Threshold and Event Generation Module

Software Version: 5.10

HP Performance Insight 5.40

User Guide

February 2009

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

© Copyright 2002 - 2009 Hewlett-Packard Development Company, L.P.

This product includes Xerces XML Java Parser software, which is Copyright (c) 1999 The Apache Software Foundation. All rights reserved.

This product includes JDOM XML Java Parser software, which is Copyright (C) 2000-2003 Jason Hunter & Brett McLaughlin. All rights reserved.

This product includes JClass software, which is (c) Copyright 1997, KL GROUP INC. ALL RIGHTS RESERVED.

This product includes J2TablePrinter software, which is © Copyright 2001, Wildcrest Associates (http://www.wildcrest.com)

This product includes Xalan XSLT Processor software, which is Copyright (c) 1999 The Apache Software Foundation. All rights reserved.

This product includes EXPAT XML C Processor software, which is Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd and Clark Cooper Copyright (c) 2001, 2002 Expat maintainers.

This product includes Apache SOAP software, which is Copyright (c) 1999 The Apache Software Foundation. All rights reserved.

This product includes O'Reilley Servlet Package software, which is Copyright (C) 2001-2002 by Jason Hunter, jhunter_AT_servlets.com.All rights reserved.

This product includes HTTPClient Package software, which is Copyright (C) 1991, 1999 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

This product includes Perl software, which is Copyright 1989-2002, Larry Wall. All rights reserved.

This product includes Skin Look And Feel software, which is Copyright (c) 2000-2002 L2FProd.com. All rights reserved.

This product includes nanoXML software, which is Copyright (C) 2000 Marc De Scheemaecker, All Rights Reserved.

This product includes Sixlegs PNG software, which is Copyright (C) 1998, 1999, 2001 Chris Nokleberg

This product includes cURL & libcURL software, which is Copyright (c) 1996 - 2006, Daniel Stenberg, <daniel@haxx.se>. All rights reserved.

This product includes Quartz - Enterprise Job Scheduler software, which is Copyright 2004-2005 OpenSymphony

This product includes Sixlegs PNG software, which is Copyright (C) 1998, 1999, 2001 Chris Nokleberg

This product includes cURL & libcURL software, which is Copyright (c) 1996 - 2006, Daniel Stenberg, <daniel@haxx.se>. All rights reserved.

This product includes Quartz - Enterprise Job Scheduler software, which is Copyright 2004-2005 OpenSymphony

This product includes Free DCE software, which is (c) Copyright 1994 OPEN SOFTWARE FOUNDATION, INC., (c) Copyright 1994 HEWLETT-PACKARD COMPANY, (c) Copyright 1994 DIGITAL EQUIPMENT CORPORATION, Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

This product includes DCE Threads software, which is Copyright (C) 1995, 1996 Michael T. Peterson

This product includes Jboss software, which is Copyright 2006 Red Hat, Inc. All rights reserved.

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

Trademark Notices

Java™ is a U.S. trademark of Sun Microsystems, Inc. Java™ and all Java based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Oracle® is a registered U.S. trademark of Oracle Corporation, Redwood City, California.

UNIX® is a registered trademark of The Open Group.

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

Documentation Updates

This guide's title page contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

http://h20230.www2.hp.com/selfsolve/manuals

This site requires that you register for an HP Passport and sign-in. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

You can visit the HP Software Support Online web site at:

http://www.hp.com/go/hpsoftwaresupport

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software Support Online provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the HP Software Support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

Contents

1 Overview

The Threshold and Event Generation Module monitors database tables for threshold conditions. The database queries that detect threshold conditions can be executed frequently, as frequently as new data is added to the database tables. When a query detects a threshold condition, the Thresholds Module logs an event and takes an action. The event log indicates the object, the time, and the data values that triggered the event. The action is configurable. The default action is to send a generic SNMP trap to an external system. If desired, you can use forms to configure additional actions, such as sending email notification or calling a program that you created.

The Thresholds Module contains three packages:

- Thresholds
- ThresholdsRP (Thresholds Report Pack)
- ThresholdsExample

Installing theThresholds package is mandatory. Installing the other two packages is optional. The Thresholds package contains:

- thresholds.pl, the core processing script responsible for reading threshold definition files, formulating database queries, and detecting threshold conditions
- Three create action definition forms
- Three update action definition forms
- Data tables for storing data about threshold events
- Property tables for storing data about configured actions

ThresholdsRP contains templates and processing routines for two reports. If you install this package, you can aggregate threshold event data by category, severity, and object and view threshold events on an hourly, daily, and monthly basis. You can also see threshold events as they occur by launching the recent events report. This report begins with the most recent time period and goes back in time.

The ThresholdExamples package is designed to illustrate the operation of the Thresholds Module. If you do not want the additional processing load on your system, do not install the ThresholdsExample package. If you install it, database tables will be populated with test data. The test data will generate threshold conditions, and the Thresholds package will respond to those conditions by sending SNMP traps to the local host.

Role of the Thresholds Sub-Package

Some report packs include a separate, optional thresholds sub-package. The thresholds sub-package defines a thresholds policy for the report pack. If you want to implement thresholding for the report pack, you must install the thresholds sub-package. Every thresholds sub-package contains threshold definitions files, a procedure file, and entries for

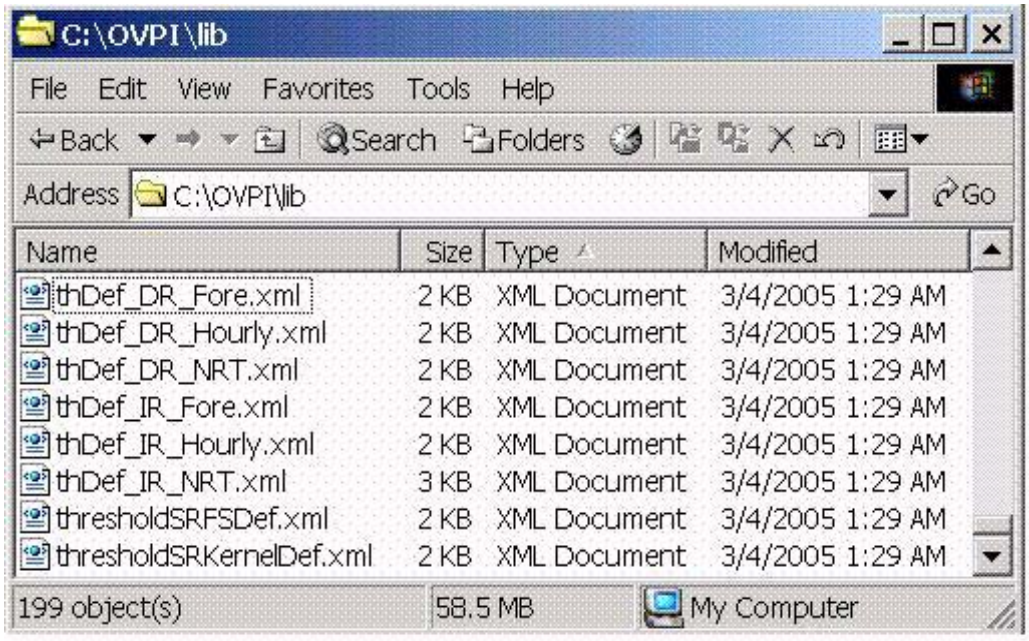
trendtimer.sched. When a thresholds sub-package is installed, the threshold definition files are copied to {DPIPE_HOME}/lib directory, the procedure file is copied to {DPIPE_HOME}/scripts, and the trendtimer entries are added to trendtimer.sched.

When PI calls the procedure file in the scripts directory, the following events take place:

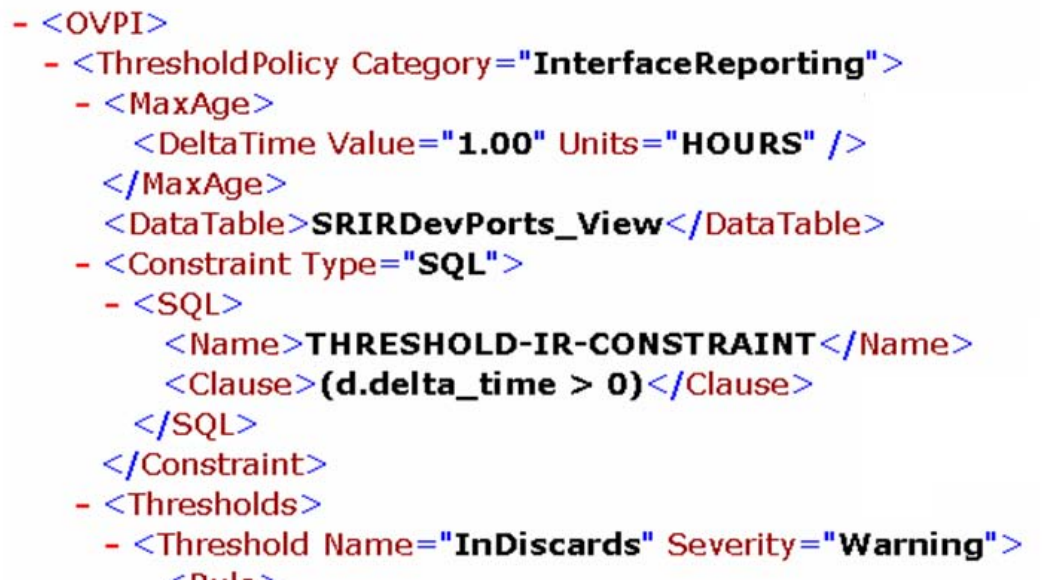
1. The procedure file calls thresholds.pl.
2. thrsholds.pl reads the threshold definition file and queries the database table.
3. thresholds.pl stores the current threshold status in a temporary table.
4. If thresholds.pl detects a threshold condition, it updates an event log.
5. The next time the same query runs, thresholds.pl compares the current threshold status to previous threshold status.
6. If a status change is detected, thresholds.pl determines if the category and severity of the new status matches a configured action.
7. If the new status matches a configured action, the script initiates that action.

Opening a Threshold Definition File

The next screen shot shows a list of threshold definitions files in the {DPIPE_Home}/lib directory. The list of files includes multiple threshold definitions files for multiple report packs, including Device Resources, Interface Reporting, and System Resources.



Use any web browser or any editor to open a threshold definition file. Following is a sample threshold definition file.



You can use any XML editor or any text editor to modify a threshold definition file. You can also create your own threshold definition files. For details about that process, see Chapter 5, Creating a Thresholds Policy.

Configuring Optional Actions

Configuring the Thresholds Module is optional. Once the package is installed, the Thresholds Module will read threshold definition files and detect threshold conditions without any user intervention. In addition, the Thresholds Module will take two default actions without any user intervention. The default actions are:

- When a threshold is breached, send an *ovpiThrehsoldBreach* trap to NNM
- When a threshold condition clears, send an *ovpiThresholdClear* trap to NNM

Configuring the Thresholds Module means creating additional actions and, if necessary, modifying the actions you created. You can configure the Thresholds Module to take the following actions:

- Send an SNMP trap
- Send SMTP email (in batch mode, after every exception has been processed)
- Call a user-defined program

You can configure a single threshold condition to trigger one action or multiple actions. For example, you could configure the Thresholds Module to take three actions — send a trap, send an email, and call to a user-defined program — in response to the same condition. To create a new action, or modify an existing action, use a form. You can get to the new forms by selecting **Objects > File > New** from the Management Console. The update forms are listed under **Objects > General Tasks** in the Management Console.

Recent Enhancements and Fixes

The following table describes recent enhancements and defect fixes.

Version/Release Date	Enhancements/Defect Fixes
5.00, April 2004	Upgrade package (4.00 to 5.00) Oracle support added
5.10, April 2007	Upgrade package (4.00/5.00 to 5.10) Defect fixes: • QXCR1000321540 — Remove_thresh_tables.pl does not work • QXCR1000318772 — Threshold reporting does not distinguish between ARM and RE-ARM events
5.10, February 2009	Defect fix: • QXCR1000318772 - Threshold Reporting Does Not Distinguish Between ARM and RE-ARM events

Sources for Additional Information

For the latest information regarding known problems affecting the Thresholds Module, see:

Threshold and Event Generation Module 5.10 Release Statement

For information about default thresholds in the threshold sub-package that comes with each report pack, refer to the user guide for the report pack. Manuals for the core product, PI, and manuals for the report packs that run on PI, can be downloaded from here:

http://h20230.www2.hp.com/selfsolve/manuals

The user guides for PI are listed under **Performance Insight**. The user guides for report packs and datapipes are listed under **Performance Insight Reporting Solutions**. The entry for a manual indicates the month and year it was posted to the web. If a manual is revised and reposted, the date will change. Since revised manuals are reposted from time to time, be sure to compare your PDF to the web edition and download the web edition if it is newer.

2 Package Installation

The Thresholds Module is a prerequisite for the threshold sub-packages that come with most report packs. This means that if you install any thresholds sub-package, Package Manager will install the Thresholds Module for you, automatically. Although automatic installation is fast and easy, you also have the option of installing the Thresholds Module before you install any report packs. If that is the approach you are taking, follow the procedure in this chapter.

This chapter covers the following topics:

Software Prerequisites

Make sure the following platform software is already installed before installing the Threshold and Event Generation Module:

- PI 5.10 with the latest Service Pack, or
- PI 5.20

At a minimum you want PI 5.10 with Service Pack 5, since Service Pack 5 includes defect fixes that pertain to the Threshold and Event Generation Module. You can download Service Pack 5 from this site:

http://support.openview.hp.com/cpe/ovpi/patch_ovpi.jsp

For details about the fixes contained in Service Pack 5, refer to the release notes. The release notes are posted here:

http://ovweb.external.hp.com/lpe/doc_serv/

When the Product Manual Search page opens, scroll down the list of products until you come to **Performance Insight.** Select version 5.10 and then look for the release notes in the list of user documentation.

Upgrading from an Earlier Release

If you are currently running version 4.00 or version 5.00, you can easily upgrade to version 5.10 by installing the following upgrade package:

Thresholds_Upgrade_to_51

If you are running an older version of this software, a pre-4.00 version, you cannot upgrade to version 5.10. Instead, you must uninstall your current version and then install version 5.10. Note that uninstalling the Thresholds Module will also uninstall any dependent packages. The dependent packages are the thresholds sub-packages you installed when you installed report packs.

Installing Thresholds Module 5.10

The report pack CD-ROM contains the latest report packs, datapipes, and shared packages. When you insert the report pack CD in the drive and launch the package extraction program, the install script extracts every package from the CD and copies the results to the Packages directory on your system. When the extract finishes, the install script prompts you to launch PI and start Package Manager.

Follow these steps to install the Thresholds Module 5.10 before installing any report packs:

- Task 1: Extract report packs, datapipes, and shared packages from the report pack CD
- Task 2: Start Package Manager and follow the prompts
- Task 3: Restart OVPI Timer

Task 1: Extract packages from the report pack CD.

1. Log in to the system. On UNIX® systems, log in as root.
2. Stop OVPI Timer and wait for processes to terminate.

   On Windows, do the following:

   a. Select **Control Panel > Administrative Tools > Services**
   b. Select OVPI Timer from the list of services.
   c. From the Action menu, select **Stop**.

   On UNIX, as root, do one of the following:

   — HP-UX: **`sh /sbin/init.d/ovpi_timer stop`**
   — Sun: **`sh /etc/init.d/ovpi_timer stop`**
3. Insert the report pack CD in the CD-ROM drive.

   Windows: The package extraction interface opens automatically.

   UNIX:

   a. Mount the CD (if the CD does not mount automatically).
   b. Navigate to the top level directory on the CD.
   c. Run **`./setup`**
4. Type **1** in the choice field and press **Enter**. The install script displays a percentage complete bar. When the copy is complete, the install script starts Package Manager. The Package Manager Welcome window opens.

Task 2: Install Thresholds Module 5.10.

1. Click **Next.** The Package Location window opens.
2. Click **Install**; approve the default installation directory, or select a different directory if necessary.
3. Click **Next**. The Report Deployment window opens. Accept the option to Deploy Reports.

   The create action definition forms, the update action definition forms, and the two reports in the report pack will not deploy unless you accept the Deploy Reports option.

4. Type your username and password for the PI Application Server.
5. Click **Next**. The Package Selection window opens.
6. Click the check box next to the following items:
   - *Thresholds*
   - *ThresholdExample* (optional)
   - *ThresholdsRP* (optional)
7. Click **Next**. The Type Discovery window opens; disable the Type Discovery option.
8. Click **Next**. The Selection Summary window opens.
9. Click **Install**. The Installation Progress window opens. When installation is complete, a package installation complete message appears.
10. Click **Done**.

Task 3: Restart OVPI Timer.

On Windows, do the following:

a. Select **Control Panel > Administrative Tools > Services**
b. Select OVPI Timer from the list of services.
c. From the Action menu, select **Start**.

On UNIX, as root, do one of the following:

- HP-UX: **`sh /sbin/init.d/ovpi_timer start`**
- Sun: **`sh /etc/init.d/ovpi_timer start`**

Verifying Proper Installation

To verify that the Threshold and Event Generation Module and all the prerequisites have been installed correctly, run one of the following commands.

UNIX:

```
$DPIPE_HOME/bin/perl $DPIPE_HOME/scripts/thresholds.pl -h
```

Windows:

```
%DPIPE_HOME%\bin\perl %DPIPE_HOME%\scripts\thresholds.pl -h
```

The system returns a usage-is statement similar to the following:

```
D:/OVPI/scripts/thresholds.pl -f <rulesfile> [-d]
```

where:

`<rulesfiles>` is an XML threshold rules definition file

`-d` enables the debug mode

The default action file is `{DPIPE_HOME}/lib/threshAct.xml`

If you do not see this statement, see Chapter 6, Troubleshooting.

Uninstalling Thresholds Module 5.10

If you uninstall the Thresholds Module, Package Manager will automatically uninstall any thresholds sub-package depends on the Thresholds Package.

Follow these steps to uninstall Threshold and Event Generation Module 5.10:

1. Log in to the system. On UNIX systems, log in as root.
2. Stop OVPI Timer and wait for processes to terminate.

   On Windows, do the following:

   a. Select **Control Panel > Administrative Tools > Services**
   b. Select OVPI Timer from the list of services.
   c. From the Action menu, select **Stop**.

   On UNIX, as root, do one of the following:

   - HP-UX: **`sh /sbin/init.d/ovpi_timer stop`**
   - Sun: **`sh /etc/init.d/ovpi_timer stop`**
3. Start Package Manager. The Package Manager welcome window opens.
4. Click **Next**. The Package Location window opens.
5. Click **Uninstall**.
6. Click **Next**. The Report Undeployment window opens. Keep the defaults.
7. Click **Next**. The Package Selection window opens. Click the check box next to:
   - *Thresholds*
   - *ThresholdExample* (if installed)
   - *ThresholdsRP* (if installed)
8. Click **Next**. The Selection Summary window opens.
9. Click **Uninstall**. The Progress window opens. When removal is complete, a package removal complete message appears.
10. Click **Done**.

11 Restart OVPI Timer.

On Windows, do the following:

a Select **Control Panel > Administrative Tools > Services**

b Select OVPI Timer from the list of services.

c From the Action menu, select **Start**.

On UNIX, as root, do one of the following:

— HP-UX: **`sh /sbin/init.d/ovpi_timer start`**

— Sun: **`sh /etc/init.d/ovpi_timer start`**

3 Configuring Actions

This chapter covers the following topics:

Using Forms to Modify Thresholds

Many PI report packs are distributed with a thresholds sub-package. The thresholds sub-package establishes a threshold policy for the report pack. If you want to modify a report pack's threshold policy, there is no need to modify the thresholds sub-package. Instead, modify the policy by using the threshold change forms that come with the thresholds sub-package.

You also have the option of setting new threshold limits for some or all of the objects you are monitoring by using the provisioning interface that comes with the report pack. The forms tend to be easier and faster than the provisioning interface. If you want to use the provisioning interface, you must export existing property data from runPI, edit the file by inserting new values, and then re-import the file into PI.

Using Forms to Create and Update Actions

Forms are available for creating and updating action definitions. To access forms, launch the Management Console and select the **Objects** icon. You can access the following create forms by selecting **File > New**:

- Create SNMP Trap Action
- Create SMTP Mail Action
- Create User Script Action Definition

You will find the following update forms listed under **Objects > General Tasks:**

- Update SNMP Trap Action
- Update SMTP Mail Action
- Update User Script Action Definition

Category Value

The category value is a type of event that will cause an action to occur. The category value is case sensitive. You can set this value to any non-null single word value *without* embedded spaces. Using special characters (punctuation marks, quotes, hash symbols) is not recommended, since such characters may have special meaning for third party systems. Wildcarding, by using an asterisk (*) to match all categories, is allowed.

Severity Value

The severity value indicates the severity of an event that will cause an action to occur. Severity level is case sensitive. Severity value can be set to any non-null single word value *without* embedded spaces. Whenever possible, use values that match the severity levels used by other systems. For example, if you are sending traps to a network management system that assigns CRITICAL, HIGH, MEDIUM, or LOW to each trap, use these values. Using special characters (punctuation marks, quotes, hash symbols) is not recommended, since such characters may have a special meaning for third party systems. Wildcarding, by using an asterisk (*) to match all severities, is allowed.

Default Actions

A default action is an action that will occur for all exceptions no matter what the category or severity values are. A default action has wildcards (*) in the category and severity fields.

One default action is added to the database during package installation. This default action is to send an SNMP trap to port 162 on the local system using a community string set to *public*. If you want to send traps to a different destination, if you want to use a nonstandard SNMP port, or if you want to use a different community string, open the Update SNMP Trap Action Definition form and modify the values for server, port, or community.

If desired, you may create an additional default action. For example, you can create a user script default action definition by typing the wildcard symbol (*) in the category and severity fields on the Create User Script Action Definition form.

Creating and Modifying Action Definitions

You can define multiple actions. For example, you may send traps to more than one system, or you may send both email and traps for the same exception. You can define the following types of actions:

- SNMP Trap
- SMTP Mail
- User Script

After you create an action definition, you can modify it using the Update SNMP Trap Action Definition form.

Disabling Actions

You can disable actions, but they will remain in the database in case you want to enable them in the future. For instructions, see Disabling an Action on page 33.

Supported Actions

Three actions are supported. Each action requires a set of parameters.

Action 1: SNMP-TRAP

Parameters

- Server
  - The name or address of a server to send traps to. If an address is used it must be resolvable to an IP address.
- Port
  - A numeric port number.
- Community
  - A community string.

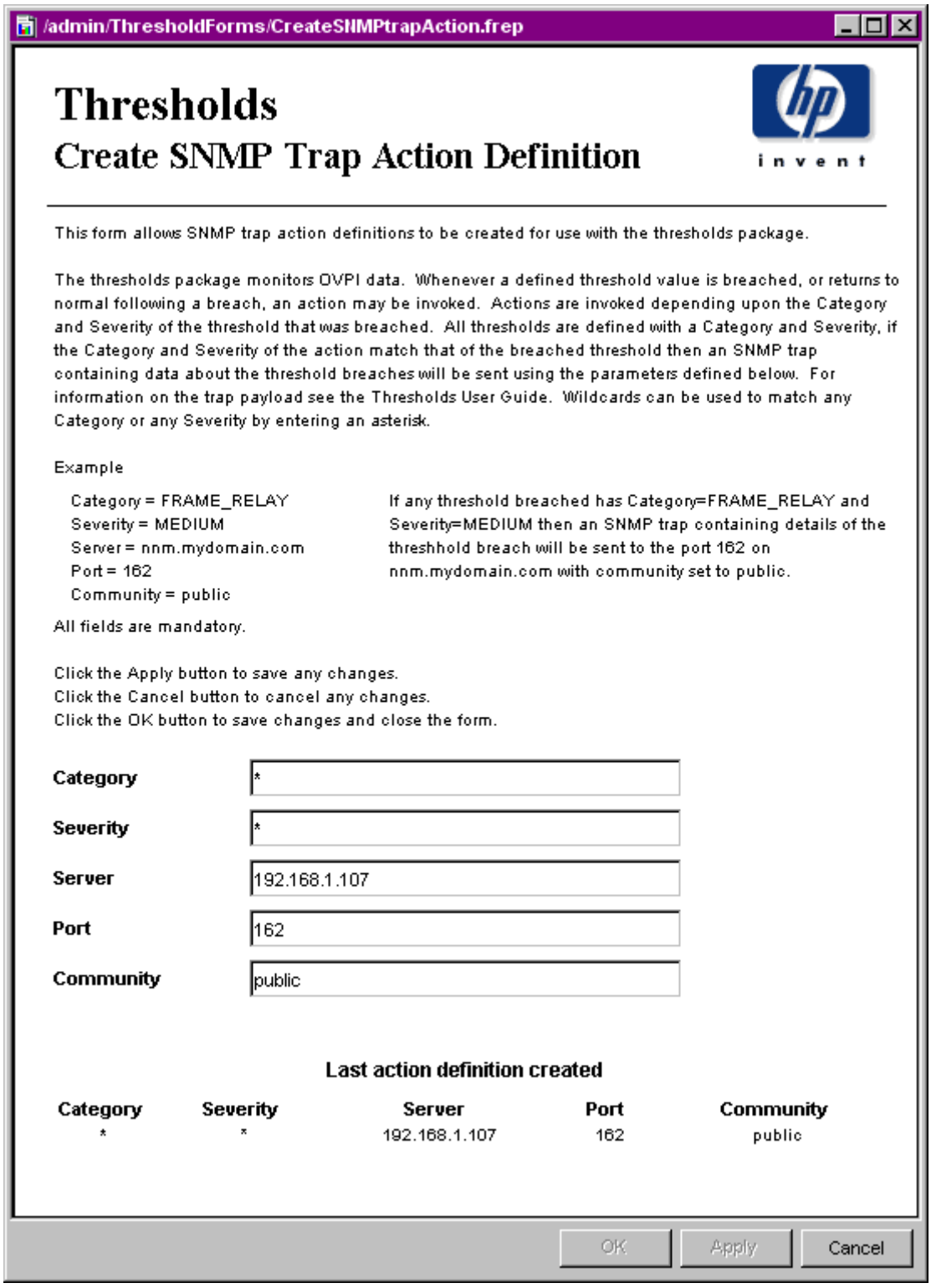
An SNMP trap is sent to the specified server and port using the specified community string.

The ovpiThresholdBreach trap is sent when a threshold is breached. The ovpiThresholdClear trap is sent when the condition returns to normal. Details about the exception are stored in trap variables. The package includes a MIB that defines ovpiThresholdBreach and ovpiThresholdClear traps.

Creating SNMP Trap Actions

To create an SNMP trap action, use the Create SNMP Trap Action Definition form. Follow these steps to launch the form:

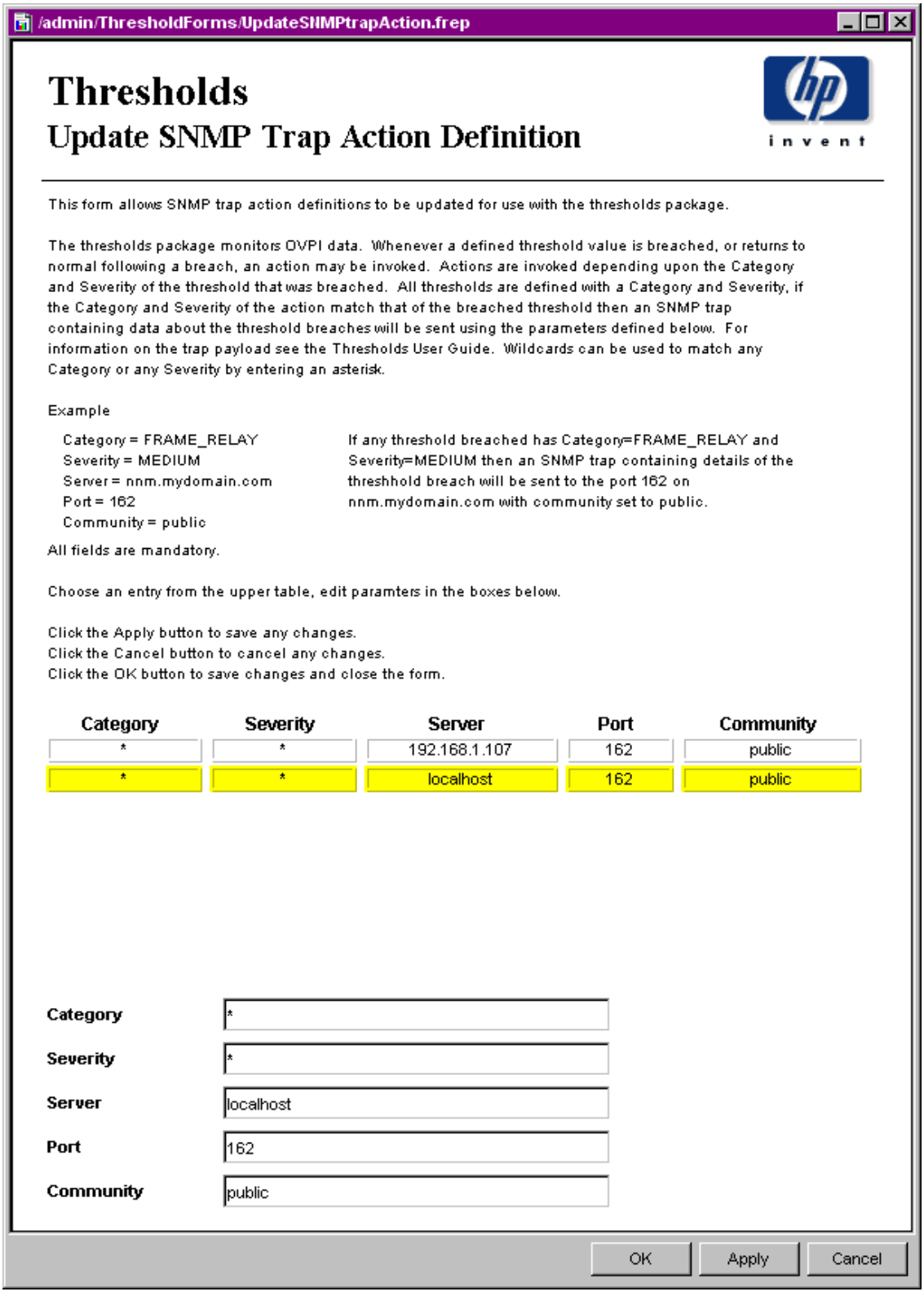
1. In the Management Console, click the **Objects** icon.
2. Select **File > New**.
3. Select **Create SNMP Trap Action** and click **Create**.
4. Follow the instructions on the form.
5. When you finish, click **OK**.


/admin/ThresholdForms/CreateSNMPtrapAction.frep
Thresholds
Create SNMP Trap Action Definition
invent
This form allows SNMP trap action definitions to be created for use with the thresholds package.
The thresholds package monitors OVPI data. Whenever a defined threshold value is breached, or returns to normal following a breach, an action may be invoked. Actions are invoked depending upon the Category and Severity of the threshold that was breached. All thresholds are defined with a Category and Severity, if the Category and Severity of the action match that of the breached threshold then an SNMP trap containing data about the threshold breaches will be sent using the parameters defined below. For information on the trap payload see the Thresholds User Guide. Wildcards can be used to match any Category or any Severity by entering an asterisk.
Example
Category = FRAME_RELAY
Severity = MEDIUM
Server = nnm.mydomain.com
Port = 162
Community = public
If any threshold breached has Category=FRAME_RELAY and Severity=MEDIUM then an SNMP trap containing details of the threshhold breach will be sent to the port 162 on nnm.mydomain.com with community set to public.
All fields are mandatory.
Click the Apply button to save any changes.
Click the Cancel button to cancel any changes.
Click the OK button to save changes and close the form.
Category
*
Severity
*
Server
192.168.1.107
Port
162
Community
public
Last action definition created
Category
Severity
Server
Port
Community
*
*
192.168.1.107
162
public
OK
Apply
Cancel

Updating SNMP Trap Actions

To modify an existing SNMP trap action, use the Update SNMP Trap Action Definition form. Follow these steps to launch the form:

1. In the Management Console, click the **Objects** icon.
2. Select an object; the **General Tasks** pane is updated.
3. Under **General Tasks**, double-click **Update SNMP Trap Action**. The form opens.
4. Click the desired action definition from the list of actions near the center of the form. The boxes in the bottom section of the form display the action definition parameters.
5. Modify the desired parameters.
6. When you finish making changes, click **OK**.


/admin/ThresholdForms/UpdateSNMPtrapAction.frep
Thresholds
Update SNMP Trap Action Definition
invent
This form allows SNMP trap action definitions to be updated for use with the thresholds package.
The thresholds package monitors OVPI data. Whenever a defined threshold value is breached, or returns to normal following a breach, an action may be invoked. Actions are invoked depending upon the Category and Severity of the threshold that was breached. All thresholds are defined with a Category and Severity, if the Category and Severity of the action match that of the breached threshold then an SNMP trap containing data about the threshold breaches will be sent using the parameters defined below. For information on the trap payload see the Thresholds User Guide. Wildcards can be used to match any Category or any Severity by entering an asterisk.
Example
Category = FRAME_RELAY
Severity = MEDIUM
Server = nnm.mydomain.com
Port = 162
Community = public
If any threshold breached has Category=FRAME_RELAY and Severity=MEDIUM then an SNMP trap containing details of the threshhold breach will be sent to the port 162 on nnm.mydomain.com with community set to public.
All fields are mandatory.
Choose an entry from the upper table, edit paramters in the boxes below.
Click the Apply button to save any changes.
Click the Cancel button to cancel any changes.
Click the OK button to save changes and close the form.
Category
Severity
Server
Port
Community
*
*
192.168.1.107
162
public
*
*
localhost
162
public
Category
*
Severity
*
Server
localhost
Port
162
Community
public
OK
Apply
Cancel

Action 2: SMTP-MAIL

Parameters

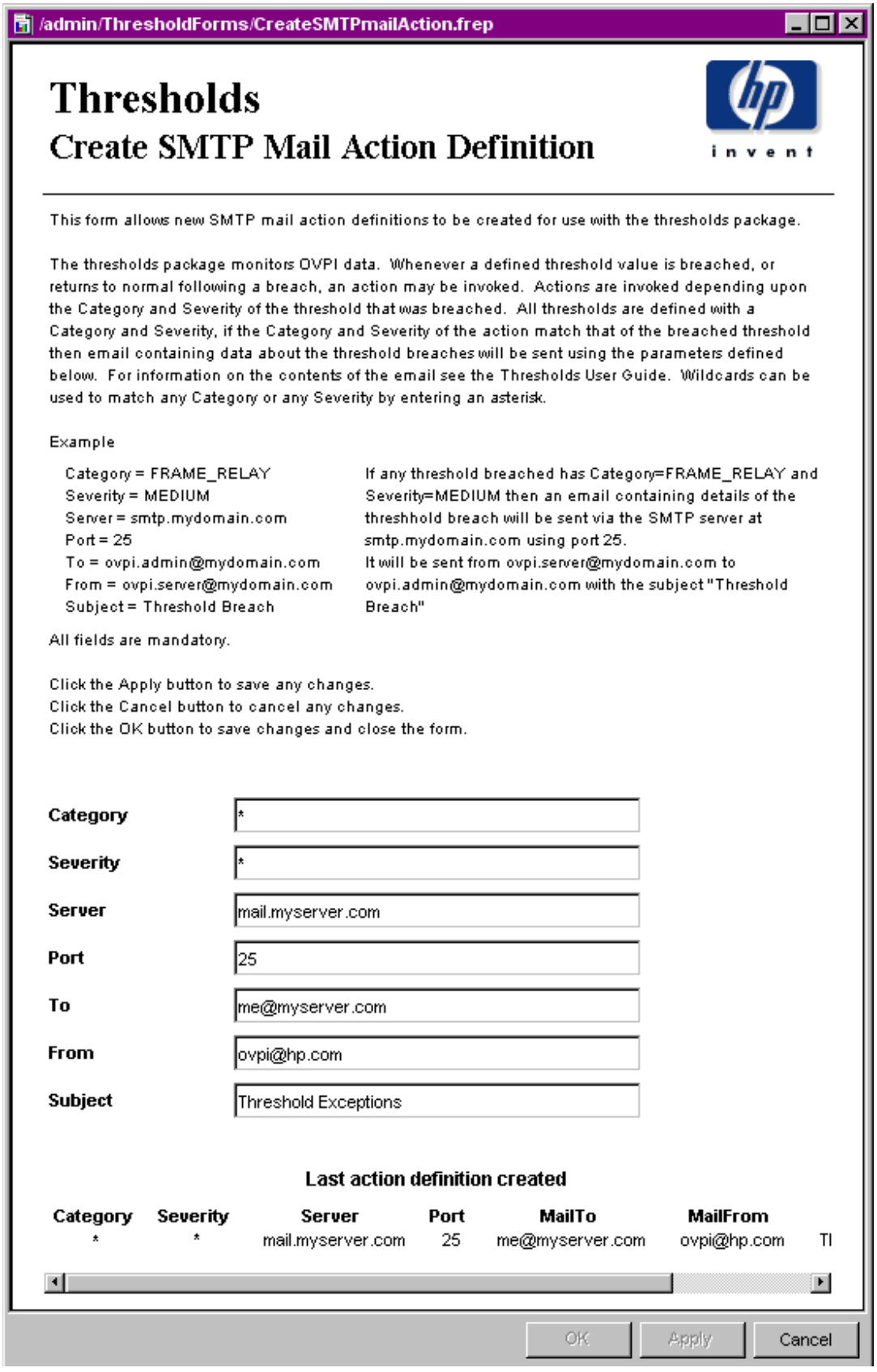
- Server
  - The name or address of an SMTP server which can be used to send email. If an address is used it must be resolvable to an IP address
- Port
  - A numeric port number. The default port for SMTP is 25 but you must check what is used by your server.
- To
  - The address to send email to. This must be a valid email address as defined by your email server, most insist on an internet style *name@domain.com* format.
  - Multiple addresses are not supported, use multiple action definitions to achieve this functionality.
  - Embedded spaces are not permitted in email addresses and may cause messages to fail.
- From
  - The address of the email sender. This must be a valid email address as defined by your email server, most insist on an internet style *name@domain.com* format.
  - Embedded spaces are not permitted in email addresses and may cause messages to fail.
- Subject
  - The subject line for the email which can be include an arbitrary string (including spaces) up to 64 characters long.

An email is sent using the specified SMTP server details. No authentication is used, because the assumption is that the SMTP server will be set up to allow unauthenticated mail from PI. The email contains a copy of the exception variables in a CSV-like format. One email message, containing details of all applicable breaches and clears, will be sent for each combination of category, severity and email address defined.

Creating SMTP Mail Actions

To create an SMTP mail action, use the Create SMTP Mail Action Definition form. Follow these steps to launch the form:

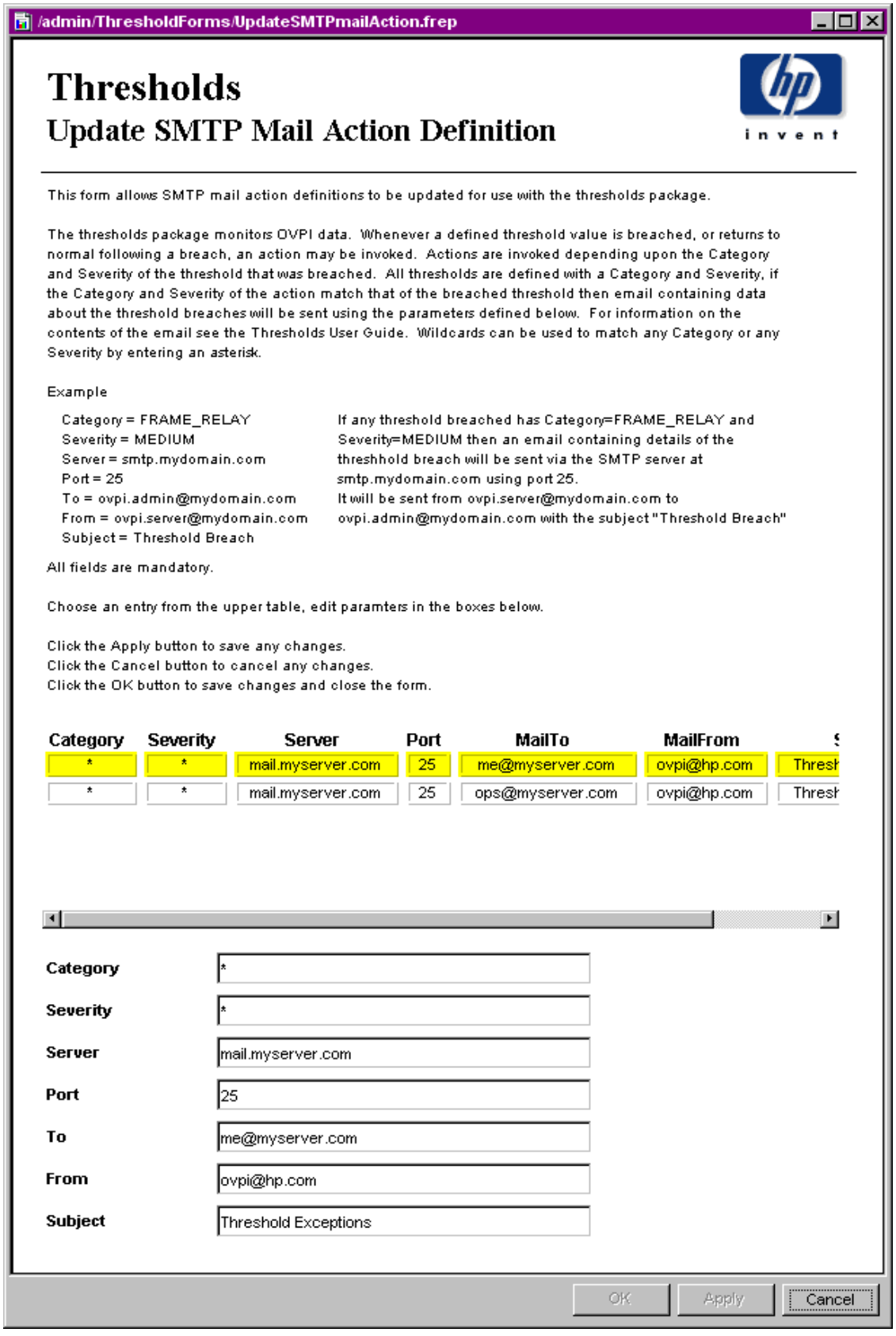
1. In the Management Console, click the **Objects** icon.
2. Select **File > New**.
3. Select **Create SMTP Mail Action** and click **Create**.
4. Follow the instructions on the form.
5. When you finish, click **OK**.


/admin/ThresholdForms/CreateSMTPmailAction.frep
Thresholds
Create SMTP Mail Action Definition
invent
This form allows new SMTP mail action definitions to be created for use with the thresholds package.
The thresholds package monitors OVPI data. Whenever a defined threshold value is breached, or returns to normal following a breach, an action may be invoked. Actions are invoked depending upon the Category and Severity of the threshold that was breached. All thresholds are defined with a Category and Severity, if the Category and Severity of the action match that of the breached threshold then email containing data about the threshold breaches will be sent using the parameters defined below. For information on the contents of the email see the Thresholds User Guide. Wildcards can be used to match any Category or any Severity by entering an asterisk.
Example
Category = FRAME_RELAY
Severity = MEDIUM
Server = smtp.mydomain.com
Port = 25
To = ovpi.admin@mydomain.com
From = ovpi.server@mydomain.com
Subject = Threshold Breach
If any threshold breached has Category=FRAME_RELAY and Severity=MEDIUM then an email containing details of the threshhold breach will be sent via the SMTP server at smtp.mydomain.com using port 25. It will be sent from ovpi.server@mydomain.com to ovpi.admin@mydomain.com with the subject "Threshold Breach"
All fields are mandatory.
Click the Apply button to save any changes.
Click the Cancel button to cancel any changes.
Click the OK button to save changes and close the form.
Category
*
Severity
*
Server
mail.myserver.com
Port
25
To
me@myserver.com
From
ovpi@hp.com
Subject
Threshold Exceptions
Last action definition created
Category Severity Server Port MailTo MailFrom
* * mail.myserver.com 25 me@myserver.com ovpi@hp.com TI
OK
Apply
Cancel

Updating SMTP Mail Actions

To modify an existing SMTP mail action, use the Update SMTP Mail Action Definition form. Follow these steps to launch the form:

1. In the Management Console, click the **Objects** icon.
2. Select an object so that the **General Tasks** pane is updated.
3. Under **General Tasks**, double-click **Update SMTP Mail Action**. The form opens.
4. Click the desired action definition from the list of actions near the center of the form. The boxes in the bottom section of the form display the action definition parameters.
5. Modify the desired parameters.
6. When you finish making changes, click **OK**.


/admin/ThresholdForms/UpdateSMTPmailAction.frep
Thresholds
Update SMTP Mail Action Definition
invent
This form allows SMTP mail action definitions to be updated for use with the thresholds package.
The thresholds package monitors OVPI data. Whenever a defined threshold value is breached, or returns to normal following a breach, an action may be invoked. Actions are invoked depending upon the Category and Severity of the threshold that was breached. All thresholds are defined with a Category and Severity, if the Category and Severity of the action match that of the breached threshold then email containing data about the threshold breaches will be sent using the parameters defined below. For information on the contents of the email see the Thresholds User Guide. Wildcards can be used to match any Category or any Severity by entering an asterisk.
Example
Category = FRAME_RELAY
Severity = MEDIUM
Server = smtp.mydomain.com
Port = 25
To = ovpi.admin@mydomain.com
From = ovpi.server@mydomain.com
Subject = Threshold Breach
If any threshold breached has Category=FRAME_RELAY and Severity=MEDIUM then an email containing details of the threshhold breach will be sent via the SMTP server at smtp.mydomain.com using port 25. It will be sent from ovpi.server@mydomain.com to ovpi.admin@mydomain.com with the subject "Threshold Breach"
All fields are mandatory.
Choose an entry from the upper table, edit paramters in the boxes below.
Click the Apply button to save any changes.
Click the Cancel button to cancel any changes.
Click the OK button to save changes and close the form.
Category
Severity
Server
Port
MailTo
MailFrom
* * mail.myserver.com 25 me@myserver.com ovpi@hp.com Thresh
* * mail.myserver.com 25 ops@myserver.com ovpi@hp.com Thresh
Category *
Severity *
Server mail.myserver.com
Port 25
To me@myserver.com
From ovpi@hp.com
Subject Threshold Exceptions
OK
Apply
Cancel

Action 3: USER-SCRIPT

Parameters

A CSV file is created for each combination of Category and Severity. Each CSV file contains details about every applicable breach and clear. Every time a file is created, the user script program is called and the filename is passed as a parameter.

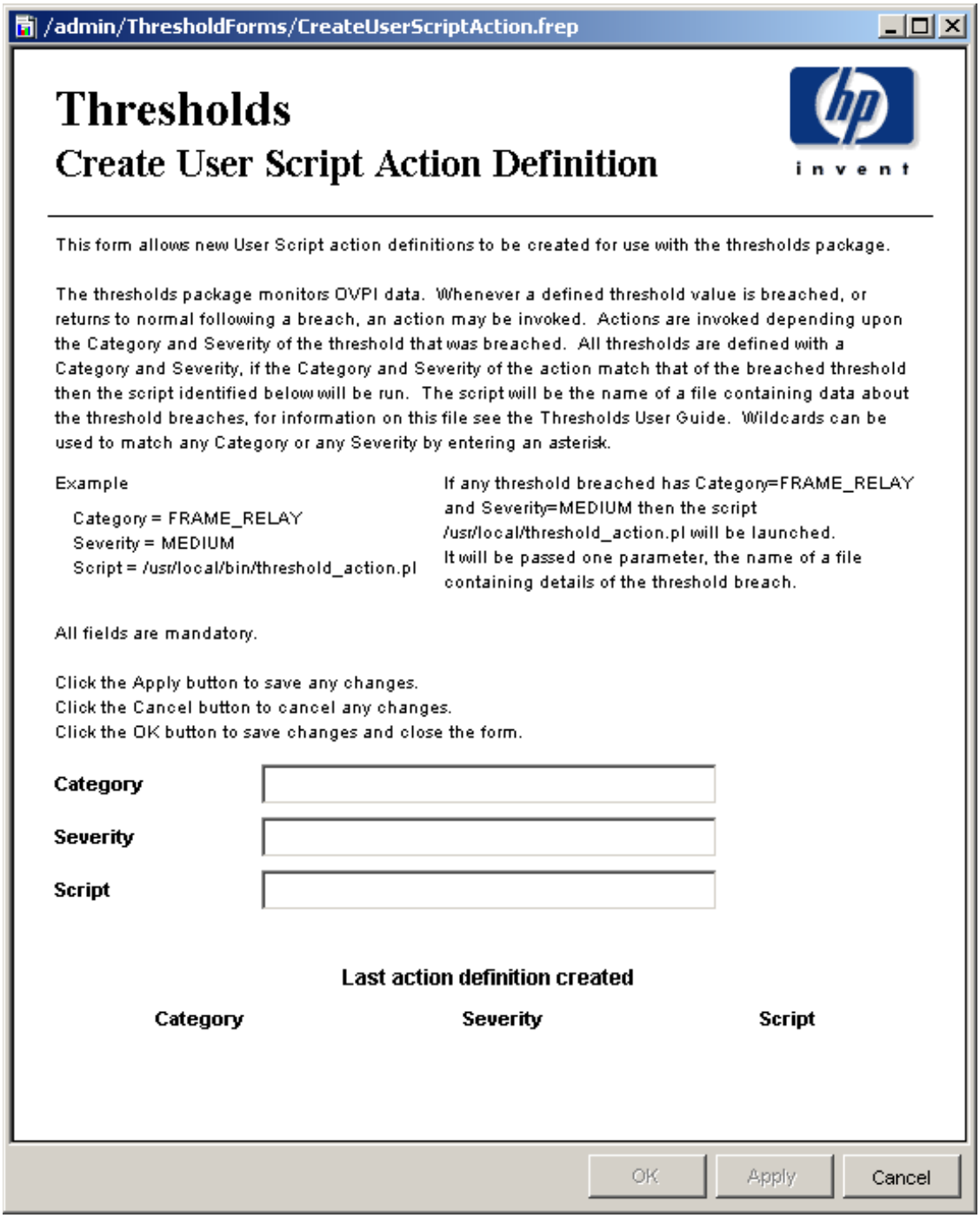
The user script program is called using the supplied command line. If the program is not on the user's path, an appropriate path name should be included. In addition, the user must have suitable permissions to run the program. Responsibility for managing the files created belongs to the program; the thresholding package does not archive these files or delete them.

The program is launched independent of the thresholding package and may outlive the instance that invokes it. Be careful when calling processes that require user intervention. If a backlog of processes develops, PI may slow down or even crash. For this reason, it is good practice to call processes that run to completion automatically.

Creating User Script Actions

To create a user script action, use the Create User Script Action Definition form. Follow these steps to launch the form:

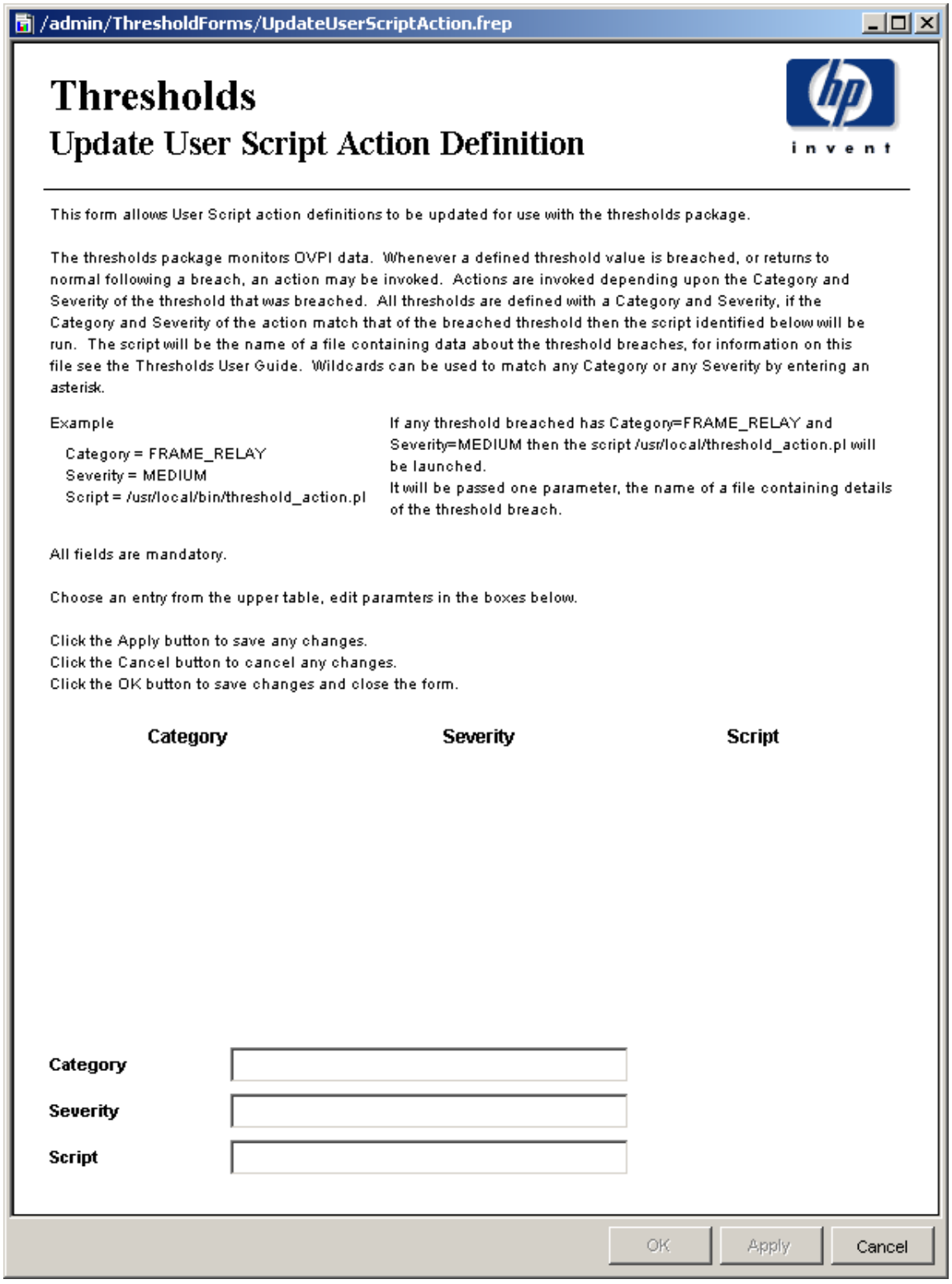
1. In the Management Console, click the **Objects** icon.
2. Select **File > New**.
3. Select **Create User Script Action Definition** and click **Create**.
4. Follow the instructions on the form.
5. When you finish, click **OK**.


/admin/ThresholdForms/CreateUserScriptAction.frep
Thresholds
Create User Script Action Definition
invent
This form allows new User Script action definitions to be created for use with the thresholds package.
The thresholds package monitors OVPI data. Whenever a defined threshold value is breached, or returns to normal following a breach, an action may be invoked. Actions are invoked depending upon the Category and Severity of the threshold that was breached. All thresholds are defined with a Category and Severity, if the Category and Severity of the action match that of the breached threshold then the script identified below will be run. The script will be the name of a file containing data about the threshold breaches, for information on this file see the Thresholds User Guide. Wildcards can be used to match any Category or any Severity by entering an asterisk.
Example
Category = FRAME_RELAY
Severity = MEDIUM
Script = /usr/local/bin/threshold_action.pl
If any threshold breached has Category=FRAME_RELAY and Severity=MEDIUM then the script /usr/local/threshold_action.pl will be launched. It will be passed one parameter, the name of a file containing details of the threshold breach.
All fields are mandatory.
Click the Apply button to save any changes.
Click the Cancel button to cancel any changes.
Click the OK button to save changes and close the form.
Category
Severity
Script
Last action definition created
Category
Severity
Script
OK
Apply
Cancel

Updating User Script Actions

To modify an existing user script action, use the Update User Script Action Definition form. Follow these steps to launch the form:

1. In the Management Console, click the **Objects** icon.
2. Select an object so that the **General Tasks** pane is updated.
3. Under **General Tasks**, double-click **Update User Script Action Definition**. The form opens.
4. Click the desired action definition from the list of actions near the center of the form. The boxes in the bottom section of the form display the action definition parameters.
5. Modify the desired parameters.
6. When you finish making changes, click **OK**.


/admin/ThresholdForms/UpdateUserScriptAction.frep
Thresholds
Update User Script Action Definition
invent
This form allows User Script action definitions to be updated for use with the thresholds package.
The thresholds package monitors OVPI data. Whenever a defined threshold value is breached, or returns to normal following a breach, an action may be invoked. Actions are invoked depending upon the Category and Severity of the threshold that was breached. All thresholds are defined with a Category and Severity, if the Category and Severity of the action match that of the breached threshold then the script identified below will be run. The script will be the name of a file containing data about the threshold breaches, for information on this file see the Thresholds User Guide. Wildcards can be used to match any Category or any Severity by entering an asterisk.
Example
Category = FRAME_RELAY
Severity = MEDIUM
Script = /usr/local/bin/threshold_action.pl
If any threshold breached has Category=FRAME_RELAY and Severity=MEDIUM then the script /usr/local/threshold_action.pl will be launched.
It will be passed one parameter, the name of a file containing details of the threshold breach.
All fields are mandatory.
Choose an entry from the upper table, edit paramters in the boxes below.
Click the Apply button to save any changes.
Click the Cancel button to cancel any changes.
Click the OK button to save changes and close the form.
Category
Severity
Script
Category
Severity
Script
OK
Apply
Cancel

Disabling an Action

You can disable actions, but they will remain in the database in case you want to enable them in the future. Do the following to disable an action:

1. In the Management Console, click the **Objects** icon.
2. Select an object; selecting an object updates the General Tasks pane.
3. In the list of forms under General Tasks, double-click the desired Update Action Definition form. The form opens.
4. Click the desired action definition from the list of actions near the center of the form. The boxes in the bottom section of the form display the action definition parameters.
5. Change Category and/or Severity to a value that will not occur (for example, “NOT_IN_USE” or “RESERVED”) to ensure that the action will not take place.
6. Click **OK**.

4 Reports: Summary and Most Recent

If you install the report pack that comes with the Thresholds Module, you will have the following reports:

- Event Summary
- Most Recent Events

The Event Summary report has a selection table at the top, with these columns:

- Category
- Severity
- Threshold breached
- Source object

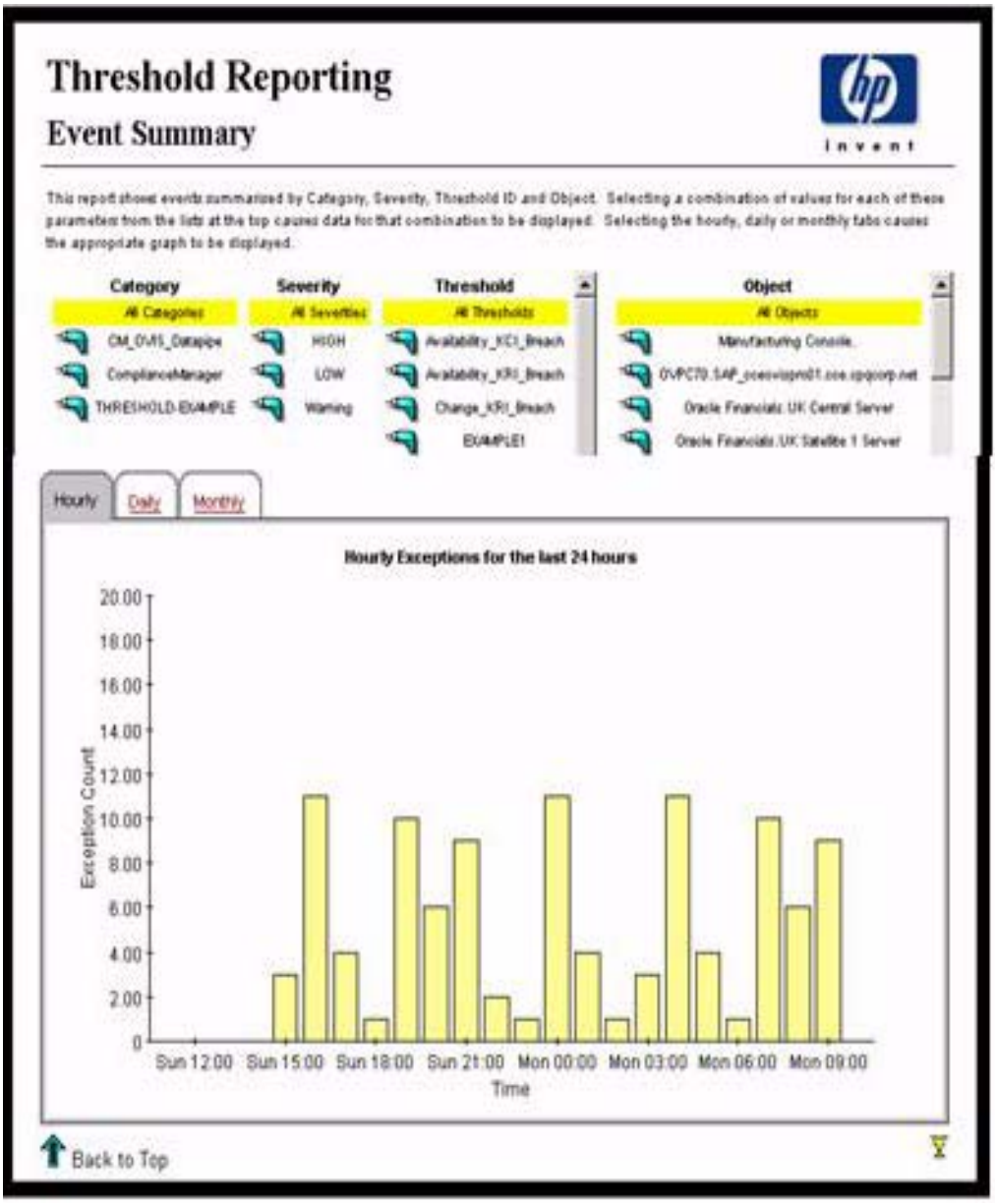
The default sort order is by category. If you want, you can rearrange how this table is sorted. For example, you can sort the table by severity. The graph below the table provides trending data for events, showing the number of threshold events for yesterday in the hourly graph, the number of threshold events for the past several days in the daily graph, and the number of threshold events per month in the monthly graph.

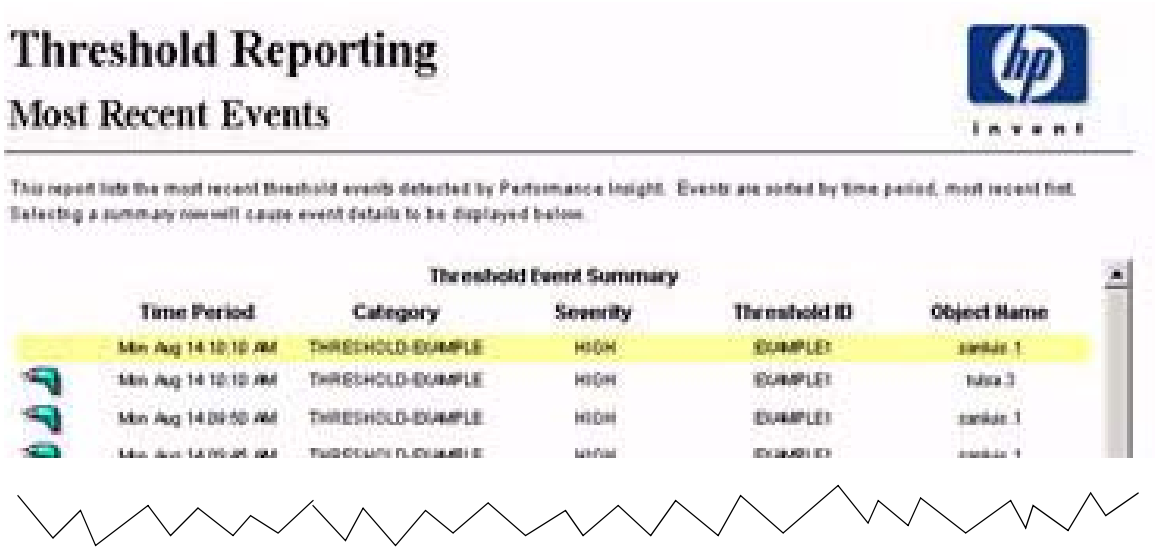
The data in the three graphs is generated from the following tables:

- SH_ThreshSum
- SD_ThreshSum
- SM_ThreshSum

Most Recent Events report provides a list of events, beginning with the most recent event. The data in this report is generated from the E_ThreshExcept table. Use this report to monitor threshold events as they occur.

Both reports are located in the **Thresholds** folder under the **System** folder.


Threshold Reporting
Event Summary
invent
This report shows events summarized by Category, Severity, Threshold ID and Object. Selecting a combination of values for each of these parameters from the lists at the top causes data for that combination to be displayed. Selecting the hourly, daily or monthly tabs causes the appropriate graph to be displayed.
Category
All Categories
OM_OVIS_Datapipe
ComplianceManager
THRESHOLD-EXAMPLE
Severity
All Severities
HIGH
LOW
Warning
Threshold
All Thresholds
Availability_KCI_Breach
Availability_KRI_Breach
Change_KRI_Breach
EXAMPLE1
Object
All Objects
Manufacturing Console
OVPC70.SAP_pceovispro01.pce.cpqcorp.net
Oracle Financials UK Central Server
Oracle Financials UK Satellite 1 Server
Hourly
Daily
Monthly
Hourly Exceptions for the last 24 hours
Exception Count
20.00
18.00
16.00
14.00
12.00
10.00
8.00
6.00
4.00
2.00
0
Sun 12:00
Sun 15:00
Sun 18:00
Sun 21:00
Mon 00:00
Mon 03:00
Mon 06:00
Mon 09:00
Time
Back to Top



Threshold Reporting

Most Recent Events

This report lists the most recent threshold events detected by Performance Insight. Events are sorted by time period, most recent first. Selecting a summary row will cause event details to be displayed below.

Threshold Event Summary

Time Period	Category	Severity	Threshold ID	Object Name
Mon Aug 14 10:10 AM	THRESHOLD-EXAMPLE	HIGH	EXAMPLE1	[illegible]
Mon Aug 14 10:10 AM	THRESHOLD-EXAMPLE	HIGH	EXAMPLE1	tulsa:3
Mon Aug 14 09:50 AM	THRESHOLD-EXAMPLE	HIGH	EXAMPLE1	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

5 Creating a Thresholds Policy

If you are capable of creating your own reports, you are also capable of creating your own threshold policy. Creating your own threshold policy involves the following tasks:

- Writing a Threshold Definition File
- Writing a .pro File
- Adding Entries to trendtimer.sched

Typically, you would write the definition file first, test it, and then write the .pro file. Your last step is adding an entry to trendtimer.sched.

Writing a Threshold Definition File

A threshold definition file provides the rules necessary to construct queries against a single database table or view and an associated property table. A view may span multiple data and property tables. Threshold definition files are written in XML. To modify them, you can use an XML editor or any text editor.

When modifying XML files, make sure that you use special characters correctly. For example, in XML the less-than (<) and greater-than (>) signs indicate the start and end of tags. If you want symbols for less-than and greater-than, use **`&lt`** and **`&gt`**. If you want to add a comment, use this format:

<!-- This is a comment -->

Most web browsers know when an XML file is correctly constructed. Load the edited file into your browser to verify it is well constructed.

The threshold policy definition file contains a number of clauses. Although some clauses are mandatory and some are optional, the structure is fixed.

File Names

A threshold definition file name cannot exceed 27 characters in length (ignoring the final period and any extension following the period). The name of the threshold definition file is used to build a PI data table that stores data required by the Thresholds Module. Exceeding this character limit may cause errors when the data table is built and when the data table is used.

File Structure

The threshold policy definition file consists of a single all-encompassing PI clause. The PI clause contains a single “ThresholdPolicy” clause.

A “ThresholdPolicy” clause consists of several clauses; a “MaxAge” clause, a “DataTable” clause, a “Constraint” clause and a “Thresholds” clause. It may optionally include “Variables” and “UserDefs” clauses.

A “Constraint” clause contains a single “SQL” clause.

An “SQL” clause contains an optional “Name” clause, a “PropertyTable” clause, and an optional SQL constraint “Clause” clause.

A “Variables” clause contains a number of “Variable” clauses.

A “Variable” clause contains a “Data” clause.

A “UserDefs” clause contains up to five numbered “UserDefX” clauses.

A “Thresholds” clause consists of a number of “Threshold” clauses.

A “Threshold” clause contains a “Rule” clause, identified by a “Name” and a “Severity”. It may also optionally be identified as being an “SLA” and may optionally contain a “Display” clause.

A “Rule” clause contains a “Data” clause.

A “Display” clause contains a “Data” clause.

Here is a sample file, showing this structure of clauses:

```
<OVPI>
  <ThresholdPolicy Category="CATEGORY-NAME">
    <MaxAge>
      <DeltaTime Value="MAXIMUM-AGE" Units="HOURS"/>
    </MaxAge>
    <DataTable>tableName</DataTable>
    <Constraint Type="SQL">
      <SQL>
        <Name>CONSTRAINT-NAME</Name>
    <!-- The Name clause is optional -->
        <PropertyTable>PROPERTY-TABLE</PropertyTable>
        <Clause>SQL-CONSTRAINT</Clause>
    <!-- The SQL constraint Clause clause is optional -->
      </SQL>
    </Constraint>
    <Variables>
      <Variable Name="VARIABLE-NAME">
        <Data>VARIABLE-SQL</Data>
      </Variable>
    </Variables>
    <UserDefs>
```

```
      <UserDef1>USERDEF-SQL</UserDef1>
       <!-- Include up to five USERDEF tags -->
    </UserDefs>
    <Thresholds>
      <Threshold Name="THRESHOLD-NAME" Severity="SEVERITY" SLA="SLA-FLAG">
        <Rule>
          <Data>THRESHOLD-SQL</Data>
        </Rule>
        <Display>
          <Data>DISPLAY-SQL</Data>
        </Display>
      </Threshold>
       <!-- Include as many additional Threshold tags as desired -->
    </Thresholds>
  </ThresholdPolicy>
</OVPI>
```

Required values, appearing in italics above, are defined below.

CATEGORY_NAME

The name of the category to which any events defined in this threshold policy belong. Category name is an arbitrary string value and can be set to any single word value, however do not use spaces. The use of special characters (for example, quotes or hash symbols) is not advised since these can have special meaning for third party software packages that integrate with the Thresholds Module. If you are integrating PI with NNM and wish to launch PI reports from NNM, you must set this value to a category that is registered with NNM.

MAXIMUM-AGE

The maximum age of data that will trigger an event. Must be entered in HOURS. This value can be used to suppress testing data that is “too old” which might in turn cause event storms.

The maximum age value will not normally be exceeded since only data which is more recent than the previous test will now be tested. For example, if data is inserted into a table on a fifteen minute polling cycle, and thresholds are checked every fifteen minutes, you might use a maximum age of one hour. The first time you invoke this threshold test, there is no previously tested data. So rather than testing all the data in the table, only data up to the maximum age is tested.

Set the parameter to at least one poll period. For heavily populated tables (“rate” tables, for example) keep the value as low as possible; for lightly populated tables it can be set higher since any impact is smaller.

DATA-TABLE

The data table to be checked. The table must be a valid PI data table or view.

CONSTRAINT-NAME

The name of the constraint applied to data to be checked. Constraint-name is an arbitrary string value and can be set to any single word value (i.e. do not use spaces). The use of special characters (e.g. quotes or hash symbols) is not advised. The constraint name does not get passed on from the thresholds module; thus, it is not externally visible. The name can be used to provide a description of what the constraint does, for example:

- "DOMESTIC-US-CIRCUITS-ONLY"
- "FRAME-RELAY-PORTS"

PROPERTY-TABLE

The property table that is being checked. This must be related to the DATA-TABLE and exist in PI's dictionary tables.

SQL-CONSTRAINT

An SQL clause that constrains the query. The query built by the threshold module is ANDed with this clause. Columns from property and/or data tables may be used. Prefix columns from the property table with "**p.**"; prefix columns in the data table with "**d.**". For example, if the property table being checked contained a column for if_type, it would be possible to check thresholds for a particular if_type by using a constraint clause similar to the following:

```
<Clause>d.if_type = 17</Clause>
```

SQL is checked only when it is passed to the database server. Invalid SQL clauses will result in errors being returned from the database, which in turn will be logged by the Thresholds Module.

VARIABLE-NAME

The name by which the variable will be known. Variable names must be unique within the definition file. Variables defined within this XML clause can be used in the DISPLAY-STRING (see below).

VARIABLE-SQL

An SQL clause that will be evaluated to provide a value for the variable. Columns from property and/or data tables may be used. Prefix columns from the property table with "**p.**"; prefix columns in the data table with "**d.**".

USERDEF-SQL

An SQL clause that will be evaluated and passed directly to output. Columns from property and/or data tables may be used. Prefix columns from the property table with "**p.**"; prefix columns in the data table with "**d.**".

Up to five user defined SQL clauses can be used and allow passing of data which is not directly part of the threshold query to third party systems via any actions defined (e.g. SNMP trap or SMTP mail).

SLA-FLAG

If this tag is present, the threshold is considered an SLA threshold which can be used to determine any breaches that affect a Service Level Agreement. The value itself is ignored, for example, the presence of SLA=”Yes” or SLA=”True” has the same effect. The tag should be omitted if the threshold does not form part of an SLA.

DISPLAY-SQL

An SQL clause that will be evaluated and passed to output. Columns from property and/or data tables may be used as well as variables (defined above). Prefix columns from the property table with “**p.**”; prefix columns in the data table with “**d.**”, prefix variables with “**v**”. The use of variables allows for some “nesting” of the results of queries which can be used to greatly simplify what is presented to the users via actions.

THRESHOLD NAME

The name of this threshold. Name is an arbitrary string value and can be set to any single word value (i.e. do not use spaces). The use of special characters (e.g. quotes or hash symbols) is not advised.

SEVERITY

The severity of the event defined in the particular threshold-policy. Severity is an arbitrary string value and can be set to any single word value (i.e. do not use spaces). The use of special characters (e.g. quotes or hash symbols) is not advised since these can have special meaning for third party software packages (e.g. SMTP servers) which integrate with the thresholds module. Using values that match with the severity levels used by other systems is recommended. For example, if you are sending traps to a network management system that assigns traps to severities CRITICAL, HIGH, MEDIUM, or LOW, use these values.

THRESHOLD-SQL

SQL clauses that constitute the main body of the threshold query. Columns from property and/or data tables may be used. Prefix columns from the property table with “**p.**”; prefix columns in the data table with “**d.**”. For example, if the property table being checked contained a column for CIR, and the data table contained a column for bytes_transmitted, it would be possible to determine if the bytes_transmitted exceeded the CIR by using the following SQL clause:

```
<Data>d.bytes_transmitted &gt; p.cir</Data>
```

Sample Threshold Definition File

This section contains a sample threshold definition file followed by an explanation.

Sample File

```
<OVPI>
  <ThresholdPolicy Category="THRESHOLD-EXAMPLE">

    <MaxAge>
      <DeltaTime Value="1" Units="HOURS"/>
    </MaxAge>

    <DataTable>R_threshEg</DataTable>

    <Constraint Type="SQL">
      <SQL>
        <PropertyTable>K_threshEg</PropertyTable>
      </SQL>
    </Constraint>

    <Variables>
      <Variable Name="utilisation">
        <Data>((d.ifinoctets * 8 * 1000) / (60 * (1+ d.delta_time)))</Data>
      </Variable>
    </Variables>

    <UserDefs>
      <UserDef1>d.received_usec</UserDef1>
    </UserDefs>

    <Thresholds>
      <Threshold Name="EXAMPLE1" Severity="HIGH" SLA="True">

        <Rule>
          <Data>(d.ifinoctets * 8 * 1000) / (60 * (1+ d.delta_time)))
                                              &gt; p.util_threshold)</Data>
        </Rule>

        <Display>
          <Data>Utilisation = v.utilisation, limit = p.util_threshold</Data>
        </Display>

      </Threshold>

    </Thresholds>
  </ThresholdPolicy>
</OVPI>
```

Explanation

The statements above define a threshold in the category THRESHOLD-EXAMPLE. The category is an arbitrary name that can be used (with Severity) to identify groups of thresholds. This mechanism is used to associate threshold breaches (or clears) with actions.

The maximum age of data that will cause an exception is set to one hour. Data samples are checked only once at most. If a sample is either older than the last sample checked (for a particular object) or the sample is older than the maximum age specified in this clause, it will be ignored.

Data from the table “R_threshEg” will be checked. The table has a related property table: “K_threshEg”.

A variable called “utilisation” is defined. Any variables defined can be used in “display” clauses (described below).

A user defined field is created. This is passed directly to output.

A single threshold rule, EXAMPLE1, is defined. The severity associated with this threshold is HIGH and, because the SLA tag is defined, any actions generated by this rule will have the SLA flag set to True.

The rule checks whether the calculated value for circuit utilisation is greater than the limit stored in the property table. Different objects can have different limits.

A display clause is defined and contains the variable defined above, some text, and the limit value from the property table. If the threshold is breached, the resulting string will look similar to this:

“Utilisation = 93, limit = 90”

Additional Samples

You can find additional samples in the Thresholds Example package. The path is:

UNIX

```
$DPIPE_HOME/packages/Thresholds/ThresholdExamples.ap/xml
```

Windows

```
%DPIPE_HOME%\pacakges\Thresholds\ThresholdExamples.ap/xml
```

Writing a .pro File

Every thresholds sub-package that comes with a report pack contains a procedure file. The procedure file calls the core processing script, thresholds.pl.

A threshold procedure file (.pro file) usually consists of a single call to the Thresholds Module within a single block. A single procedure file could also be used to check multiple thresholds across multiple tables by simply inserting multiple calls to thresholds.pl, either in the same block or another block. A call to thresholds.pl within a procedure file looks like this:

```
begin: checkThreshold

{DPIPE_HOME}/bin/perl {DPIPE_HOME}/scripts/thresholds.pl -f policy.xml

end: checkThreshold
```

policy.xml should be replaced with the complete path to the desired configuration file. For more information about PI procedure files, refer to the *Performance Insight Reference Guide*.

Adding Entries to trendtimer.sched

The frequency of threshold checking is determined by entries in trendtimer.sched.

To check thresholds on a regular basis, you should set up an entry in the `trendtimer.sched` file to call an appropriate procedure file. You should check thresholds at a frequency that is less than or equal to the frequency at which data is inserted into the table you are checking. For example, if data is collected and inserted into the table every 15 minutes, you should not check thresholds more often than every 15 minutes.

Here is an example of a `trendtimer.sched` entry that calls a thresholds procedure every 15 minutes:

```
15 - - {DPIPE_HOME}/bin/trend_proc -f {DPIPE_HOME}/scripts/thresh.pro
```

For more information about PI `trendtimer.sched` entries, refer to the *Performance Insight Reference Guide*.

6 Troubleshooting

This chapter explains how to:

- Troubleshoot error and warning messages
- Check execute permissions (possible cause for thresholds.pl not running)
- Debug a threshold definition

Although the Thresholds Module writes log entries to trend.log, the Thresholds Module also calls functions located in PI's Java-based engine. Error logging from these calls is written to website.log. In general, website.log contains greater detail than trend.log.

Error and Warning Messages

The following table provides recommended responses to specific error messages.

Message	Type	Recommended Response
Cannot find system information Error code: 10	FATAL	Use the system manager component in the Management Console to identify a database system as the default collector database. Usually this is the local host.
Failed to lock rules file (another instance may be running) Error code: 11	FATAL	The requested policy is still in use. Wait and try again.
Invalid property table Error code: 12	FATAL	Make sure the key table specified in the policy file matches the key table defined in the database.
Some threshold actions reported errors. See log file for more details. Error code: 99 Reason: The threshold action (SNMP, User-Script, or Mail) reported an error during processing	FATAL	You can find additional information in the website.log file. Verify that the thresholds policy file and threshold actions are correctly formatted and that the required statistics appear in the key and data tables.
Unknown error has occurred at <LOCATION> Error code: 99 This error code is usually followed by a reason message and line number that HP Technical Support can use to help you resolve the problem.	FATAL	You can find additional information in the website.log file. Verify that the thresholds policy file and threshold actions are correctly formatted and that the required statistics appear in the key and data tables.

Checking Execute Permissions

On UNIX systems, check that execute permission has been granted to the files in the Scripts directory, located beneath the $DPIPE_HOME directory. Run the following command:

```
ls -l $DPIPE_HOME/scripts/thresholds.pl
```

If execute permission has been granted, a message similar to this message appears:

```
-rwxr-x--x 1 trendadm adm 25591 Aug 24 19:42 thresholds.pl
```

Execute permission for the current user is shown by the fourth letter in the permission string ("`-rwxr-x--x`" in the example above) and must be set to "`x`".

Debugging a Threshold Definition

If a threshold definition is not working as it should, you should check the following:

- Is the PI server running?
  - For Unix systems, check that the daemon is running; on Windows, check that the service is running.
- Are all actions correctly defined?
  - Ensure that "category" and "severity" identifiers do not contain spaces or special characters (e.g. quotes or hash symbols).
  - Ensure that servers are identified using a valid IP address or resolvable name.
  - Ensure that validly formatted email addresses are used for both "from" and "to" parameters.
- Are all XML definitions correctly constructed?
  - Check that the XML file can be loaded into an XML editor or browser.
  - Ensure that all clauses, tags and values meet the requirements described in this document.

If after checking these, you are still experiencing problems, the following may help:

1. Comment out all thresholds entries in trendtimer.sched file.
2. Deactivate all actions using the "modify" forms to change the category to "NOT_IN_USE" or some other suitable string.
3. Identify any status tables used by the threshold module. These will all appear under the thresholds category and be named "RTH*".
4. Delete any TEEL files associated with the "RTH*" tables identified above found in `$DPIPE_HOME/lib` (UNIX) or `%DPIPE_HOME%\lib` (Windows).
5. Drop the tables identified above using table manager from the PI console.
6. Truncate the E_threshExcept table using table manager from the PI console.
7. From the command line, start the thresholds module using the same command as found within the .pro which you commented out of trendtimer.sched.

If this is successful, you should restore desired actions one at a time, repeating steps 4 through 7 for each action.

Index

T

U

V

X

We appreciate your feedback!

If an email client is configured on this system, by default an email window opens when you click on the bookmark “Comments”.

In case you do not have the email client configured, copy the information below to a web mail client, and send this email to **docfeedback@hp.com**

Product name:

Document title:

Version number:

Feedback:


invent


Java™
COMPATIBLE