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.

*Italic*: Italicized Courier New 10 pt is used to indicate `<variable_information>` the user must enter and *[Soft Buttons]*.

Computer Output: 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]).

User Input: 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:

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:


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:
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 troubleshooting 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
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 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:

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.

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.


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>
<thead>
<tr>
<th>Role</th>
<th>Privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operator</td>
<td>Allows Server Management from the Enterprise Service Console.</td>
</tr>
<tr>
<td>Administrator</td>
<td>Allows User Management from the Enterprise Service Console.</td>
</tr>
<tr>
<td>Support Manager</td>
<td>Provides unlimited support privileges.</td>
</tr>
<tr>
<td>Senior Support Analyst</td>
<td>Provides broad support privileges.</td>
</tr>
<tr>
<td>Support Analyst</td>
<td>Allows limited support privileges.</td>
</tr>
</tbody>
</table>

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.

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 SPOP 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.

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.

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 (for 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 and/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

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

There are devices pending approval

The Enterprise View enables Support Engineers and Administrators to manage and view contacts, motive users, devices, device groups, and incident information. Please make a selection from the left to begin.
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**

<table>
<thead>
<tr>
<th>incident_id</th>
<th>wdm_id</th>
<th>opened</th>
<th>device_name</th>
<th>status</th>
<th>queue</th>
<th>problem_area</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident 41</td>
<td>1 30 2004, 12:36</td>
<td>example</td>
<td>open</td>
<td>Win2000</td>
<td>New_Installation</td>
<td>New_Installation</td>
<td></td>
</tr>
<tr>
<td>Incident 42</td>
<td>1 30 2004, 12:36</td>
<td>example</td>
<td>open</td>
<td>Win2000</td>
<td>New_Installation</td>
<td>New_Installation</td>
<td></td>
</tr>
<tr>
<td>Incident 43</td>
<td>1 30 2004, 12:36</td>
<td>example</td>
<td>open</td>
<td>Win2000</td>
<td>Enrollment_Check</td>
<td>Enrollment_Check</td>
<td></td>
</tr>
<tr>
<td>Incident 44</td>
<td>1 30 2004, 12:36</td>
<td>example</td>
<td>open</td>
<td>Win2000</td>
<td>TEST incident</td>
<td>cpg4000॥GenericTrap</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 3-4 Review This Incident**

The review this incident screen (Figure 3-4) displays incident status.
Using the Enterprise Service Console

Using the Enterprise View

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

![Review This Incident](image)

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

Figure 3-6 Review This Incident

![Review This Incident](image)
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**

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

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

**Figure 3-8 Enter Contact Information**

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**

6. Click **[next]**.

7. Select the account roles for this account (see Figure 3-10).

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

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*

<table>
<thead>
<tr>
<th>queue</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motive</td>
<td>Motive Queue</td>
</tr>
<tr>
<td>Solaris</td>
<td>Solaris Problems</td>
</tr>
<tr>
<td>Linux</td>
<td>Linux Problems</td>
</tr>
<tr>
<td>AIX</td>
<td>AIX Problems</td>
</tr>
<tr>
<td>HP-UX</td>
<td>HP-UX Problems</td>
</tr>
<tr>
<td>WinMe</td>
<td>Windows Millennium Problems</td>
</tr>
<tr>
<td>WinXP</td>
<td>WinXP Problems</td>
</tr>
<tr>
<td>Win2000</td>
<td>Windows 2000 Problems</td>
</tr>
<tr>
<td>WinNT</td>
<td>Windows NT Problems</td>
</tr>
<tr>
<td>Win98</td>
<td>Windows 98 Problems</td>
</tr>
<tr>
<td>Win95</td>
<td>Windows 95 Problems</td>
</tr>
<tr>
<td>Default</td>
<td>Default Queue</td>
</tr>
</tbody>
</table>

[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

[Default 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).

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

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).

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

Figure 3-15 View All Users

Figure 3-16 Review User Details
4. Enter and confirm the new password (see Figure 3-17).

**Figure 3-17 Enter Password Information**

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**

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**

<table>
<thead>
<tr>
<th>device details</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
</tr>
<tr>
<td>key</td>
</tr>
<tr>
<td>company name</td>
</tr>
<tr>
<td>device type</td>
</tr>
<tr>
<td>service type</td>
</tr>
<tr>
<td>model type</td>
</tr>
<tr>
<td>operating system</td>
</tr>
<tr>
<td>location</td>
</tr>
<tr>
<td>domain</td>
</tr>
<tr>
<td>status</td>
</tr>
<tr>
<td>timezone</td>
</tr>
<tr>
<td>support handle</td>
</tr>
<tr>
<td>ip address</td>
</tr>
</tbody>
</table>

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**

```plaintext
<table>
<thead>
<tr>
<th>Device Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>name</strong></td>
</tr>
<tr>
<td><strong>key</strong></td>
</tr>
<tr>
<td><strong>company name</strong></td>
</tr>
<tr>
<td><strong>device type</strong></td>
</tr>
<tr>
<td><strong>model type</strong></td>
</tr>
<tr>
<td><strong>location</strong></td>
</tr>
<tr>
<td><strong>status</strong></td>
</tr>
<tr>
<td><strong>time zone</strong></td>
</tr>
<tr>
<td><strong>ip address</strong></td>
</tr>
</tbody>
</table>
```

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

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

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

From the view all device groups page you can:

- Add devices to your new device group by checking the device name box for the selected device.
d. Click \textit{next} when you are finished subscribing devices to your new device group.

The \textit{enter device group title} screen (Figure 3-25) displays.

\textbf{Figure 3-25 Enter Device Group Title}

\begin{verbatim}
enter device group title

* Indicates Required Fields

Title

*description

[preview] [next] [finish] [cancel]
\end{verbatim}

e. Enter the \textit{title} of your new device group and a brief \textit{description} in the text box.

f. Click \textit{finish} to save your new device group.

\begin{itemize}
  \item Edit an existing device group
    a. Select the device group name you want to edit from the \textit{view all device groups} page.

\textbf{Figure 3-26 Review This Group—Devices}

\begin{verbatim}
review this group

identification

Title: test group
Description: new group

devices

device name support handle device type os ip address status

EXAMPLE not_available Windows 2000 31.6.37.93 available

[edit]
\end{verbatim}

b. Select the \textit{device name} you want to edit.

c. Change the identification and subscription list for the selected device group
   by clicking \textit{edit} on either heading from the \textit{review this group} page.
   Review step 3, \textit{Adding a New Device Group}, for more detail about these processes.

\begin{itemize}
  \item Delete an existing device group

  Click \textit{delete} on the same line as the device group that you want to remove.

  This process only deletes the \textit{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 information is 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).

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

---

**Figure 3-27  Scheduler Window**

<table>
<thead>
<tr>
<th>name</th>
<th>completed date</th>
<th>status</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAP1</td>
<td>2023-01-01</td>
<td>Available</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>name</th>
<th>map type</th>
<th>os platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAP1</td>
<td>HPUK</td>
<td>Windows 2000</td>
</tr>
<tr>
<td>MAP2</td>
<td>Linux</td>
<td>Windows 2003</td>
</tr>
<tr>
<td>MAP3</td>
<td>Solaris</td>
<td>Windows 2000</td>
</tr>
<tr>
<td>MAP4</td>
<td>Windows</td>
<td>Windows 2003</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
</tr>
<tr>
<td>Description</td>
</tr>
<tr>
<td>OS Platform</td>
</tr>
</tbody>
</table>

**Actions**

- [Schedule this MAP](#)

**Map Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter a timeout multiplication factor</td>
<td>1</td>
<td>Enter a timeout multiplication factor</td>
</tr>
</tbody>
</table>

**Map Source**

- [Show Map Source](#)

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

**Figure 3-30 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_NetworkConfigurationInformation
Addl_BusConfigurationInformation
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 \textit{add new schedule} in the left navigation list.

\textbf{Figure 3-31}  \textbf{Scheduler Activity Log}

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

\textbf{Figure 3-32}  \textbf{Select a MAP}

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

\textbf{NOTE}  To enable Contract Compare assessments, choose both the Comprehensive System Map and Additional Mission Critical Collectibles.

5. Click \textit{[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

11. Click [next].

12. Enter a title and a description for your schedule.

Figure 3-36  Enter Schedule Title

13. Click [finish].
The view all schedules screen (Figure 3-37) displays showing the schedule you created.

**Figure 3-37  View All Schedules**

<table>
<thead>
<tr>
<th>name</th>
<th>description</th>
<th>occurrences remaining</th>
<th>actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>LP Test 3</td>
<td>LP Test</td>
<td>1</td>
<td>suspend</td>
</tr>
</tbody>
</table>

**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).
Using the Enterprise Service Console
Using the Scheduler

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

- Command1.properties.bat: d:

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

```
25125227-6503-0047-7547-BF3BFB00000
```

#### Standard Out:

```
```

#### Standard Error:

```
```

#### Script Log:

```
THIS SCRIPT IS BEING RUN BY \nEXECUTING C:\WINNT\TEMP\hpservices\399\properties.bat -d
```

---

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**

```
```

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

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.
Using the Enterprise Service Console
Using the Scheduler

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

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](image)

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

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**

<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adapter/Controlleradapter.FailAdapt</td>
<td>true</td>
</tr>
</tbody>
</table>

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**

   ![HP Tools Screen](image)

   2. Select Content Version Management.
      The content version management screen (Figure 3-54) displays.

   **Figure 3-54 Content Version Management**

   ![Content Version Management Screen](image)

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

   ![Notification](image)
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

![HP Tools](image)

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

#### Figure 3-56  Content Version Management

![Content Version Management](image)
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.

2. Click 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](image)

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.
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.

![Unreachable Device Configuration](image)

**Figure 3-61 Unreachable Device Configuration**

<table>
<thead>
<tr>
<th>parameter</th>
<th>current value</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create an alert</td>
<td>yes</td>
<td>Defines whether an IDEE incident should be created when the status of a device changes.</td>
</tr>
<tr>
<td>Notify Email</td>
<td>yes</td>
<td>Defines whether an email should be sent to the configured recipients when the status of a device changes.</td>
</tr>
<tr>
<td>Create Problem Notifications</td>
<td>yes</td>
<td>Defines whether a notification should be created when devices become reachable. In addition to the unreachable notifications.</td>
</tr>
<tr>
<td>Notification Frequency</td>
<td>1 min</td>
<td>The frequency for E/CDR service to poll a device to determine its state.</td>
</tr>
<tr>
<td>Unreachable Threshold</td>
<td>2 polls</td>
<td>The number of consecutive polls for the device to be unreachable before an unreachable notification is created.</td>
</tr>
<tr>
<td>SNMP Community</td>
<td>none</td>
<td>The SNMP community name used in polling SNMP-capable devices.</td>
</tr>
</tbody>
</table>

[Table 3-6 Unreachable Device Configuration Parameters]
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.

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.

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.

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.

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.

2. Click [edit settings].

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

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

Figure 3-66 Global Default Settings Section

<table>
<thead>
<tr>
<th>parameter</th>
<th>default value</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create Incident</td>
<td>yes</td>
<td>Defines whether an SIE incident should be created to notify the HP Support Center when the status of a device changes.</td>
</tr>
<tr>
<td>Notify Email</td>
<td>yes</td>
<td>Defines whether an email should be sent to the configured recipients when the status of a device changes.</td>
</tr>
<tr>
<td>Create Reachable notifications</td>
<td>yes</td>
<td>Defines whether a notification should be created when devices become reachable, in addition to the unreachable notifications.</td>
</tr>
<tr>
<td>Polling Frequency</td>
<td>1 min</td>
<td>The frequency the DPA server should poll a device to determine its state.</td>
</tr>
<tr>
<td>Reachable Threshold</td>
<td>2 polls</td>
<td>The number of consecutive polls for the device to be reachable before a reachable notification is created.</td>
</tr>
<tr>
<td>SNMP Community Name</td>
<td>SNMPP community name used in polling SNMP-capable devices.</td>
<td></td>
</tr>
</tbody>
</table>

Figure 3-67 Modify Global Default Settings Windows

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.

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

<table>
<thead>
<tr>
<th>device name</th>
<th>description</th>
<th>enabled?</th>
<th>settings</th>
<th>Email Address (default)</th>
</tr>
</thead>
<tbody>
<tr>
<td>monolith</td>
<td></td>
<td>yes</td>
<td>Customized Settings</td>
<td>Email Address (default)</td>
</tr>
<tr>
<td></td>
<td>build and test system</td>
<td></td>
<td>Polling Frequency 10 min.</td>
<td>Maintenance Windows Daily 00:00 to 03:01 (default)</td>
</tr>
<tr>
<td>MON01</td>
<td></td>
<td>yes</td>
<td>Customized Settings</td>
<td>Email Address (default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Maintenance Windows Daily 11:00 to 11:01 (default)</td>
</tr>
<tr>
<td>pepper</td>
<td></td>
<td>yes</td>
<td>Customized Settings</td>
<td>Email Address (default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Maintenance Windows Daily 00:00 to 00:01 (default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Weekly 00:00 to 00:01 (default)</td>
</tr>
<tr>
<td>splash</td>
<td></td>
<td>yes</td>
<td>Customized Settings</td>
<td>Email Address (default)</td>
</tr>
<tr>
<td></td>
<td>system</td>
<td></td>
<td></td>
<td>Maintenance Windows</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Daily 00:00 to 00:01 (default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Weekly 00:00 to 00:01 (default)</td>
</tr>
<tr>
<td>SPL223</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
3. Modify the appropriate settings, and click [save] to return to the device unreachable configuration window.

Figure 3-69  Modify Device Settings Window
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


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

**Figure 4-2  SPOP Server Details**

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

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

5. Use the browser's **[Refresh]** button to monitor the progress.

6. 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

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.

   ![Logging into the Software Management Tool](image)

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

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.
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.
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