.
2. Select the name of the schedule you want to view.

**Figure 3-38 Review Schedule Results Detail**



3. Select an attachment to view by clicking on the corresponding link under the attachments heading in the review schedule results detail window (Figure 3-38).

A new Internet Explorer browser displays (Figure 3-39) showing the results of the schedule run.

**Figure 3-39 View Schedule Attachment**

**Windows\_GSI\_System\_Attributes**

**Table of Contents**

[Command 1. properties.bat -d:](#)

**Command Title: properties.bat -d:**

**Standard Out:**

25125227-0503-0347-7547-BFEBFBFF0000

**Standard Error:**

**Script Log:**

THIS SCRIPT IS BEING RUN BY \  
EXECUTING C:\WINNT\TEMP\hpservices\393\properties.bat -d  
COMMAND C:\WINNT\TEMP\hpservices\393\properties.bat RETURNED 0

[Return to the Top](#)

4. Select View Telemetry in the review schedule results detail window (Figure 3-38) to view the telemetry data.

**Figure 3-40 Review This Telemetry**

» home » scheduler » enterprise view » servers & status » hp tools » hp admin » help

> contact hp

home | enterprise view | view all incidents | review this incident | review this telemetry

**review this telemetry**

map name	severity	map id	collection date	map uuid
Windows Comprehensive System Information MAP		M/SDC_production/maps/MapContent/WindowsComprehensiveSystemInfo.mzp	June 25, 2003 5:03:12 PM MDT	a3f6eh2335fu3iqocuk6

[View raw telemetry](#)

**enterprise view**

- » hewlett-packard contact information
- » review company details
- » view all users
- » view all devices
- » view all device groups
- » view all incidents

5. Select View raw telemetry from the review this telemetry window (Figure 3-40) to view the raw telemetry data.



A new Internet Explorer browser window displays (Figure 3-41) showing the raw telemetry data in an XML file format.

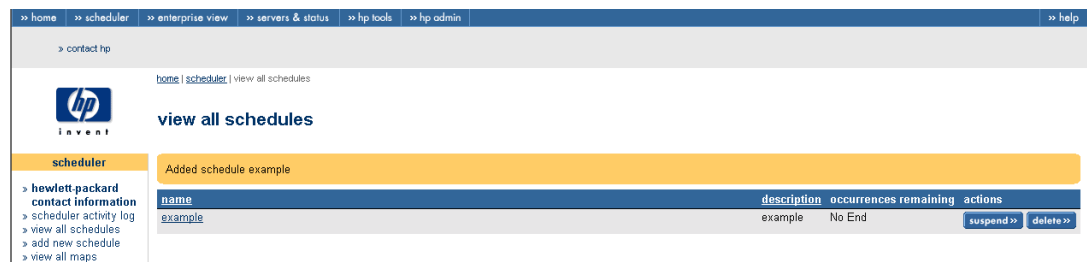
**Figure 3-41 Raw Telemetry Data**

```
<?xml version="1.0" encoding="UTF-8" ?>
- <SUBFRAME>
  <xmlVersion>1.0</xmlVersion>
  <metaframeID>1077639003765@Content</metaframeID>
  <subFrameID>17</subFrameID>
  <ProblemArea />
  <ProblemDescription />
  <MapName>Additional HP-UX Comprehensive Information MAP</MapName>
  <severity />
  <consumableId />
  <mapID>/wt/default/maps/MapContent/Addl_ComprehensiveInformation.mzp</mapID>
  <collectionDate>February 24, 2004 11:36:20 AM EST</collectionDate>
  <MapUUID>I5ulitfq4xrcxbbacrea</MapUUID>
- <displayGroup TITLE="Map Results ( default )">
  - <RunMap>
    <MapFile>MapContent.commonFunctions</MapFile>
  </RunMap>
  - <RunMap>
    <MapFile>MapContent.configDbFunctions</MapFile>
  </RunMap>
  - <host>
    <os>HPUX</os>
    <machineName>default.hp.com</machineName>
    <OS_Release>11.23</OS_Release>
    <majorVersion>11.23</majorVersion>
    <minorVersion />
    <Machine>.default</Machine>
    <processorType>Itanium 40</processorType>
    <processorCount>4</processorCount>
    <processorSpeed>0</processorSpeed>
    <processorSize>64</processorSize>
```

## Altering a Scheduled Collection

- To suspend a scheduled collection:
  1. Select scheduler in the horizontal blue navigation bar.
  2. Click view all schedules in the left navigation panel.
  3. Find the name of the schedule you want to suspend, and click the *[suspend]* button (see Figure 3-42).

**Figure 3-42 Suspend Scheduled Collection**



4. Click OK when prompted to approve the schedule suspension.
- To resume a scheduled collection:
    1. Select scheduler in the horizontal blue navigation bar.
    2. Click view all schedules in the left navigation panel.

3. Find the name of the schedule you want to resume, and click the `[resume]` button (see Figure 3-43).

**Figure 3-43 Resume or Delete Scheduled Collection**



4. Click OK when prompted to approve the schedule suspension.
- To delete a schedule collection:
    1. Select scheduler in the horizontal blue navigation bar.
    2. Click view all schedules in the left navigation panel.
    3. Find the name of the schedule you want to delete, and click the `[delete]` button (see Figure 3-43).
    4. Click OK when prompted to approve the schedule suspension.

## Using Servers & Status

If you are unfamiliar with the Servers and Status utility, please see “Understanding the Servers and Status Utility” on page 23.

### CAUTION

Changing any other server management settings than those described in this section may cause HP ISEE to fail.

## Changing E-mail Notification for Failed Client Polling

To change your e-mail notification for monitored clients that are not communicating with the SPOP, you must reconfigure your e-mail notification default value in the Enterprise Service Console.

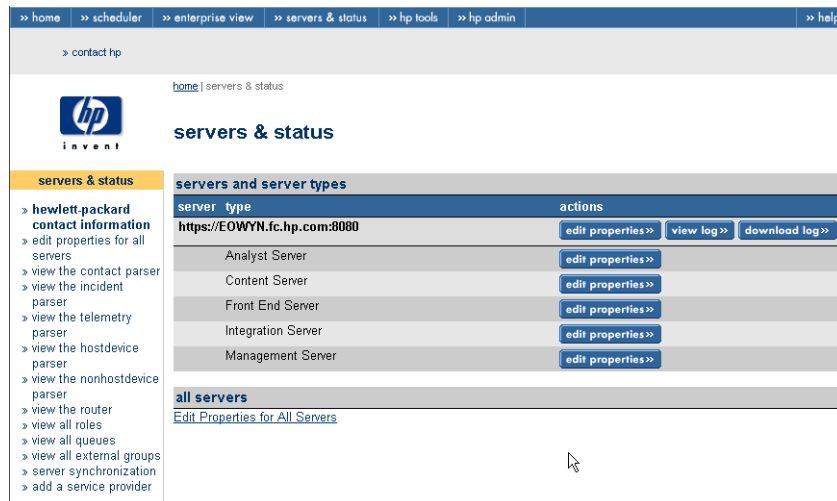
### NOTE

Your default value for e-mail notification is configured during the SPOP installation.

To reconfigure e-mail notification, complete the following steps:

1. Select `servers & status`.
2. Select `[edit properties]` for the Integration Server (see Figure 3-44).

**Figure 3-44 Servers and Status**



3. Click the property:

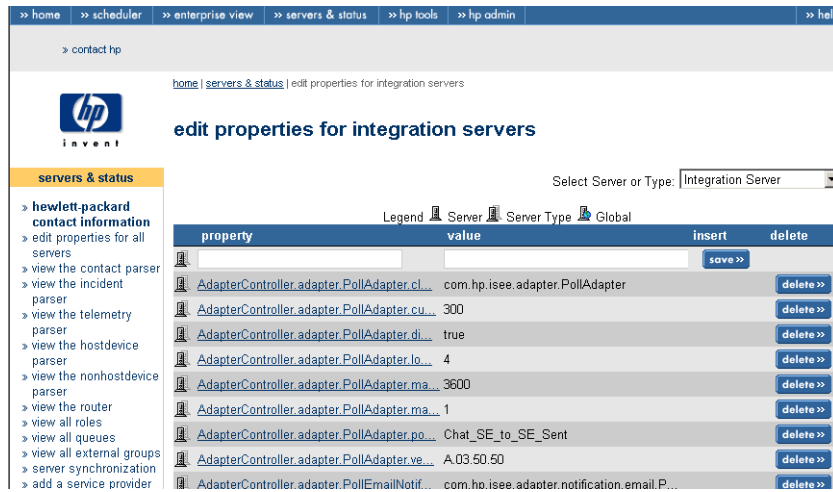
`AdapterController.adapter.PollEmailNotifier.custom.recipients`

You will be directed to the bottom of the page to enter a new value for the property.

**NOTE**

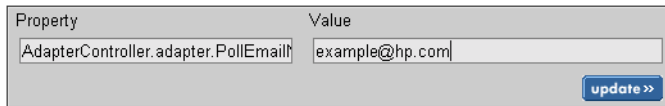
If you cannot read the full property name, the mouse-over function will display the complete property key.

**Figure 3-45 Integration Server Properties**



4. Enter the e-mail address(es) of the person(s) to notify if the client polling fails (see Figure 3-46). Multiple e-mail addresses are separated by commas.

**Figure 3-46 Changing the Down Polling Notification Value**



5. Click Update.

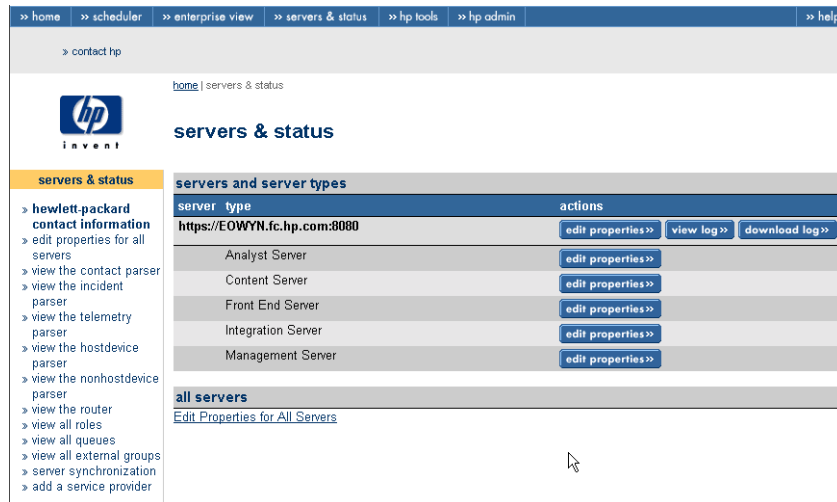
## Changing your SMTP Mail Server

If you change your SMTP mail server after installing HP ISEE, you must reconfigure SMTP server parameters in the Enterprise Service Console.

To change your SMTP mail server, complete the following steps:

1. Select servers & status.
2. Select *[edit properties]* for the Integration Server (see Figure 3-47).

**Figure 3-47 Servers and Status**



3. Click the property:

`AdapterController.adapter.PollEmailNotifier.custom.mailServer`

---

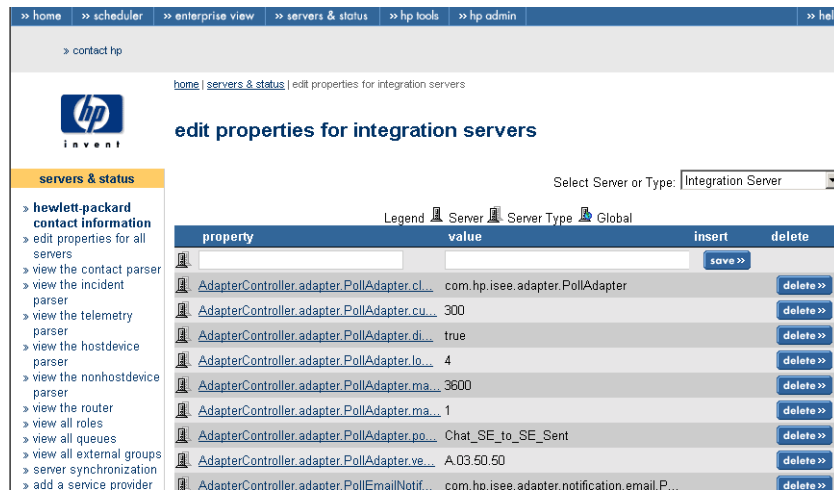
### NOTE

---

If you cannot read the full property name, the mouse-over function will display the complete property key.

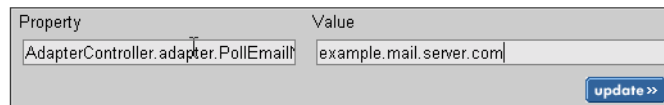
You will be directed to the bottom of the page to enter a new value for the property.

**Figure 3-48 Integration Server Properties**



4. Enter the fully qualified hostname or IP addresses for the new SMTP server (see Figure 3-49). Multiple e-mail addresses are separated by commas.

**Figure 3-49 Changing the SMTP Server Value**



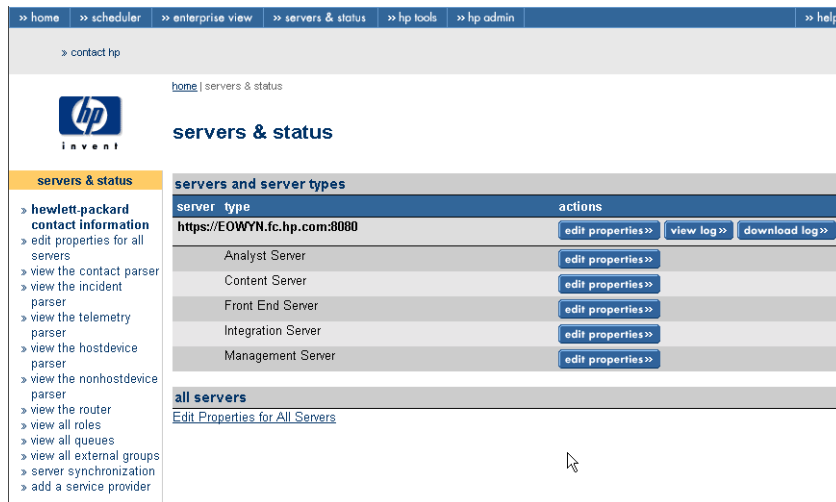
5. Click Update.

## Disabling Notifications to Your SMTP Mail Server

To discontinue notifications sent to your SMTP server, complete the following steps:

1. Select servers & status.
2. Select *[edit properties]* for the SPOP (see Figure 3-50).

**Figure 3-50 Servers and Status**



3. Click the property:

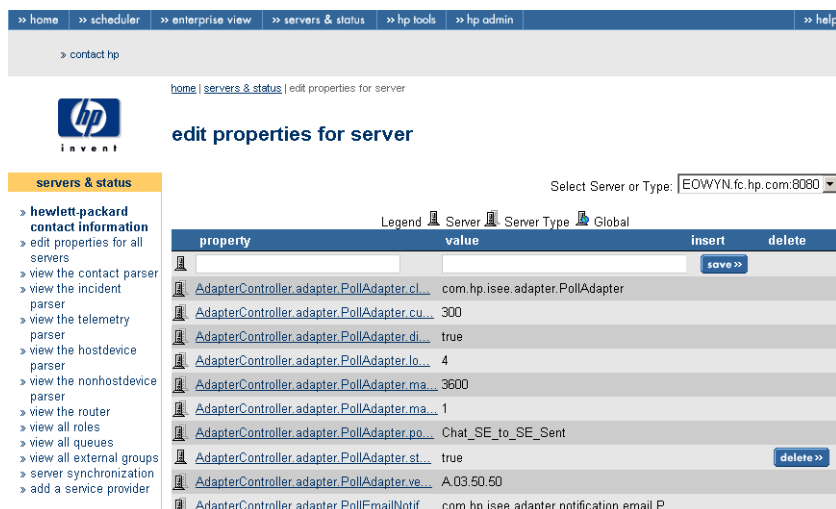
`AdapterController.adapter.PollEmailNotifier.started`

You will be directed to the bottom of the page to enter a new value for the property.

### NOTE

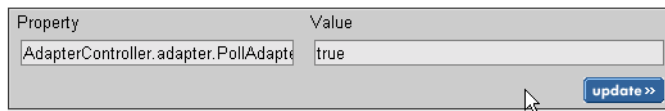
If you cannot read the full property name, the mouse-over function will display the complete property key. Additionally, the property value will display either `true` or `false`.

**Figure 3-51 Integration Server Properties**



4. Set the value to `false` to disable SMTP notifications (see Figure 3-52).

**Figure 3-52** Changing the SMTP Server Value



Property	Value
AdapterController.adapter.PollAdapt	true

update >>

5. Click `[Update]`.



## Using HP Tools: Managing Content Versions

If you are unfamiliar with the content management, please see “Understanding Content Version Management” on page 24.

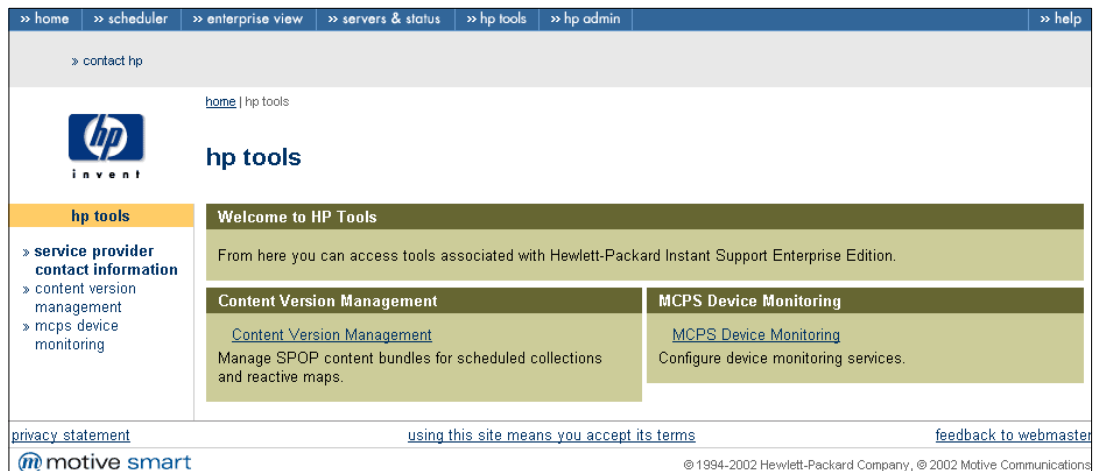
### Downloading New Content Bundles

To accept new software updates and stay synchronized with the HP Support Center, complete the following steps from the Enterprise Service Console:

1. Select `hp tools`.

The `hp tools` screen (Figure 3-53) displays.

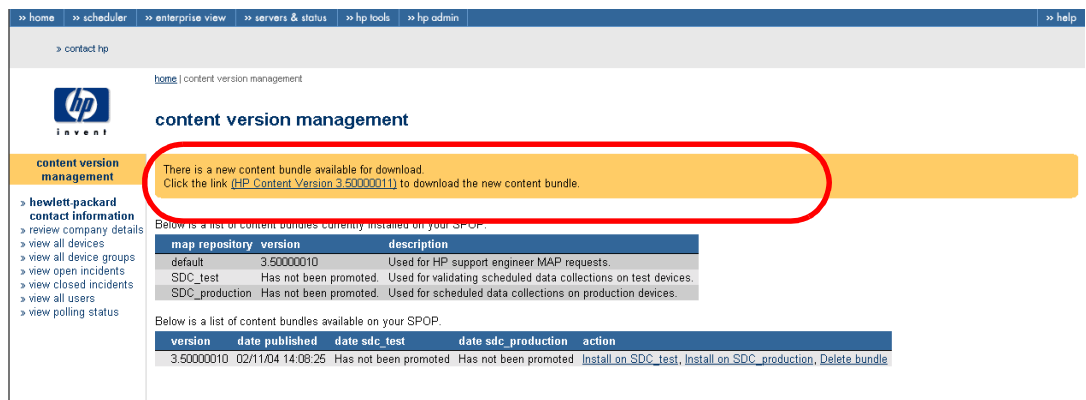
**Figure 3-53** HP Tools



2. Select Content Version Management.

The content version management screen (Figure 3-54) displays.

**Figure 3-54** Content Version Management



If a new SPOP content bundle is available, you will see a notification on the content version management page.

3. Click the **HP Content Version** link to download the content bundle if the notification is there.

Your content is current if no notification is present.

4. Click *[Yes]* to download the executable to the SPOP, when prompted, then run it.

The content is pulled automatically by the monitored clients from the SPOP when needed.

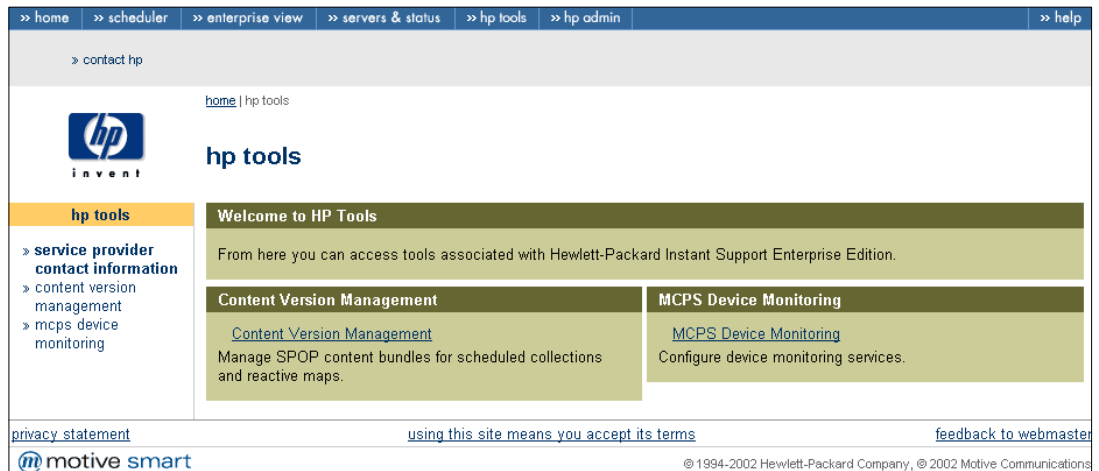
## Managing Content Web Targets

If you are unfamiliar with the content management web targets, please see “Understanding Content Version Management” on page 24.

To promote content to a web target, complete the following steps:

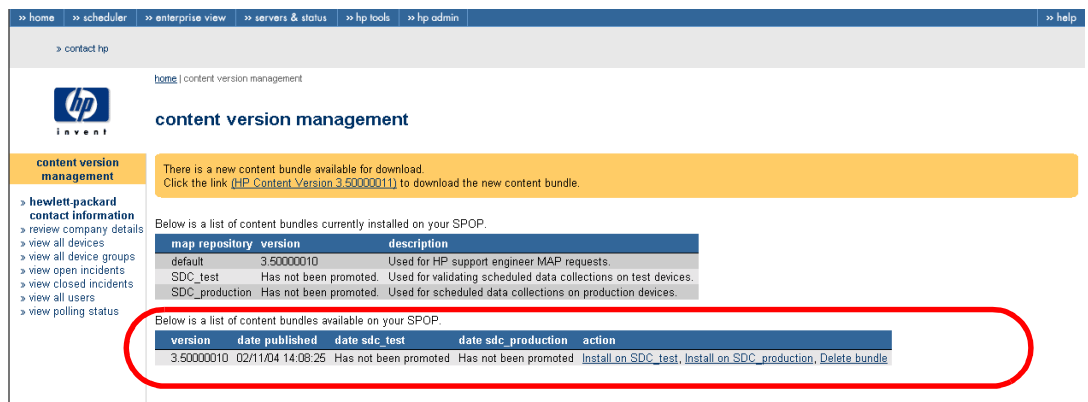
1. From the Enterprise Service Console select **hp tools**.
2. Select **Content Version Management** (see Figure 3-55).

**Figure 3-55 HP Tools**



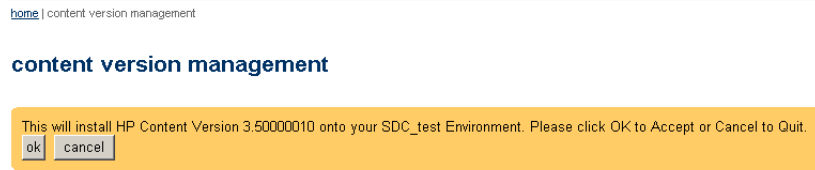
3. Choose a web target to promote/install the content (see Figure 3-56).

**Figure 3-56 Content Version Management**



4. Accept the prompt to download the content by clicking `[OK]` (see Figure 3-57). The content version management window will reload (see Figure 3-56), and the version number of the selected web target should reflect the change.

### Figure 3-57 Content Version Management Continued



## Using HP Tools: Unreachable Device Notification

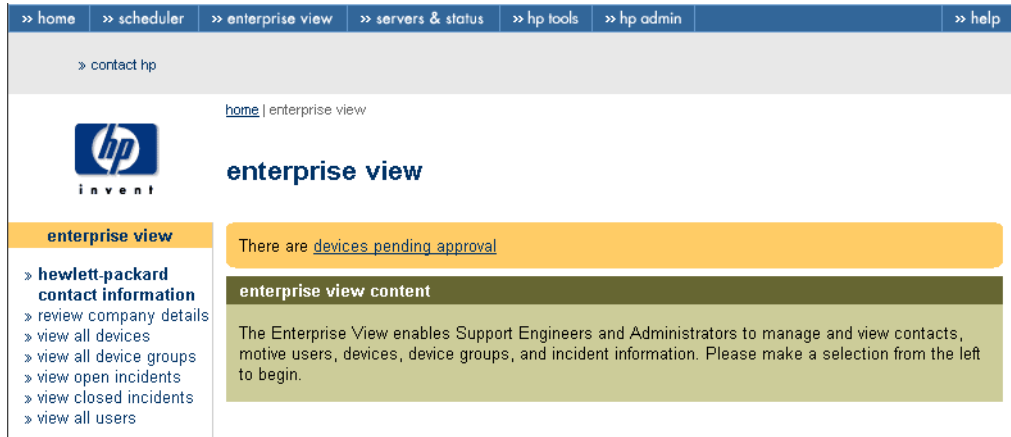
If you are unfamiliar with Unreachable Device Notification, please see “Understanding Unreachable Device Notification” on page 24.

### Accessing the Unreachable Device Notification Application

Access the Device Monitoring features by completing the following steps:

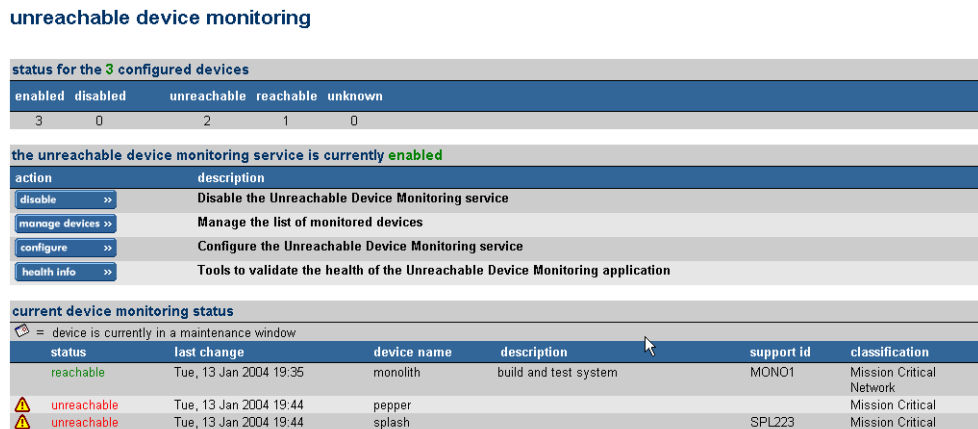
1. Click `hp tools` in the Enterprise Services Console window.

**Figure 3-58** Unreachable Device Notification Access



2. Click Unreachable Device Notification.

**Figure 3-59** Unreachable Device Notification



## Enabling the Device Unreachable Monitoring Service

The status bar at the top of the Unreachable Device Notification window indicates the status of the Device Unreachable monitoring service. When disabled, no devices are monitored. To enable or disable the service, click *[enable]* or *[disable]* see Figure 3-59, “Unreachable Device Notification.”

## Managing Devices

By default all ISEE monitored Clients in your network are added to Unreachable Device Notification with monitoring disabled. Using the Manage Devices option on the Unreachable Device Notification page, you can enable or disable device unreachable monitoring of both ISEE and non-ISEE devices. Additionally, you can add or delete non-ISEE Client devices from the monitoring service and modify the auto-enable device feature.

To access the Device Management window:

1. Click Manage Devices from the Unreachable Device Notification window.

The manage monitored devices screen (Figure 3-60) displays.

Figure 3-60

### Manage Monitored Devices

The screenshot shows the 'manage monitored devices' page. It features a sidebar with navigation links and a main content area. The main content area includes a form to add a device, a table of contacts, and a table of devices configured for monitoring.

selected?	name	email	login name	phone number
<input type="checkbox"/>	test1	test@hp.com		555-0000
<input checked="" type="checkbox"/>	test1	test@hp.com		555-0000
<input type="checkbox"/>	test1	test@hp.com		555-0000
<input type="checkbox"/>	test1	test@hp.com		555-0000

device name	description	support id	classification	enabled?	actions
monolith	build and test system	MONO1	Mission Critical Network	yes	<a href="#">disable &gt;&gt;</a> <a href="#">delete &gt;&gt;</a>
pepper			Mission Critical	yes	<a href="#">disable &gt;&gt;</a> <a href="#">delete &gt;&gt;</a>

2. Enter the Device name, Description, and Support ID in the fields provided, select the proper device classifications, and click *[add device]* to add a non-ISEE device.

### NOTE

The device classification option automatically assigns incidents to the proper support team. This distinction enables HP to support Mission Critical and Network customers more quickly.

3. Select one or more contacts to be associated with this device.

---

**NOTE**

---

To manage contacts use the Enterprise Service Console. For more information, see “Understanding Contact and User Management” on page 18.

4. Click *[enable]* or *[disable]* next to the Auto-Enable Device feature to enable or disable the Auto-Enable Device feature.

When the Auto-Enable Device feature is enabled, any new ISEE device discovered is automatically enabled for monitoring.

5. Click *[enable]* or *[disable]* next to the non-ISEE device you want to enable or disable.
6. Click *[delete]* next to the non-ISEE device you want to delete.

## Configuring Device Monitoring Features

The Unreachable Device Management features enable you to control the following tasks:

- “Managing Maintenance Windows” on page 64.
- “Managing the E-mail Notification Address List” on page 65.
- “Managing Global Default Settings” on page 66.
- “Managing Device Settings” on page 67.

To access these configuration settings, click *[configure]* in the Unreachable Device Notification window.

The unreachable device configuration screen (Figure 3-61) displays.

Figure 3-61

### Unreachable Device Configuration

The screenshot shows the 'unreachable device configuration' page in the HP Enterprise Service Console. The page has a blue header with navigation links: home, scheduler, enterprise view, servers & status, hp tools, hp admin, and help. Below the header is a breadcrumb trail: home | hp tools | device monitoring | unreachable configuration. The main content area is titled 'unreachable device configuration' and includes an HP logo. A left sidebar contains 'hp tools' and a tree view with 'service provider contact information', 'content version management', and 'unreachable device monitoring'. The main content area has several sections:
 

- unreachable device configuration**: A brief description of the Unreachable Device Monitoring (UDN) application.
- maintenance windows**: A section for configuring maintenance periods. It lists three default windows: Daily (00:00 to 00:01), Weekly (Sun 00:05 to Sun 00:07), and Daily (11:00 to 11:01). A 'manage list' button is present.
- email notification address list**: A section for configuring email addresses. It shows a default address 'default@hp.com'. A 'manage list' button is present.
- global default settings**: A section for configuring global parameters. It includes a table of settings.

parameter	current value	description
Create Incident	yes	Defines whether an ISEE incident should be created to notify the HP Support Center when the status of a device changes.
Notify Email	yes	Defines whether an email should be sent to the configured recipients when the status of a device changes.
Create Reachable Notifications	yes	Defines whether a notification should be created when devices become reachable, in addition to the unreachable notifications.
Polling Frequency	1 min.	The frequency the UDN service should poll a device to determine its state.
Failure Threshold	2 polls	The number of consecutive polls for the device to be unreachable before an unreachable notification is created.
Reachable Threshold	2 polls	The number of consecutive polls for the device to be reachable before a reachable notification is created.
SNMP Community Name	****	The SNMP community name used in polling SNMP-capable devices.

At the bottom of the settings section is an 'edit settings' button.

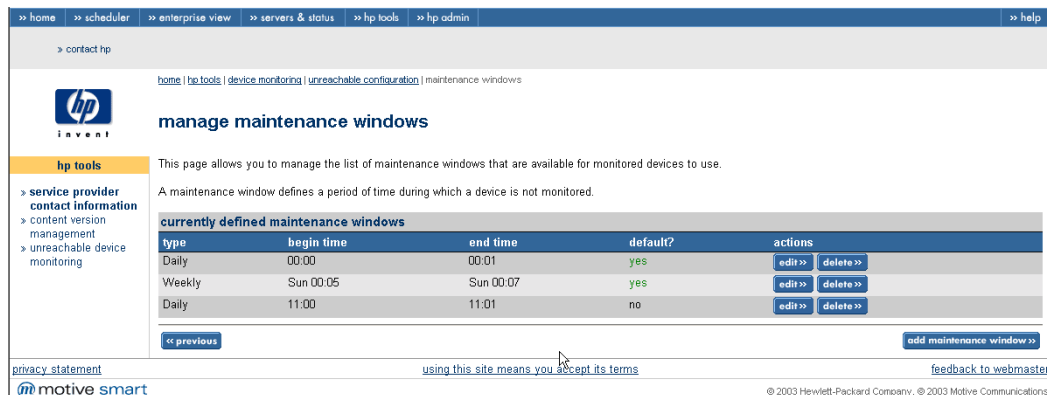
## Managing Maintenance Windows

You can view, edit, and create maintenance windows through the device unreachable configuration window.

1. Click *[manage list]* in the maintenance windows section of the device unreachable configuration window.

The manage maintenance windows screen (Figure 3-62) displays.

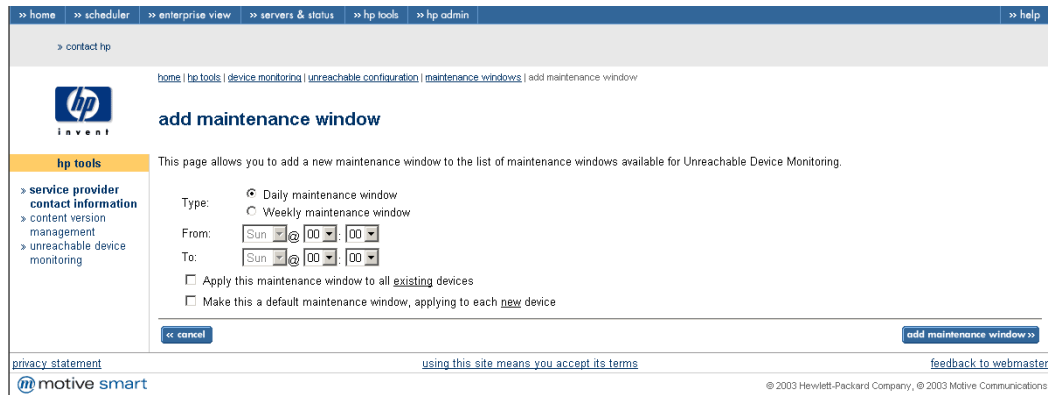
**Figure 3-62** Manage Maintenance Windows



2. Click *[edit]* next to an existing maintenance window to change its settings, or click *[delete]* to remove it.
3. Click *[add maintenance window]* to access the add maintenance window.

The add maintenance window screen (Figure 3-63) displays.

**Figure 3-63** Add Maintenance Window



4. Set your preferred configuration information and click *[add maintenance window]* again.



## Managing the E-mail Notification Address List

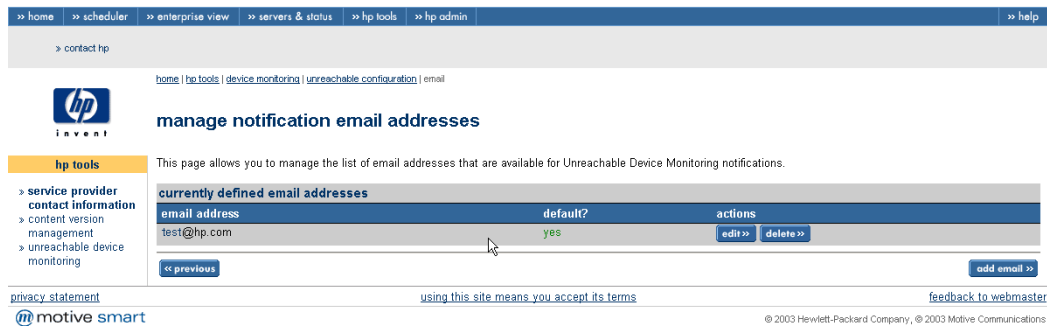
You can manage addresses for e-mail notification through the device unreachable configuration window.

To edit or add an e-mail address:

1. Click *[manage list]* in the e-mail notification address list section of the device unreachable configuration window (Figure 3-64).

The manage notification email addresses screen (Figure 3-64) displays.

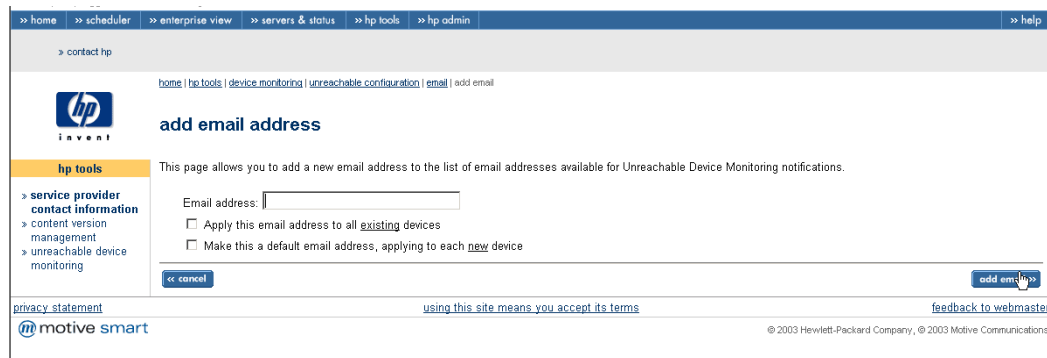
**Figure 3-64** Manage Notification E-Mail Addresses



2. Click *[edit]* next to an e-mail address to update it, or click *[delete]* to remove it.
3. Click *[add e-mail]* to access the add email address window.

The add email address screen (Figure 3-65) displays.

**Figure 3-65** Add E-Mail Address



4. Enter the updated e-mail information and click *[add e-mail]* again.

## Managing Global Default Settings

You can manage the global default settings for your monitored devices through the device unreachable configuration window.

To edit all of the global default settings:

1. Click *[edit settings]* in the global default settings section of the device unreachable configuration window.

The global default settings section (Figure 3-66) of the screen displays.

**Figure 3-66 Global Default Settings Section**

**global default settings**

The following settings are default parameters available for use by each monitored device. Each of these parameters can be overridden by an individual device in the [Device Settings](#) section below.

parameter	current value	description
Create Incident	yes	Defines whether an ISEE incident should be created to notify the HP Support Center when the status of a device changes.
Notify Email	yes	Defines whether an email should be sent to the configured recipients when the status of a device changes.
Create Reachable Notifications	yes	Defines whether a notification should be created when devices become reachable, in addition to the unreachable notifications.
Polling Frequency	1 min.	The frequency the UDN service should poll a device to determine its state.
Failure Threshold	2 polls	The number of consecutive polls for the device to be <b>unreachable</b> before an unreachable notification is created.
Reachable Threshold	2 polls	The number of consecutive polls for the device to be <b>reachable</b> before a reachable notification is created.
SNMP Community Name	*****	The SNMP community name used in polling SNMP-capable devices.

[edit settings >>](#)

2. Click *[edit settings]*.

The modify global default settings screen (Figure 3-67) displays.

**Figure 3-67 Modify Global Default Settings Windows**

[home](#) | [hp tools](#) | [device monitoring](#) | [unreachable configuration](#) | [edit global default settings](#)

**modify global default settings**

This page allows you to modify the global default settings listed below. Each device will use these default values only if the values have not been overridden by the individual device settings.

parameter	value	description
Create Incident	<input type="text" value="yes"/>	Defines whether an ISEE incident should be created to notify the HP Support Center when the status of a device changes.
Notify Email	<input type="text" value="yes"/>	Defines whether an email should be sent to the configured recipients when the status of a device changes.
Create Reachable Notifications	<input type="text" value="yes"/>	Defines whether a notification should be created when devices become reachable, in addition to the unreachable notifications.
Polling Frequency	<input type="text" value="1"/> min.	The frequency the UDN service should poll a device to determine its state.
Failure Threshold	<input type="text" value="2"/> polls	The number of consecutive polls for the device to be <b>unreachable</b> before an unreachable notification is created.
Reachable Threshold	<input type="text" value="2"/> polls	The number of consecutive polls for the device to be <b>reachable</b> before a reachable notification is created.
SNMP Community Name	<input type="text" value="*****"/>	The SNMP community name used in polling SNMP-capable devices.

[cancel](#) [save >>](#)

3. Edit the appropriate global default settings and click *[save]* to return to the device unreachable configuration window.

## Managing Device Settings

You can manage individual monitored device settings through the device settings section of the device unreachable configuration window. This lets you customize the device unreachable service if one of your systems requires special configuration settings.

1. Click *[enable]* or *[disable]* next to the device you want to enable or disable.
2. Click *[edit]* next to the device you want to edit.

**Figure 3-68** Modify Device Settings Section

**device settings**

For each monitored device, you can:

- View the current monitor settings
- Edit the monitoring parameters (select the *Edit* button)
- Enable or disable the monitoring of a device (select the *Disable/Enable* button)

device name	enabled?	settings	
<b>monolith</b>	yes	<a href="#">Customized Settings</a> Polling Frequency 10 min.	<a href="#">Email Addresses</a> Email Address @hp.com (default) <a href="#">Maintenance Windows</a> Daily 00:00 to 00:01 (default) Daily 11:00 to 11:01
build and test system MONO1			
<b>pepper</b>	yes	<a href="#">Customized Settings</a> -- none set --	<a href="#">Email Addresses</a> Email Address @hp.com (defe <a href="#">Maintenance Windows</a> Daily 00:00 to 00:01 (defe Weekly Sun 00:05 to Sun 00:07 (defe
<b>splash</b>	yes	<a href="#">Customized Settings</a> -- none set --	<a href="#">Email Addresses</a> Email Address @hp.com (defe <a href="#">Maintenance Windows</a> Daily 00:00 to 00:01 (defe Weekly Sun 00:05 to Sun 00:07 (defe
system SPL223			

[<< previous](#)

3. Modify the appropriate settings, and click [save] to return to the device unreachable configuration window.

**Figure 3-69 Modify Device Settings Window**

**hp tools** modify device settings: test system

This page allows you to modify the device settings listed below.

**Device description** (optional)

**Support ID** (optional)

**Device Classification**  
 Used for routing notifications to appropriate HP support teams.  
 Mission Critical (default)  
 Network  
 (select at least one)

**Contacts** (optional)  
 Select the contact(s) to be associated with this device.  
 To manage this list of contacts, go to the [View All Users](#) page.

selected?	name	email	login name	phone number
<input checked="" type="checkbox"/>	test	test@hp.com		555-0000
<input type="checkbox"/>	test	test@hp.com		555-0000
<input type="checkbox"/>	test	test@hp.com		555-0000
<input type="checkbox"/>	test	test@hp.com		555-0000

**monitoring parameters**  
 Note: if default is chosen for a parameter, the global default setting will be used for this device.

parameter	value	default value	description
Create Incident	default	yes	Defines whether an ISEE incident should be created to notify the HP Support Center when the status of a device changes.
Notify Email	default	yes	Defines whether an email should be sent to the configured recipients when the status of a device changes.
Create Reachable Notifications	default	yes	Defines whether a notification should be created when devices become reachable, in addition to the unreachable notifications.
Polling Frequency	10 min.	1 min.	The frequency the UDN service should poll a device to determine its state.
Failure Threshold	default polls	2 polls	The number of consecutive polls for the device to be unreachable before an unreachable notification is created.
Reachable Threshold	default polls	2 polls	The number of consecutive polls for the device to be reachable before a reachable notification is created.
SNMP Community Name	default	*****	The SNMP community name used in polling SNMP-capable devices.

**maintenance window subscription**

apply?	type	begin time	end time	default?	notes
<input checked="" type="checkbox"/>	Daily	00:00	00:01	yes	A maintenance window defines a period of time during which a device is not monitored.
<input type="checkbox"/>	Weekly	Sun 00:05	Sun 00:07	yes	Select the checkboxes by the maintenance windows you want to apply to this system.

---

## **4 Using Software Management**

This chapter describes the processes that are used to secure the SPOP against viruses and ensure that it is up to date with the latest relevant security patches. The Software Management application is the tool that accomplishes these tasks.

## Anti-Virus Protection on the SPOP

---

### IMPORTANT

Updates are mandatory and are automatically downloaded and installed on the SPOP during a regularly occurring polling interval. You must subscribe to the update to make it active on the SPOP.

You will be notified of updates as they become available. When a Symantec Anti Virus update is available, complete the section “Updating Symantec Anti Virus Definitions” to update the SPOP.

### Virus Protection Process

Virus definition updates are automatically downloaded once every two weeks to all SPOPs that have established connectivity to the Regional Data Centers. ISEE Support Services may distribute emergency patches if an urgent security issue is identified by HP Corporate IT.

Every SPOP running software at A.03.00 or higher is installed with Symantec Anti-Virus software (SAV). Every two weeks, the ISEE Support Services team releases SAV definition file updates. These updates occur every other Monday. If a scheduled update falls on a US holiday, the update is published on the next business day. Emergency updates will be released on the next business day after a notification has been received from HP Corporate IT.

The virus protection process is as follows:

- Definition files are collected from Symantec.
- A distribution package is created and tested within HP.
- Email notification is sent to each of the Current customer SPOP contacts
- Updates are automatically downloaded and installed via Spirian, unless Spirian has been configured to require manual intervention.

### Symantec LiveUpdate Options

**A.03.00 and A.03.50 SPOP:** Users who require virus updates more often than ISEE sends out an update, you may enable a direct connection from Symantec Anti-Virus on the SPOP to Symantec for auto updates. You must have direct internet connectivity to the Symantec web site. Go to

`http://ftp.symantec.com/public/english_us_candada/liveupdate/updates/lusetup.exe`

to download a free version of the LiveUpdate Software. Normally this utility would be included with SAV, but it has been removed from the SPOP.

---

### WARNING

**Symantec Anti-Virus is the only supported anti-virus software on the SPOP. Installing other anti-virus software on the SPOP will move it to an unsupported state.**

---

Automatic downloads through Spirian continue unless you manually disable them. SAV will not install an earlier definition file over a later one: your virus definition file can not go backwards.

**A.03.90 SPOP:** Users automatically receive Symantec LiveUpdate with the SPOP configuration or upgrade.

---

**NOTE**

For more information about configuring schedules with Symantec LiveUpdate, see “Enabling and Scheduling Symantec LiveUpdate” on page 73.

---

## Updating Symantec Anti Virus Definitions

If your SPOP is configured for manual intervention, when you receive a notification of updated content, you must complete the following steps:

1. Open an Internet Explorer browser to:

`http://<spop_hostname>:7717/console`

Where <spop\_hostname> is the fully qualified hostname or IP address of the SPOP.

2. Log on as administrator with the password you set for the SPOP.

---

**NOTE**

You may use any account with administrator privileges that has been configured on this SPOP.

---

**Figure 4-1** Logging into the Software Management Tool

03:44 PM on 2/11/2004

---

You are not logged into the Instant Support Enterprise Edition Console.  
Please login.

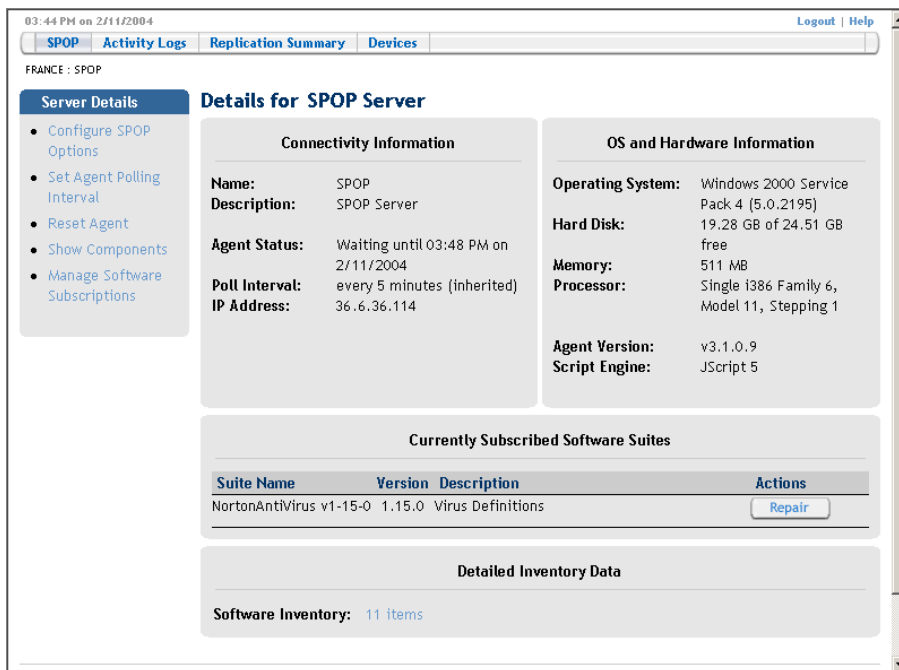
User name:	<input type="text" value="administrator"/>
Password:	<input type="password"/>
Domain:	<input type="text" value="localhost"/>

**Enter your credentials**

Please enter your credentials in the fields on the left to authenticate against your NT-based security database. Failure to provide the correct information will cause this screen to reload.

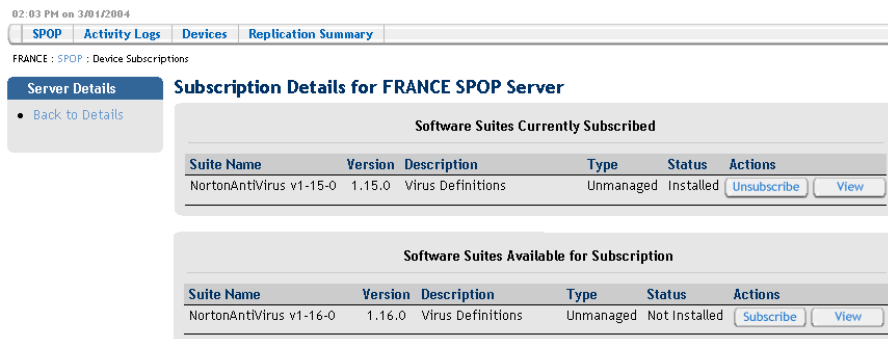
- Click Manage Software Subscriptions on the left side of the screen (see Figure 4-2).

**Figure 4-2 SPOP Server Details**



- Click *[subscribe]* to add the Symantec Anti Virus version update (see Figure 4-3).

**Figure 4-3 Selecting Software to Install**



- Use the browser's *[Refresh]* button to monitor the progress.
- View the Manage Software Subscriptions window to verify that the updated version of Symantec Anti Virus is displayed under Software Suites Currently Subscribed.

You can also view the logs for Symantec Anti Virus updates by clicking the *[View]* button on the Currently Subscribed entry for the software suite.



## Troubleshooting

**Confirming a correct Spirian installation** On the SPOP console, log in to `http://<localhost>:7717/console`. Use “administrator” for the user name and the SPOP password for the password. If the login screen displays, Spirian is operating correctly.

**Confirming a Download of Anti-Virus Definitions** On the SPOP, go to Start > Programs > Symantec Anti-Virus Corporate Edition > Symantec Anti-Virus Corporate Edition. Compare the date of the virus definition file on the screen with the date of the latest file that was distributed (in your email notification)

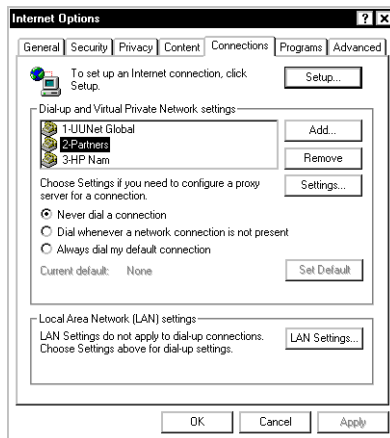
## Enabling and Scheduling Symantec LiveUpdate

You may optionally enable LiveUpdate and schedule regular antivirus updates. Symantec LiveUpdate is installed in a disabled state. If the customer chooses to leave LiveUpdate inactive, antivirus updates can still be made using the software management application. See the SPOP Users Guide for more information about Norton antivirus updates using the software management application.

To enable Symantec LiveUpdate, the customers network administrator must configure an opening to be used for communication from the SPOP to Symantec. Consult your HP Account Team for more information. Once the opening is established, complete the following steps:

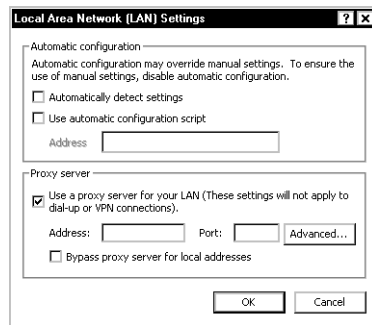
1. Open Internet Explorer
2. Select Tools > Internet Options
3. Click the Connections tab

**Figure 4-4 Internet Options Connections Tab**



4. Click the Lan Settings button

**Figure 4-5 LAN Settings Window**



5. In the Proxy Server panel check the Use a proxy server box

---

**NOTE**

These settings will not apply to dial-up or VPN connections.

6. Enter the information provided by the customer's network administrator in the Address and Port fields.

---

**NOTE**

If the SPOP is behind a firewall (in the DMZ), the network administrator must also open the corresponding port in the firewall to enable access to Symantec for LiveUpdate.

7. Check the Bypass proxy server for local address option.

8. Click the OK button on the Local Area Network (LAN) Settings window.

9. Click the OK button on the Internet Options window.

10. Close Internet Explorer.

11. Open the Symantec AntiVirus application.

---

**NOTE**

This can be done from the task bar or the start menu.

12. Click File and select LiveUpdate.

13. Click Start when prompted to start LiveUpdate.

**Figure 4-6 Start LiveUpdate**

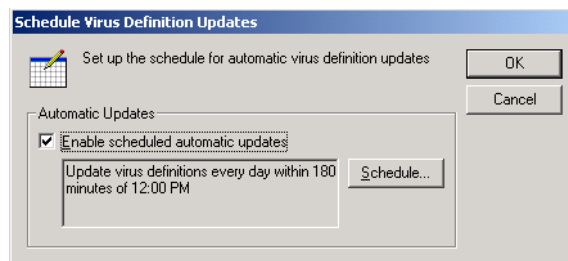


14. Click Close when LiveUpdate is finished.

15. Click File and select Schedule Updates.

16. In the Automatic Updates panel check the Enable scheduled automatic updates box.

**Figure 4-7 Schedule LiveUpdate**



---

**NOTE**

Click the Schedule button to optionally customize the schedule.

17. Click OK.

## Security Patching Process

ISEE contains the most current relevant security patches in each SPOP release image. New security patches are made available on an as-needed basis after testing within HP. When ISEE Support Services is notified of a new security threat, the patch is evaluated for applicability to the SPOP and tested.

Apply pertinent security patches to the SPOP, based on SPOP patch notifications. The notifications indicate that a specific patch does not adversely affect the SPOP functionality, and that the specific patch is supported. These security patches are not automatically distributed to the SPOPs. Your HP account team member must obtain and apply the pertinent security patches.

## Controlling Automatic Downloads with the Software Management Application

Software updates are automatically downloaded to the SPOP to expedite the subscription process, however the software is not updated until you *subscribe* to it. These download updates occur when the SPOP polls the HP software management server and finds new software available.

Disabling automatic downloads is *Highly Discouraged* if you are relying on the software management application (Spirian) for Symantec AntiVirus (SAV) updates. If you do disable automatic updates, you will also disable automatic SAV updates, and all further SAV updates will require manual application. However, if you have enabled Symantec LiveUpdate, you may safely disable automatic downloads. See “Symantec LiveUpdate Options” on page 70 for more information about Symantec LiveUpdate.

If you do not want the software to download updates automatically, complete the following steps:

1. Open an Internet Explorer browser to:

`http://<spop_hostname>:7717/console`

Where `<spop_hostname>` is the fully qualified hostname or IP address of the SPOP.

2. Log on as administrator with the password you set for the SPOP.

### NOTE

You may use any account with administrator privileges that has been configured on this SPOP.

**Figure 4-8** Logging into the Software Management Tool

03:44 PM on 2/11/2004

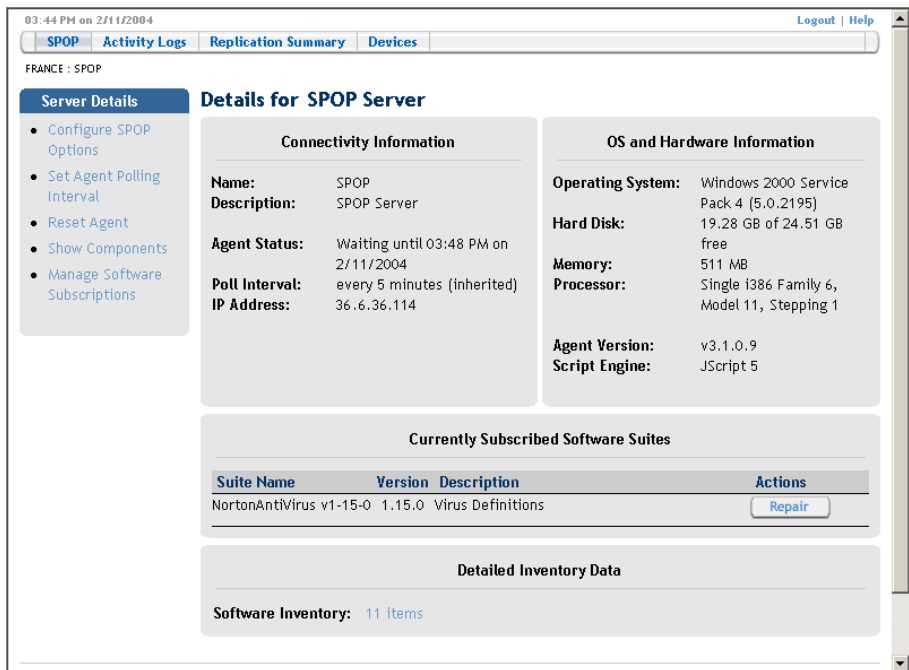
---

You are not logged into the Instant Support Enterprise Edition Console.  
Please login.

User name:	<input type="text" value="administrator"/>	<b>Enter your credentials</b> Please enter your credentials in the fields on the left to authenticate against you NT-based security database. Failure to provide the correct information will cause this screen to reload.
Password:	<input type="password"/>	
Domain:	<input type="text" value="localhost"/>	
<input type="button" value="Login"/>		

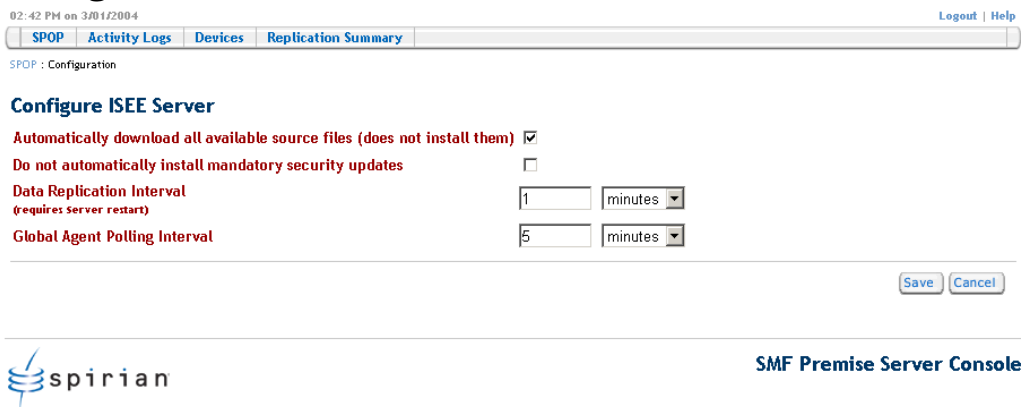
3. Click **Configure SPOP Options** on the left side of the screen (see Figure 4-9).

**Figure 4-9 SPOP Server Details**



4. Uncheck the box to **Automatically download all available source files to disable automatic downloading** (see Figure 4-10). Simply recheck this box if you want to enable automatic downloading in the future.

**Figure 4-10 Configure ISEE Server**



---

# Glossary

## A-C

**Advanced Configuration** One of two HP ISEE supported customer configurations. Much of HP ISEE information and data transport is managed through the Support Point of Presence (SPOP).

## D

**Demilitarized Zone (DMZ)** A DMZ is the area between an internal network and the Internet.

## E-G

**Enterprise Service Console** Resides on the Management Server and the SPOP (available only in the Advanced Configuration), provides a consolidated view of your enterprise components, and enables you to perform some management tasks.

**External Gateway** Used for communication from the SPOP through the external firewall to the HP Support Center.

## H-L

**HP Support Center** HP Support Center is a general term that refers to any of the regional support centers that provide customer support.

**HP Support Engineer** HP Support Engineer is a general term that refers to any engineer providing support to a customer through the HP ISEE application, telephone, or in person onsite.

## M-Q

**Motive Application Program (MAP)** Predefined scripts designed to gather basic system information and to diagnose hardware and software problems on your HP ISEE monitored Clients. MAPs are used for incident creation, diagnostics, and telemetry collection.

**Monitored Client** A monitored Client is any server covered by your HP Support Contract that has HP ISEE installed on it.

## R

**Resource Portal** The Resource Portal is access through the Insight application on the SPOP and provides information about HP ISEE MAPs.

## S

**Secure Shell** In the Advanced Configuration, Secure Shell can be used by authorized HP Support Analysts to access customer's monitored Clients from the SPOP.

**Standard Configuration** is one of two HP ISEE supported customer configurations. The Standard Configuration is targeted at customers with HP-UX, Linux, and Windows servers, and storage devices attached to supported hosts.

**Support Point of Presence (SPOP)** is the ProLiant systems owned and deployed by HP to the Advanced Configuration customer site for centralized management of the customer enterprise.

## **T-Z**

**Telemetry** Telemetry refers to the event data of results of a diagnostic MAP (script) that is executed when an incident is created.



## A

AntiVirus definitions 70

## C

Client Polling failures 23  
company contact management 33  
content management web targets 58  
Contract Compare Assessments 11, 44

## D

device classification option 61  
device group  
    add 40  
    delete 41  
device name 17  
device unreachable configuration 66  
device unreachable service  
    customize 67

## E

e-mail notification  
    default 51  
Enterprise Service Console (ESC) 16  
    Enterprise View 17

## I

incident ID 17  
incident management 28  
Instant Support Enterprise Edition (ISEE)  
    supported products 13

## ISEE

    Advanced Configuration 11  
    Monitored Client 19, 23  
    Remote Connectivity 11  
    Standard Configuration 11  
    User Privileges 18

## M

MAP 21  
    Available MAPs 21  
    Definition 79  
    Source for New 24  
    View All MAPs 42  
Microsoft Internet Explorer 5.0+ 16, 26  
Mission Critical and Network customers 61

## Monitored Clients

    Advanced Configuration 11  
    Standard Configuration 11

## P

Password 19  
    management 34

## S

Schedule  
    testing 46  
Scheduled Collection 11, 20  
    Deadline 45  
    Enable 21  
    Escalation 45  
    First Run 12  
    Time-out 45  
SMTP server 23  
Software Updates  
    subscribe 77  
Support Point of Presence (SPOP)  
    Architecture Overview 11  
    Features 13  
    Users 18

## T

Terminal Services 16  
typeface conventions 4

## W

wfm ID 17