

# HP Operations Smart Plug-in For Microsoft<sup>®</sup> Exchange Server

for the HP Operations Manager for Windows<sup>®</sup>

Software Version: 13.00

---

## Installation and Configuration Guide

Document Release Date: December 2009

Software Release Date: December 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 – 2005, 2007 – 2009 Hewlett-Packard Development Company, L.P.

### Trademark Notices

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

## Documentation Updates

The title page of this document 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

Visit the HP Software Support Online web site at:

**[www.hp.com/go/hpsoftwaresupport](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 online support 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 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 register for an HP Passport ID, go to:

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

To find more information about access levels, go to:

**[http://h20230.www2.hp.com/new\\_access\\_levels.jsp](http://h20230.www2.hp.com/new_access_levels.jsp)**

# Contents

<b>1</b>	<b>Introducing the Smart Plug-in for Microsoft Exchange Server</b>	<b>9</b>
	About the Smart Plug-in for Microsoft Exchange Server	10
	Components of Microsoft Exchange SPI	10
	Policies	10
	Tools	10
	Reports	11
	Graphs	11
	Functions of Microsoft Exchange SPI	11
	Servicemap View	12
	Message Browser	13
	Reports and Graphs	13
	HP Operations Topology Viewer Tool	13
	EXSPI Configuration Utility Tool	14
	Monitoring Microsoft Exchange 2007 Server in SAN Environment	14
<b>2</b>	<b>Installing and Upgrading Microsoft Exchange SPI</b>	<b>15</b>
	Installation Packages	17
	SPI Package	17
	Graphing Package	18
	Reporting Package	18
	Console Package	18
	Installation Environments for Microsoft Exchange SPI	18
	Standard Installation of SPI Components on HPOM 8.10 Server	18
	Standard Installation on Remote Consoles	19
	Standalone HP Reporter or HP Performance Manager	19
	Prerequisites to Install Microsoft Exchange SPI	19
	Hardware Requirements	19
	Software Requirements	19
	Installing Microsoft Exchange SPI	20
	Installing Microsoft Exchange SPI on a Remote Console	20
	Installing SPI on a Standalone Management Server	20
	Installing Microsoft Exchange SPI in an HPOM Cluster Environment	22
	Upgrading Microsoft Exchange SPI	22
	Upgrading Microsoft Exchange SPI on a Remote Console	23
	Upgrading Microsoft Exchange SPI on a Standalone Management Server	23
	Upgrading Microsoft Exchange SPI in a HPOM Cluster Environment	24
	Verifying the Installation/Upgrade of Microsoft Exchange SPI	24

<b>3</b>	<b>Configuring Microsoft Exchange SPI</b>	<b>27</b>
	Basic Configuration Procedure	28
	Change Unmanaged Node to Managed Node	28
	Deploy the Instrumentation Categories on the Managed Nodes	29
	Redeploying Instrumentation on Managed Nodes	30
	Run Tools - Create DataSources, Register DataCollector, and Start PowerShell Collector	30
	Starting PowerShell Collector Tool	31
	Specify the Credentials for EXSPI-8X Check Collector Server Policy	35
	Customize policies	35
	Deploy Microsoft Exchange SPI policies on Managed Nodes	36
	Data Logging Scenarios	39
	Discovery Configuration Scenario	39
	Edit Discovery Policy	39
	Deploy Discovery Policy to Managed Nodes	41
	View the Service Map	43
	Additional Configuration Procedure	44
	Functions of EXSPI Data Collectors	44
	EXSPI Configuration Utility Tool	45
	Using EXSPI Configuration Utility	45
	Viewing the EXSPI Configuration Utility	46
	EXSPI Configuration Utility Menubar	47
	EXSPI Configuration Utility Toolbar	48
	EXSPI Collection Configuration Utility Panes	49
	Saving Collection Configuration	49
	File and Save Option	50
	File and Save As Option	50
	Adding Collection Data	50
	Adding a MetricSet	50
	Adding an OpCMsg Call	56
	Adding an OpCMon Call	59
	Adding a DataStore	60
	Adding a Collection Configuration	62
	Modifying a Collection	67
	Modifying a MetricSet	67
	Modifying OpCMsg Call	68
	Modifying OpCMon Call	70
	Modifying a Data Store	70
	Modifying Collection Configuration	71
	Using Additional Cmdlets	72
	Configuring Microsoft Exchange SPI for Exchange Server Cluster Environment	73
	Additional Configuration for Policy Name Change	77
	Map View for Exchange Cluster Services	77
<b>4</b>	<b>Using Policies</b>	<b>79</b>
	Policy Group and Policy Type	79
	Policy Group	79
	Policy Type	80

<b>5</b>	<b>Using Tools</b>	83
	Launching Microsoft Exchange Tools	83
	HP Operations Topology Viewer	83
	Using the HP Operations Topology Viewer	84
	HP Operations Topology Viewer Toolbar	84
	HP Operations Topology Viewer Menus	86
	HP Operations Topology Viewer Map	89
<b>6</b>	<b>Integrating Microsoft Exchange SPI with Reporting and Graphing Solutions</b>	91
	Using Reports and Graphs	91
	Integrating Microsoft Exchange SPI with HP Reporter	91
	Installing and/or Upgrading Report Package	92
	Configuring Report Package	92
	Generating Reports	93
	Integrating Microsoft Exchange SPI with HP Performance Manager	94
	Generating Graphs	95
<b>7</b>	<b>Troubleshooting</b>	97
	Troubleshooting Discovery	97
	Insufficient Privilege	97
	Failed Binary on the Managed Node	97
	Discovery Binary times-out on Managed Node	98
	Troubleshooting through Tracing	98
	Troubleshooting Reports and Graphs	99
	Reports and Graphs are not generated	99
	Data Logging Policies cannot log Data	100
	Browser Crashes while Viewing HTML Report	100
	Reports Fails with Oracle Database	100
	Modifying Policy Names	101
<b>8</b>	<b>Removing Microsoft Exchange SPI</b>	103
	Using DVD	103
	Removing Microsoft Exchange SPI Components	103
	Using Windows Control Panel	104
	Removing Microsoft Exchange from Management Server	104
	Removing Reporting package	104
	Removing Graphing package	104
	Removing Reporting and Graphing Package using .msi File	105
	Removing Reporting Package using .msi file	105
	Removing Graphing Package using .msi File	105
<b>A</b>	<b>List of Microsoft Exchange SPI Instrumentation Files</b>	107
	Exchange2k7_Collector	107
	Exchange 2k7_Core	107
	Exchange2k7_Discovery	111
	<b>Index</b>	113



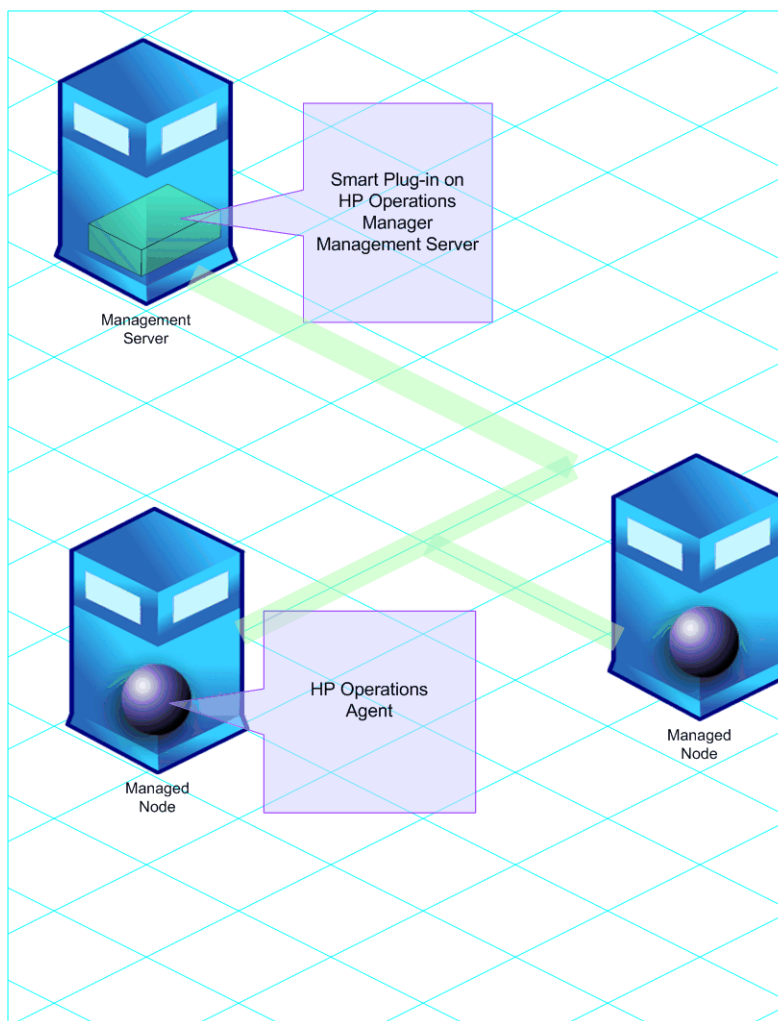


# 1 Introducing the Smart Plug-in for Microsoft Exchange Server

Smart Plug-in (SPI) is plug-in or add-on software for HP Operations Manager (HPOM). It functions as a modular component of HPOM and further improves its monitoring capabilities in managing your IT resources. SPIs help you to simplify the tasks of your environment by:

- Monitoring availability and health
- Detecting performance lapse
- Detecting, preventing, and solving problems
- Documenting problem solutions
- Generating reports

**Figure 1 HPOM Client Structure Architecture**



# About the Smart Plug-in for Microsoft Exchange Server

The Smart Plug-in for Microsoft Exchange Server (Microsoft Exchange SPI) helps you to manage the Microsoft Exchange Server 2007 in your environment. The Microsoft Exchange SPI keeps you informed about the conditions related to the Microsoft Exchange Server 2007 and updates you with the following

- Availability of Microsoft Exchange Server and its roles.
- Monitoring events that occur on Microsoft Exchange Servers.
- Monitoring functions of different Microsoft Exchange Servers.
- Monitoring and reporting important metrics like Mail Flow Latency, Transport Agent Queue Lengths, Information Store DB Cache Size, and SPAM Statistics among others.
- Providing ExBPA Integration.

The Microsoft Exchange SPI enables you to oversee your distributed Microsoft Exchange environment from a central, easy-to-use console. You can apply the performance and problem management processes that you use for networks and systems to monitor Microsoft Exchange Server 2007. The Microsoft Exchange SPI:

- Increases Microsoft Exchange availability and performance.
- Reduces support costs associated with the Microsoft Exchange services.
- Improves capacity management and planning for Microsoft Exchange.

## Components of Microsoft Exchange SPI

The components of Microsoft Exchange SPI are policies, tools, reports, and graphs. Each of these components contributes to enhance the monitoring capability of the SPI.

### Policies

Policies are the pre-defined thresholds to keep a constant vigilance over the Microsoft Exchange Server 2007 environment and improve monitoring schedules in the form of service map alerts and messages. Service map alerts are shown in service map while messages are available in message browser. The Microsoft Exchange SPI provides a range of policies. For more information on policies, see [Chapter 4, Using Policies](#).

### Tools

Tools are the utilities to configure and gather more Microsoft Exchange Server 2007 related information. The Microsoft Exchange SPI tools enable you to perform certain tasks on managed nodes to simplify monitoring the Microsoft Exchange Server 2007. Tools are also used to configure the Microsoft Exchange SPI. For example, EXSPI Configuration Utility and Create DataSource tools. For more information on tools, see [Chapter 5, Using Tools](#).

## Reports

Reports are the pictorial representation of various metrics of the Microsoft Exchange Server 2007. Data collected by policies are used to generate reports. For more information on reports see [Chapter 6, Integrating Microsoft Exchange SPI with Reporting and Graphing Solutions](#).

## Graphs

Graphs represent the various metrics of the Microsoft Exchange Server 2007. Graphs contain the data that are collected by policies. For more information on graphs, see [Chapter 6, Integrating Microsoft Exchange SPI with Reporting and Graphing Solutions](#).

Reports and graphs generated with the help of HP Reporter and HP Performance Manager provide you an overview to determine corrective actions to be taken in the long term.

See *HP Operations Smart Plug-in for Microsoft Exchange Server Online Help* or *HP Operations Smart Plug-in for Microsoft Exchange Server Online Help PDF* for a detailed description of policies, tools, reports, and graphs.

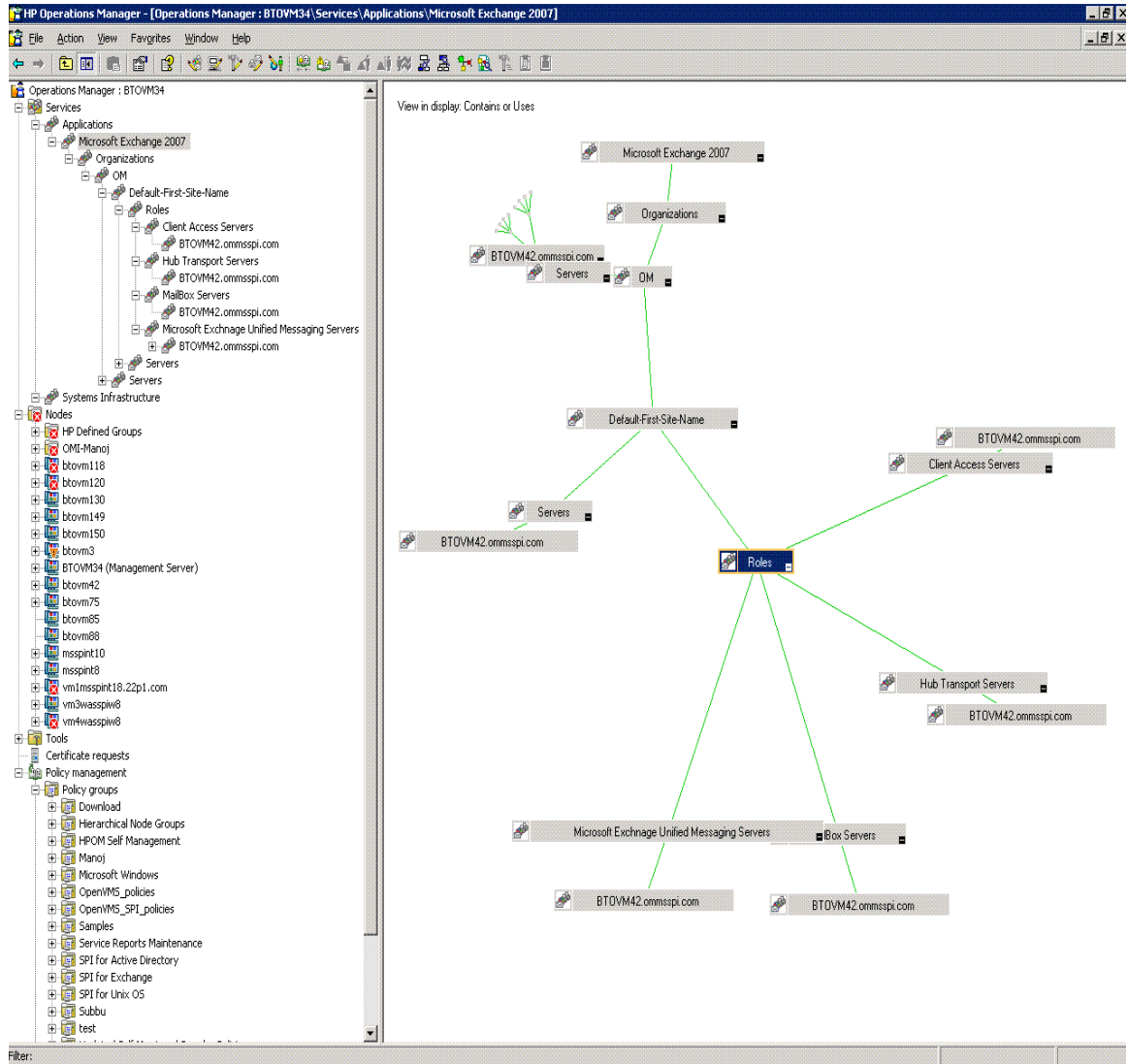
## Functions of Microsoft Exchange SPI

After you configure the Microsoft Exchange SPI, you can view critical information about your Microsoft Exchange Server 2007 environment through the HPOM console in the form of:

- Service map view
- Message alerts
- Reports and graphs
- Topology viewer tool
- EXSPI Configuration Utility tool

## Servicemap View

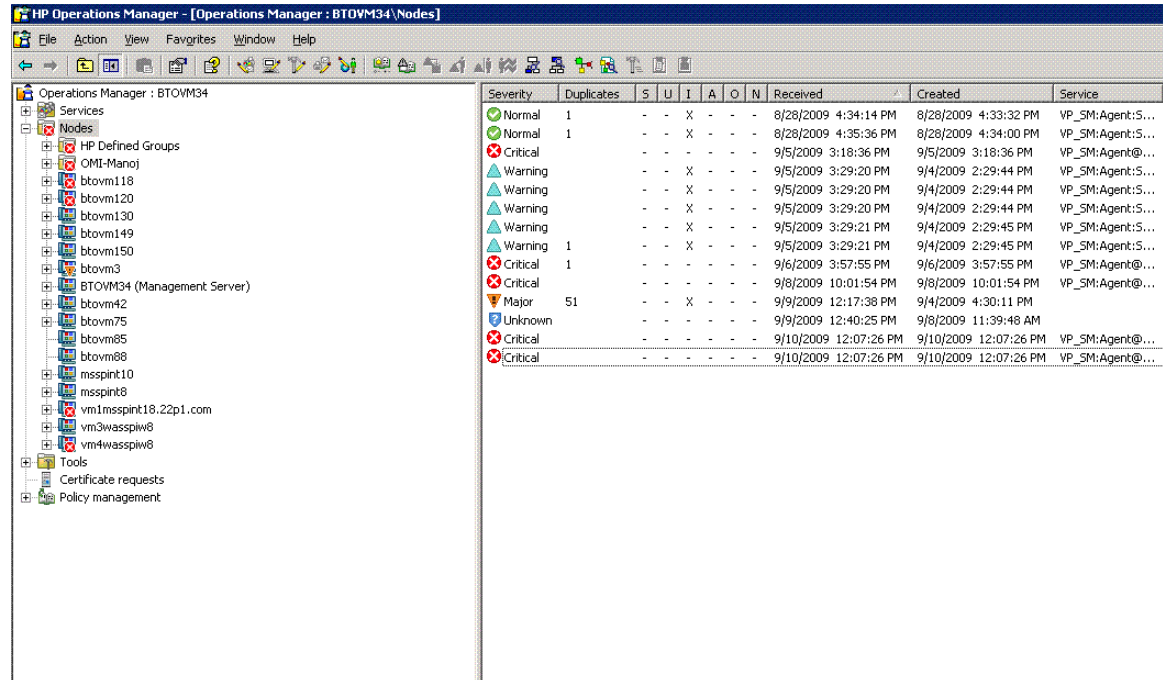
The map view of HPOM presents a graphical and structural view of the Microsoft Exchange Server 2007 in your environment. The Microsoft Exchange SPI discovers the Microsoft Exchange Server 2007 nodes and Microsoft Exchange Server 2007 services and displays them in the map view. The map view displays the near real-time status of your Microsoft Exchange Server 2007 environment.



The map view indicates severity levels problems in the Microsoft Exchange organization through colors (red and blue).

## Message Browser

The Microsoft Exchange SPI monitors events and services on the managed nodes (servers on which the Microsoft Exchange Server 2007 is installed and the HP Operations agent is deployed) and generates messages, which are displayed on the message browser of HPOM console.



Severity	Duplicates	S	U	I	A	O	N	Received	Created	Service
Normal	1	-	-	X	-	-	-	8/28/2009 4:34:14 PM	8/28/2009 4:33:32 PM	VP_SM:Agent:...
Normal	1	-	-	X	-	-	-	8/28/2009 4:35:36 PM	8/28/2009 4:34:00 PM	VP_SM:Agent:...
Critical		-	-	-	-	-	-	9/5/2009 3:18:36 PM	9/5/2009 3:18:36 PM	VP_SM:Agent@...
Warning		-	-	X	-	-	-	9/5/2009 3:29:20 PM	9/4/2009 2:29:44 PM	VP_SM:Agent:...
Warning		-	-	X	-	-	-	9/5/2009 3:29:20 PM	9/4/2009 2:29:44 PM	VP_SM:Agent:...
Warning		-	-	X	-	-	-	9/5/2009 3:29:20 PM	9/4/2009 2:29:44 PM	VP_SM:Agent:...
Warning		-	-	X	-	-	-	9/5/2009 3:29:21 PM	9/4/2009 2:29:45 PM	VP_SM:Agent:...
Warning	1	-	-	X	-	-	-	9/5/2009 3:29:21 PM	9/4/2009 2:29:45 PM	VP_SM:Agent:...
Critical	1	-	-	-	-	-	-	9/6/2009 3:57:55 PM	9/6/2009 3:57:55 PM	VP_SM:Agent@...
Critical		-	-	-	-	-	-	9/8/2009 10:01:54 PM	9/8/2009 10:01:54 PM	VP_SM:Agent@...
Major	51	-	-	X	-	-	-	9/9/2009 12:17:38 PM	9/4/2009 4:30:11 PM	
Unknown		-	-	-	-	-	-	9/9/2009 12:40:25 PM	9/8/2009 11:39:48 AM	
Critical		-	-	-	-	-	-	9/10/2009 12:07:26 PM	9/10/2009 12:07:26 PM	VP_SM:Agent@...
Critical		-	-	-	-	-	-	9/10/2009 12:07:26 PM	9/10/2009 12:07:26 PM	VP_SM:Agent@...

Microsoft Exchange SPI has two message groups:

- EXSPI\_2007: Contains alerts from Microsoft Exchange SPI policies related to the Exchange server status.
- EXSPI\_2007\_Errors: Contains alerts related to the Microsoft Exchange SPI code exceptions and errors that occur during the monitoring process of the Exchange 2007 Server.

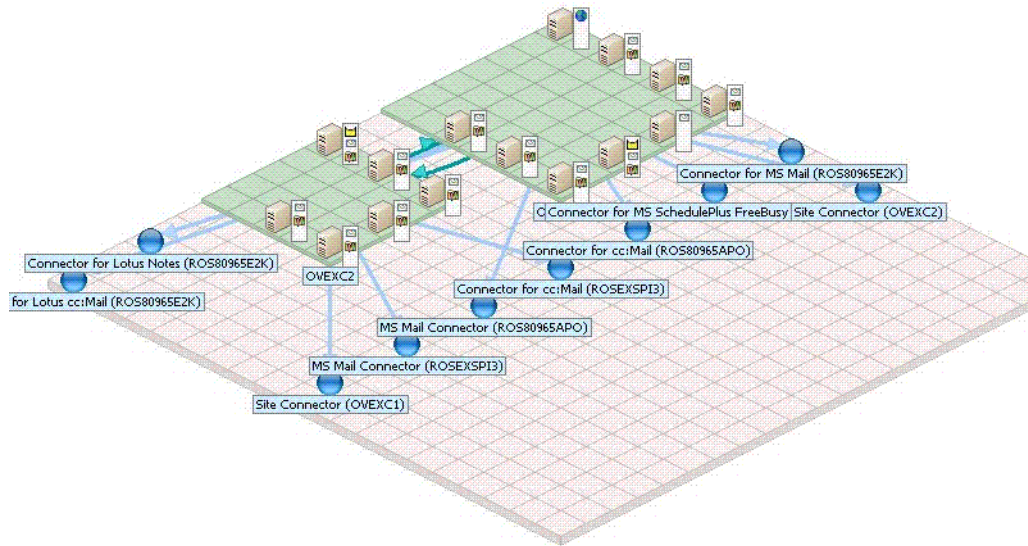
## Reports and Graphs

You can integrate the Microsoft Exchange SPI with HP Reporter and HP Performance Manager to generate reports and graphs based on collected metric data. HP Reporter captures and formats data collected at nodes and generates web-based reports. HP Performance Manager generates graphs from near real-time data gathered from the managed nodes. You can access these graphs from the HPOM console if you install HP Performance Manager on HPOM management server.

## HP Operations Topology Viewer Tool

The Microsoft Exchange SPI enables you to view a Microsoft Exchange organization graphically with the help of three-dimensional maps of routing groups and server connections. From the topology view you can quickly view routing groups, Exchange servers, and the roles

they play within your Exchange organization. Figure 4 displays the Topology view. For more information on the HP Operations Topology Viewer tool, see [HP Operations Topology Viewer](#) on page 83.



## EXSPI Configuration Utility Tool

The EXSPI Configuration Utility tool enables you to edit the collection configuration data for Microsoft Exchange SPI. You can also create new collections and metrics and can modify them, if required. For more information on the EXSPI Collection Configuration Utility tool, see [Additional Configuration Procedure](#) on page 44.

## Monitoring Microsoft Exchange 2007 Server in SAN Environment

You can use Microsoft Exchange SPI in a SAN environment where the high availability of Microsoft Exchange Servers ensure storage consolidation, movement towards centralized management of messaging systems, and real-time mirroring of data. The Microsoft Exchange SPI monitors these activities from the Microsoft Exchange database (Information Store) configured on external SAN storage.

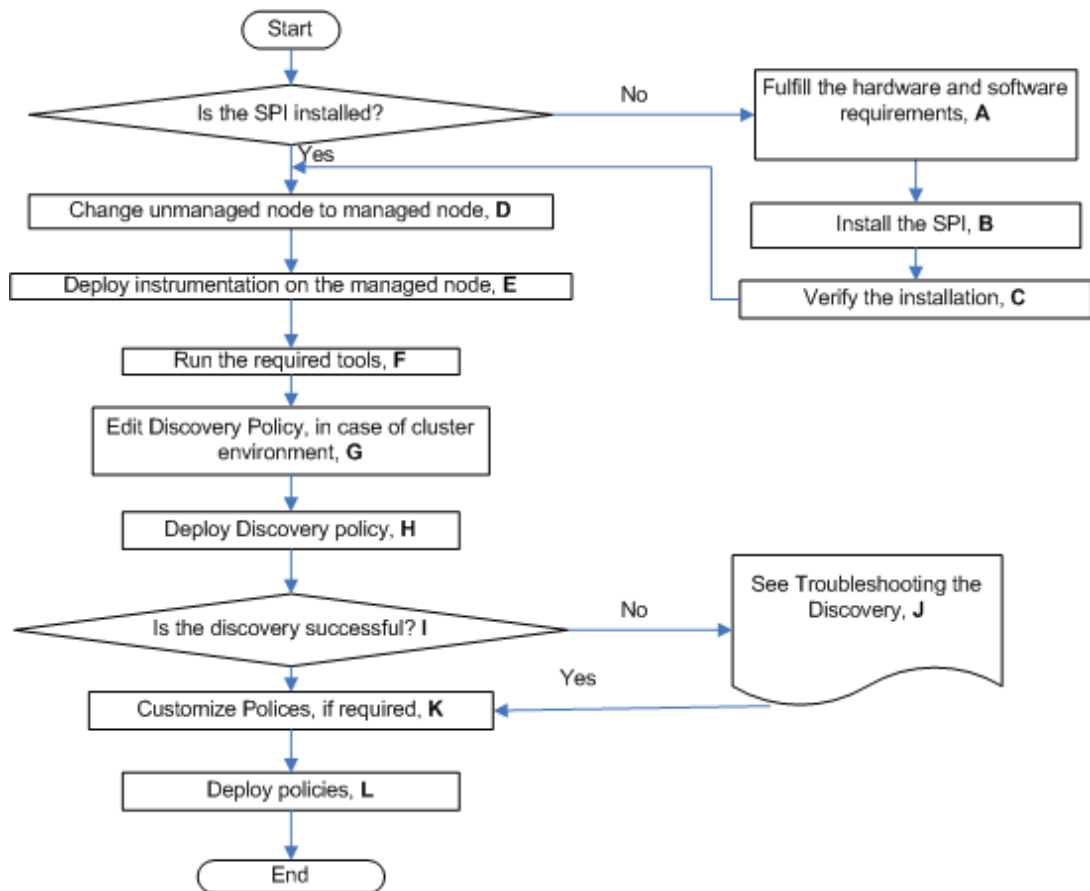
## 2 Installing and Upgrading Microsoft Exchange SPI

Perform the tasks mentioned in the following sections to install and upgrade the Microsoft Exchange SPI.

- ▶ If you are upgrading the Microsoft Exchange SPI from the earlier version to version 13.00, perform the steps in Upgrading Microsoft Exchange SPI, and then install the Microsoft Exchange SPI.

The following flowchart shows an overview of installing and configuring the Microsoft Exchange SPI. See Table 1 to know the sections referred as legends.

**Figure 2 An Overview of Installation and Configuration Steps**



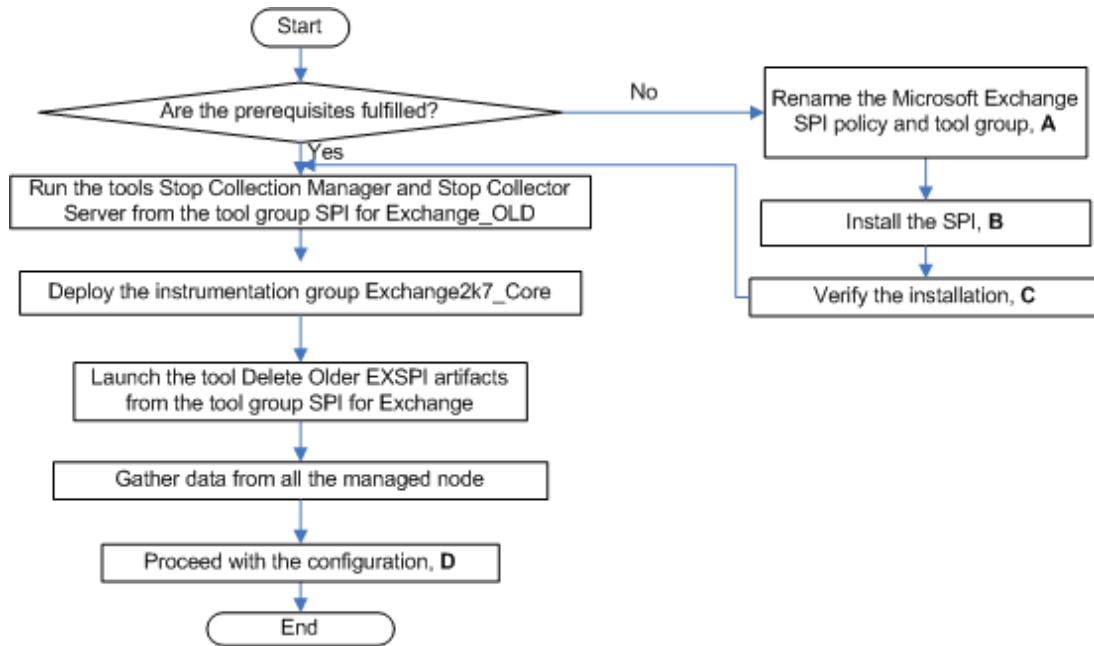
**Table 1 References of Legends of Flowchart**

<b>Legends</b>	<b>References</b>
<b>A</b>	Prerequisites to Install Microsoft Exchange SPI on page 19
<b>B</b>	Installing Microsoft Exchange SPI on page 20
<b>C</b>	Verifying the Installation/Upgrade of Microsoft Exchange SPI on page 24
<b>D</b>	Change Unmanaged Node to Managed Node on page 28
<b>E</b>	Deploy the Instrumentation Categories on the Managed Nodes on page 29
<b>F</b>	Run Tools - Create DataSources, Register DataCollector, and Start PowerShell Collector on page 30
<b>G</b>	Edit Discovery Policy on page 39
<b>H</b>	Deploy Discovery Policy to Managed Nodes on page 41
<b>I</b>	View the Service Map on page 43
<b>J</b>	Troubleshooting Discovery on page 97
<b>K</b>	Customize policies on page 35
<b>I</b>	Deploy Microsoft Exchange SPI policies on Managed Nodes on page 36

The following flowchart shows an overview of upgrading the Microsoft Exchange SPI. See Table 2 for references of the legends.



**Figure 3 An Overview of Upgrade Steps**



**Table 2 References of Legends of Flowchart**

Legends	References
<b>A</b>	Rename the Microsoft Exchange SPI policy group and tool group SPI for Exchange as SPI for Exchange_OLD. on page 23
<b>B</b>	Installing Microsoft Exchange SPI on page 20
<b>C</b>	Verifying the Installation/Upgrade of Microsoft Exchange SPI on page 24
<b>D</b>	Configuring Microsoft Exchange SPI on page 27

## Installation Packages

The Microsoft Exchange SPI installation packages include the SPI package, graphing, reporting, and console packages.

### SPI Package

The SPI package is the .msi package, which contains all the functionality of the SPI. It must be installed on a HPOM Server. You can find the Microsoft Exchange SPI package in the following location:

```
<SPI DVD>\SPIS\Exchange SPI\EXSPI-Server.msi
```

## Graphing Package

The Graphing package contains the graphs provided by the SPI. Graphs are drawn from metrics that are collected in the datasources created by the SPI. You can find the Microsoft Exchange SPI graphing package in the following location:

```
<SPI DVD>\SPIS\EX SPI OVPM ConfigurationPackage\HPOvSpiExGc.msi
```

## Reporting Package

The Reporter package contains the reports provided by the SPI. The Reporter gathers the data from the nodes managed by the SPI, stores the data in its local database, and creates .html reports based on the default SPI report policies. You can find the Microsoft Exchange SPI reporting package in the following location:

```
<SPI DVD>\SPIS\Exchange SPI Reporter Package\EXSPI-Reporter.msi
```

## Console Package

The Console package contains HP Operations Topology Viewer and EXSPI Configuration Utility tools. You can find the Microsoft Exchange SPI console package in the following location:

- For HP Operations Topology Viewer tool:

```
<SPI DVD>\SPIS\SPIS Console Packages\OVTV-Console.msi
```

- For EXSPI ConfigurationUtility

```
<SPI DVD>\SPIS\SPIS Console Packages\EXSPI-Console.msi
```

# Installation Environments for Microsoft Exchange SPI

HPOM for Windows provide the scalable feature of monitoring enterprise application servers. SPIs are part of this scalable architecture, allowing for monitoring specific application servers.

## Standard Installation of SPI Components on HPOM 8.10 Server

An HPOM for Windows 8.10 server does not have the OVPMLite and ReporterLite installed by default. Only the full versions of these products are available for install. As a result, through the HP Operations Smart Plug-Ins DVD you can select to install only the SPI packages and not the reporter and graphing packages. However, if the full version of Reporter or Performance Manager is installed on the same machine, then the corresponding packages can be installed or uninstalled on the HPOM 8.10 server.

## Standard Installation on Remote Consoles

All the Remote Console packages on the SPI DVD are installed at once on to remote consoles. No option is provided to select a particular remote console package.

## Standalone HP Reporter or HP Performance Manager

For such a system only the corresponding package of any SPI is enabled and available for selection from the HP Operations Smart Plug-ins DVD. For example, if a system has only HP Reporter installed then the reporter package of any SPI could be installed on it. The same applies to the graphing package and HP Performance Manager.

## Prerequisites to Install Microsoft Exchange SPI

Fulfill the hardware and software requirements before installing the Microsoft Exchange SPI. Also, ensure that you install the HPOM server before installing the Microsoft Exchange SPI. It is not necessary to stop HPOM sessions before beginning the installation of the Microsoft Exchange SPI.

### Hardware Requirements

See the *HP Operations Manager for Windows Installation Guide* for information on hardware requirements.

### Software Requirements

Ensure that the following software requirements are fulfilled:

On management server:

- HP Operations Manager for Windows: 8.10 and the latest patch
- HP Reporter: 3.80
- HP Performance Manager: 8.20 (if you want to generate graphs)
- HP Operations SPI Data Collector (DSI2DDF): 2.40
- HP SPI Self-Healing Services. (SPI-SHS-OVO, automatically installed while installing the SPI using SPIDVD): 3.00



You must install HPOM console, Management Server, and agents to enable the Microsoft Exchange SPI.

On managed node:

- HP Operations agent (version 8.53 or 8.60 (HTTPS) and 7.35 (DCE)) installed and configured
- HP Performance Agent: 5.00 (required if you want to use HP Performance Agent for data logging)

# Installing Microsoft Exchange SPI

Install the Microsoft Exchange SPI on HPOM for Windows 8.10. You can install on a remote console or on a standalone management server.

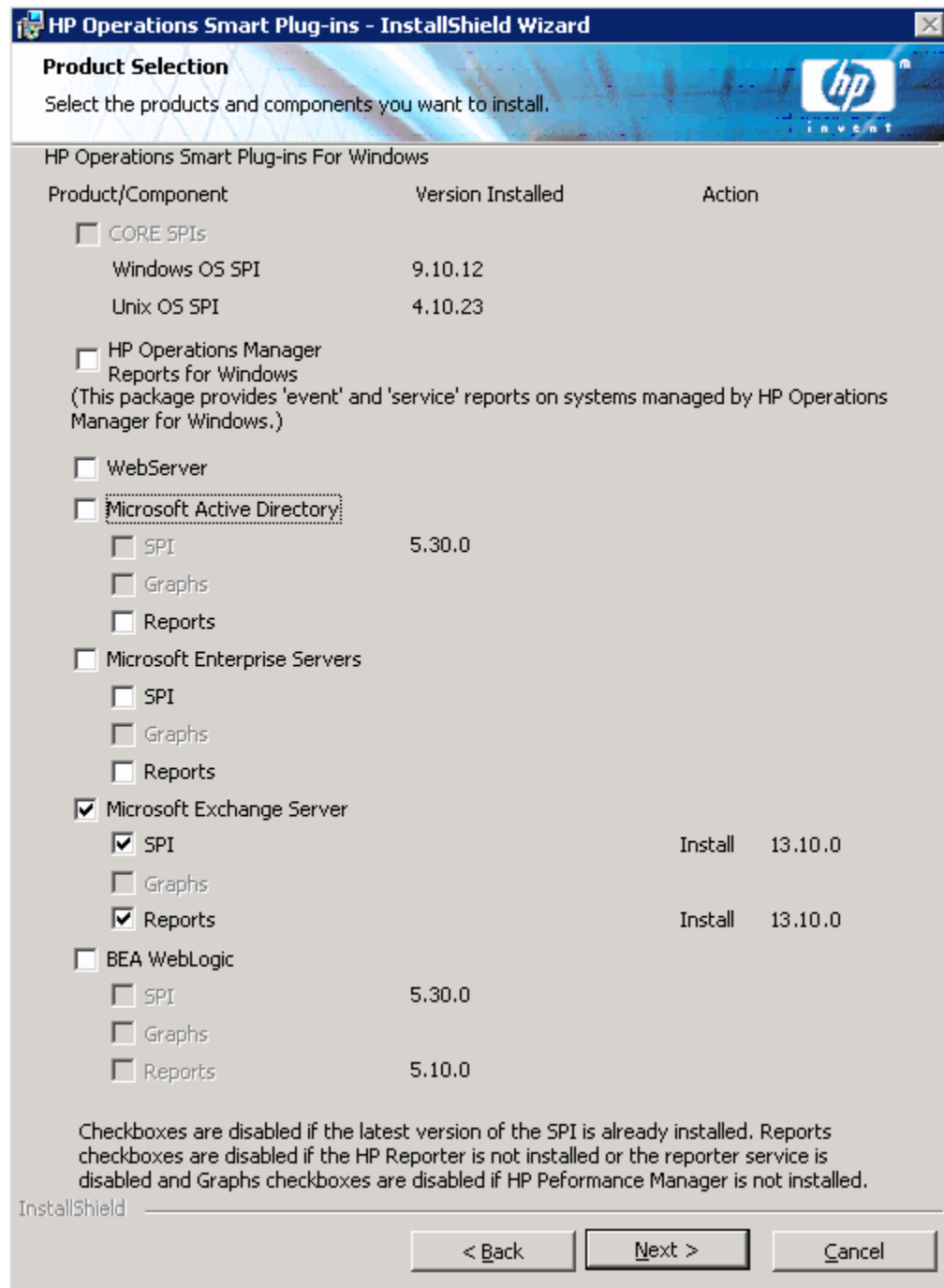
## Installing Microsoft Exchange SPI on a Remote Console

Install only the Microsoft Exchange SPI console packages on the HPOM remote consoles.

## Installing SPI on a Standalone Management Server

The HP Operations Smart Plug-ins DVD contains the Microsoft Exchange SPI. To install the Microsoft Exchange SPI on the management server, follow these steps:

- 1 Insert the *Smart Plug-ins*, DVD into the DVD drive of the management server or console system. The Installation wizard opens.
- 2 Click **Next** to continue. The Smart Plug-ins Release Notes and Other Documentation screen appears.
- 3 Click **Next**. The Product Selection screen appears.



- 4 Click **Next**. The Enable/Disable AutoDeployment screen appears.
- 5 Check the **Enable** or **Disable** button and click **Next**. The License Agreement screen appears.
- 6 Accept the terms by selecting the option **I accept the terms in the license agreement**, and click **Next**. The Ready to Install the Program screen appears.

7 Selecting **Back** allows you to edit previous selections. Otherwise click **Install** to begin the installation. The installation begins. The wizard installs the core SPIs, all necessary packages, and the Microsoft Exchange SPI.

➤ Selecting the **Cancel** button after the installation has started does not halt the entire installation process, but only that of the product currently being installed (shown in the Status area); installation of the next selected product then begins.

8 Click **Finish** after the installation is complete.

## Installing Microsoft Exchange SPI in an HPOM Cluster Environment

Before installing the Microsoft Exchange SPI in a cluster environment, make sure that HPOM for Windows 8.10 is installed on each system of the cluster..

➤ The HPOM console does not function properly until you install the Microsoft Exchange SPI on all nodes in the HPOM cluster.

Task 1: [At the first cluster-aware management server, select and install Smart Plug-ins.](#)

Complete the steps described in [Installing SPI on a Standalone Management Server](#) before proceeding to the next management server.

➤ Before beginning, be sure that sufficient disk space is available on each management server for the Microsoft Exchange SPI. Cancelling the installation process before completion could result in partial installations and require manual removal of the partially installed components.

Task 2: [At the next cluster-aware management server, install pre-selected Smart Plug-ins.](#)

Repeat the steps described in [step 1](#), [step 2](#), and [step 8](#) in [Installing SPI on a Standalone Management Server](#) on each management server in the cluster and continue to every management server (as was defined in the HP Operations Manager cluster installation) until you have finished.

➤ The HPOM console does not function properly until installations are completed on all the nodes in the cluster.

## Upgrading Microsoft Exchange SPI

Perform the tasks in the following sections for upgrading the Microsoft Exchange SPI in different environments.

➤ Delete all versions of the Exchange 2007 Discovery policy from **Policy Management** → **Agent policies grouped by type** → **Service Auto-discovery**, prior to upgrading from Microsoft Exchange SPI 12.10 to 13.00

## Upgrading Microsoft Exchange SPI on a Remote Console

If you are using HPOM on a remote console, follow the Smart Plug-ins upgrade procedure for console-only systems:

- 1 At the console-only system, insert the *HP Operations Smart Plug-ins* DVD.
- 2 Follow the instruction screens until a dialog appears saying that a remote console installation has been found.
- 3 Click **Next**.

The upgrade of all previously installed packages now occurs.

## Upgrading Microsoft Exchange SPI on a Standalone Management Server

To upgrade the Microsoft Exchange SPI on a standalone Management Server:

- 1 Rename the Microsoft Exchange SPI policy group and tool group **SPI for Exchange** as **SPI for Exchange\_OLD**.
- 2 Install the Microsoft Exchange SPI 13.00. See [Installing SPI on a Standalone Management Server](#).
- 3 Run the tools Stop Collection Manager and Stop Collector Server from the tool group **SPI for Exchange\_OLD** on all the managed Microsoft Exchange servers. This stops collection manager and collector server on the nodes.
- 4 Deploy the instrumentation group **Exchange2k7\_Core** to all the managed Microsoft Exchange server nodes. To deploy the instrumentation category see [Deploy the Instrumentation Categories on the Managed Nodes](#).
- 5 Launch the tool **Delete Older EXSPI artifacts** from the tool group **SPI for Exchange** on all the managed Microsoft Exchange server nodes to remove the previous version of the Microsoft Exchange SPI policies and instrumentation categories deployed on the nodes.
- 6 Gather data from all the managed node and perform the following steps:

Ensure to perform the following steps before upgrading the Microsoft Exchange SPI reporter package to 13.00 on the HP Reporter Server.

Exchange SPI 13.00 uses a different format of data to be logged into the data stores on managed nodes, which is used by HP Reporter. You must gather all the previous data sources from all the managed Microsoft Exchange nodes before re-creating EXSPI data stores. For this:

- a Ensure to install the .NET Framework 2.x (or higher) on the HP Reporter server. Insert the HP Operations Smart Plug-ins DVD on the HP Reporter server.
- b Run the discovery command to discover all the managed nodes on the HP Reporter server. Check the %OvDataDir%\trace.discover file to ensure that all the Microsoft Exchange managed nodes are discovered.
- c Open a command prompt and browse to the following path:  
<DVD-Drive>\SPIs\Exchange SPI
- d Ensure that all the Microsoft Exchange managed nodes are discovered by the HP Reporter, and then run the following command:  
**EXSPI\_run\_gatherCODA.exe** <reporter\_system\_dsn> <reporter\_db\_username>  
<reporter\_db\_password>

In this instance, <reporter\_system\_dsn> is the system DSN for the HP Reporter database; <reporter\_db\_username> and <reporter\_db\_password> are the user name and password to access the HP Reporter database.

- e Check the %OvDataDir%\trace.gather file for any errors. Ensure that the data is collected for all the metric lists from all the managed Microsoft Exchange nodes.
- 7 Launch the tool **Delete older EXSPI classes** from the tool group **SPI for Exchange** on all the managed Microsoft Exchange server nodes to delete the previous version of the Microsoft Exchange SPI data store on the managed nodes.
- 8 Proceed with configuring the Microsoft Exchange SPI. See [Basic Configuration Procedure](#).

➤ Use Software Upgrade Tool Kit 2.0 to retain the customization of the policies. See *HP Operations Smart Plug-in Upgrade Toolkit Windows User Guide* for more details.

## Upgrading Microsoft Exchange SPI in a HPOM Cluster Environment

To upgrade the Microsoft Exchange SPI in an HPOM cluster, perform the following tasks:

**Task 1:** [At the first cluster-aware management server, select and install Smart Plug-ins.](#)

Complete the steps in [Upgrading Microsoft Exchange SPI](#) before proceeding to the next management server.

➤ Before starting the installation, ensure that there is sufficient disk space on each management server for the Microsoft Exchange SPI. Cancelling the installation process before completion could result in partial installations and require manual removal of the partially installed components.

**Task 2:** [At the next cluster-aware management server, install pre-selected Smart Plug-ins.](#)

Repeat the steps [step 1](#), [step 2](#), and [step 8](#) in [Upgrading Microsoft Exchange SPI on a Standalone Management Server](#) on page 23 on each management server in the cluster. Continue the upgrade on every management server (as was defined in the HP Operations Manager cluster installation) until you have finished.

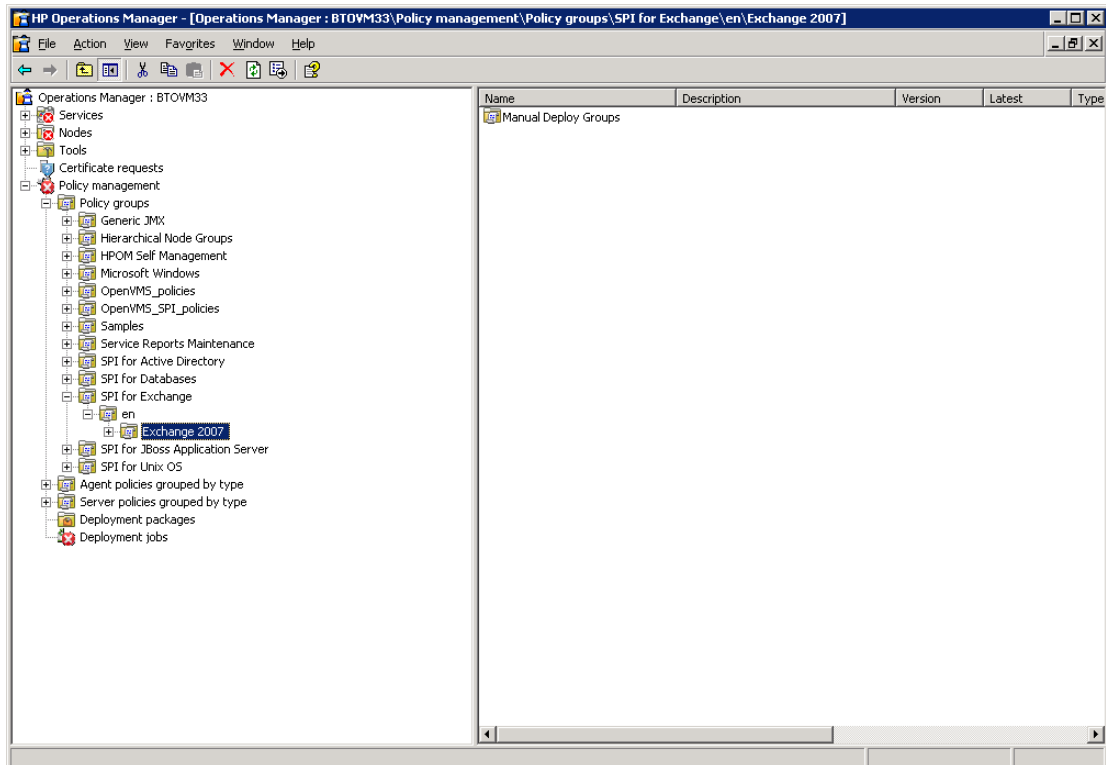
➤ The HPOM console cannot function properly until the installations are completed on all the Microsoft Exchange nodes in the cluster.

## Verifying the Installation/Upgrade of Microsoft Exchange SPI

To verify the Microsoft Exchange SPI has been installed or upgraded properly perform either of the following:



- Check the SPI under policy group. Expand **Policy Group** under **Policy Management**. The **SPI for Exchange** in the list verifies the installation. You can further expand **SPI for Exchange** and check for **Exchange Server 2008** policies.

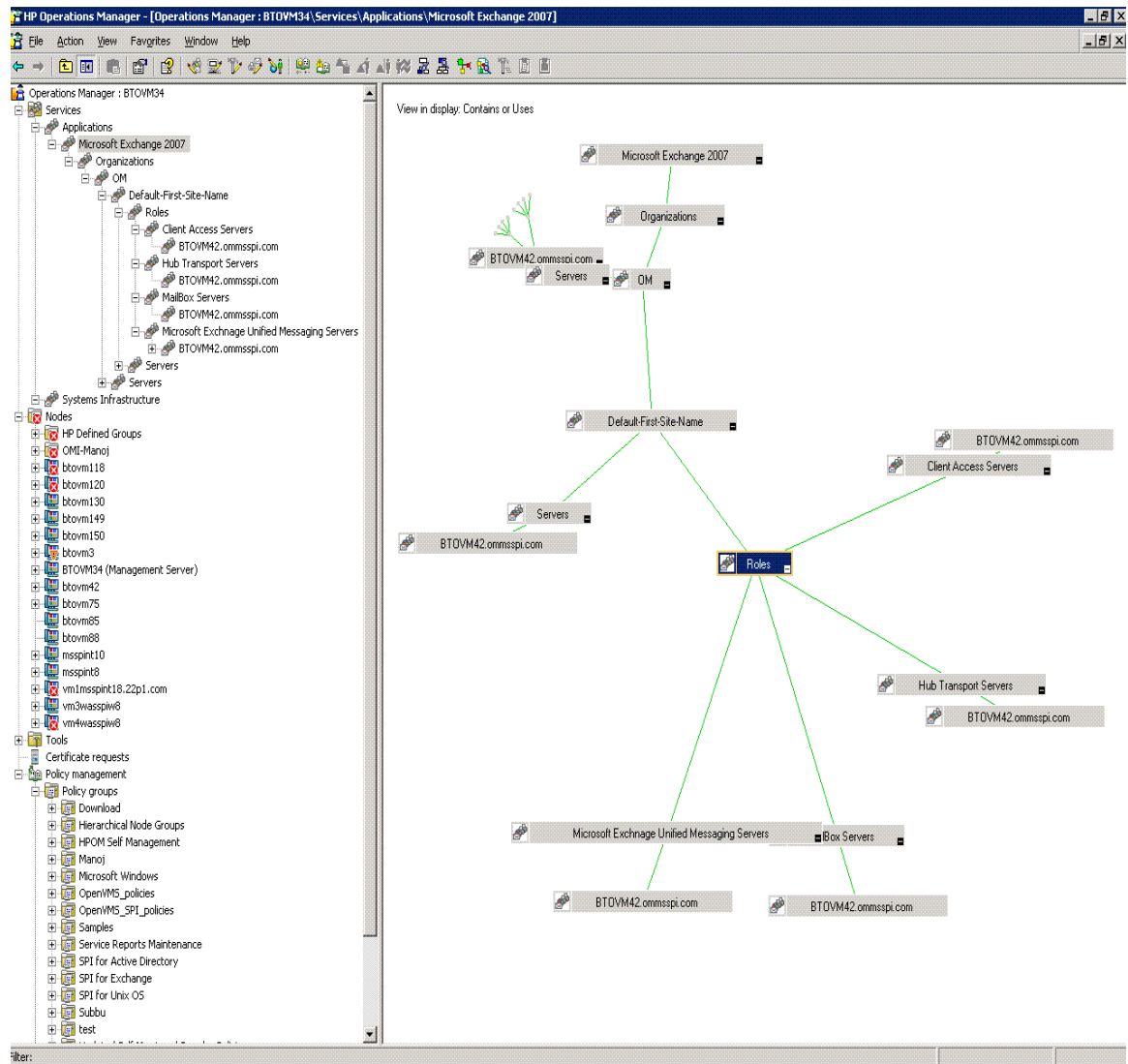


- Verify the policies and instrumentation binaries have 13.00 version.



# 3 Configuring Microsoft Exchange SPI

The SPI monitors the Microsoft Exchange Server by discovering the existing components of the Microsoft Exchange Server 2007 in your environment and maintaining the thresholds set up by the policies. After you install the Microsoft Exchange SPI, you must configure it to monitor the Microsoft Exchange Server 2007 nodes in your organization.



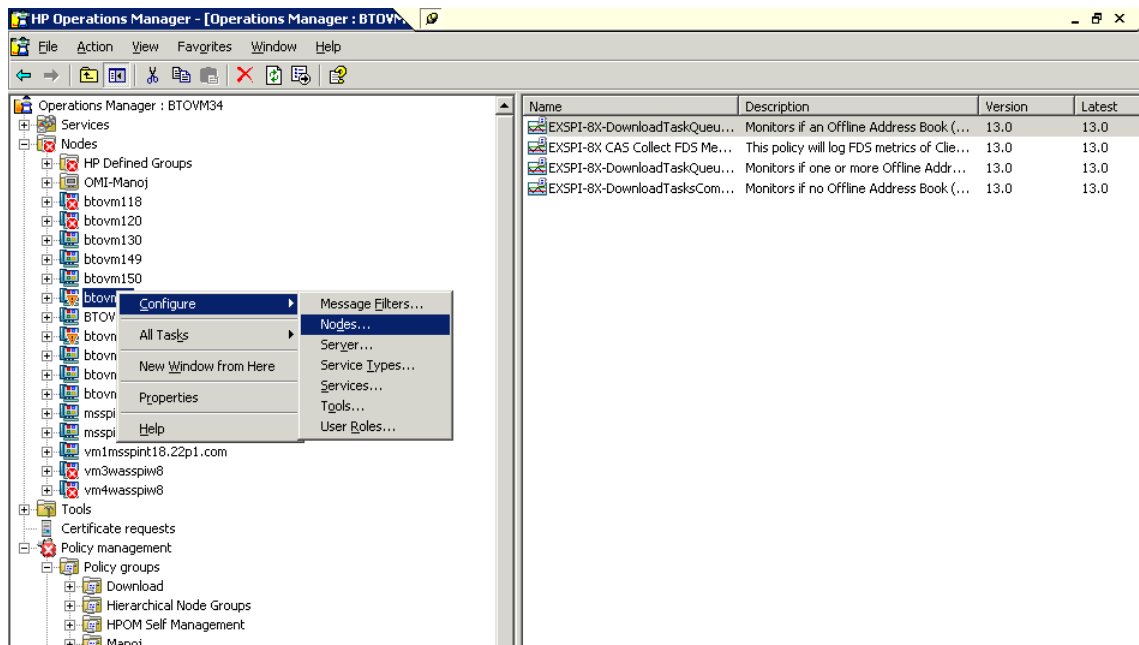
# Basic Configuration Procedure

Configure the Microsoft Exchange SPI by performing the tasks in the following sections.

## Change Unmanaged Node to Managed Node

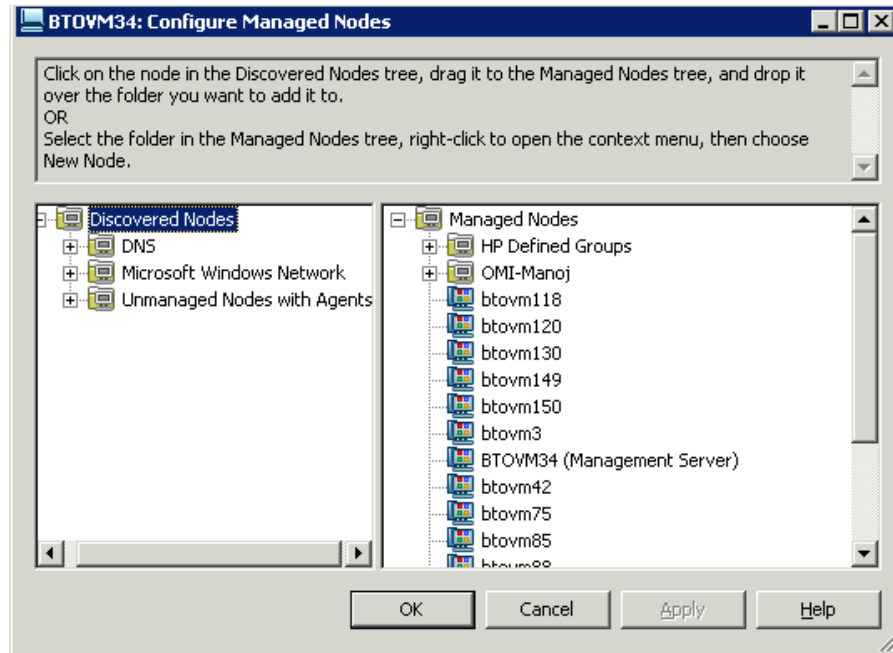
To change unmanaged node to a managed node, add the nodes to the HPOM console's nodes folder. By adding nodes, you can launch an automated service discovery process that duplicates the manually invoked process.

- 1 In the console, right-click **Nodes**, and select **Configure** → **Nodes**.



- 2 In the **Configure Managed Nodes** box, add the unmanaged nodes to the **Nodes** using any of the following methods:
  - In the left pane double-click each node you want to add.
  - Drag and drop nodes from left to right.

- In the left pane, right-click each node, and then select **Manage**.



- 3 (As needed) If a system running the HP Operations agent software is not available in the discovered nodes folder in the left pane, in the details pane right-click **Nodes**, select **New Node**, and then type the system name and other relevant information, and then click **OK**.

## Deploy the Instrumentation Categories on the Managed Nodes

Deploy the following instrumentation categories for the Microsoft Exchange SPI:

- SPIDataCollector
- Exchange2k7\_Core
- Exchange2k7\_Collector
- Exchange2k7\_Discovery

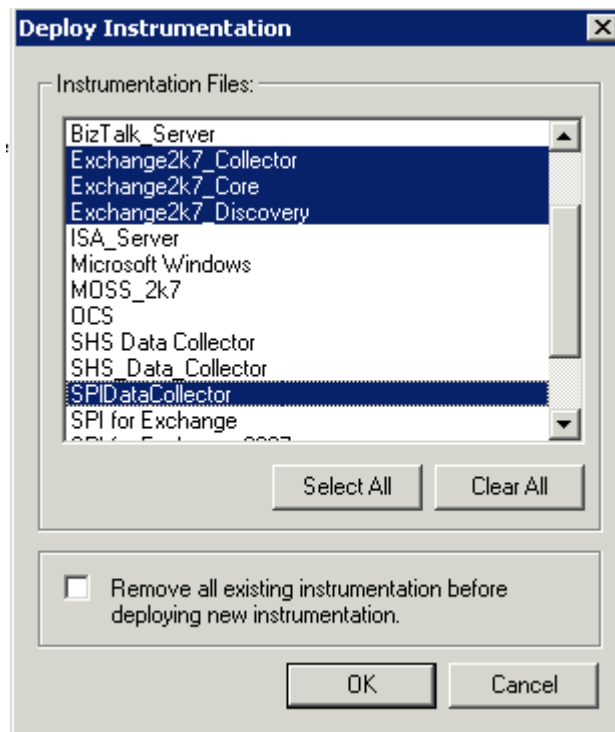


Configuration Deployment fails, if the PowerShell prompt, with EXSPI pssnapin loaded, is kept open on managed node.

To deploy instrumentation:

- 1 In the console tree of HPOM, right-click a node and select **All Tasks**. Select **Deploy instrumentation....** The **Deploy Instrumentation** box opens.
- 2 Select the mandatory instrumentation category, **SPIDataCollector**.

- 3 Select **Exchange2k7\_Core**, **Exchange2k7\_Collector**, and **Exchange2k7\_Discovery** categories, and then click **OK**.



- 4 Perform steps 1 through 3 for all the other Exchange managed nodes.

## Redeploying Instrumentation on Managed Nodes

When you redeploy instrumentation to the Exchange 2007 server, verify whether EXSPI PowerShell Collector (hp.ov.spi.excollectorserver.exe) is running or not.

To redeploy instrumentation, follow these steps:

- 1 Disable the **EXSPI-8X Check Collector Server** policy in the Exchange 2007 server.
- 2 From the HPOM console, run the **Stop PowerShell Collector** tool and select the Exchange 2007 server.
- 3 Redeploy the instrumentation. For more information on how to deploy instrumentation, see [Deploy the Instrumentation Categories on the Managed Nodes](#) on page 29.
- 4 From the HPOM console, run the **Start PowerShell Collector** tool and select the Exchange 2007 server.
- 5 Enable the **EXSPI-8X Check Collector Server** policy in the Exchange 2007 server.

## Run Tools - Create DataSources, Register DataCollector, and Start PowerShell Collector

Run the following Exchange SPI tools in each Microsoft Exchange node in the given order:

- *Create Data Sources*: The Create Data Sources tool creates databases either into the HP Operations agent's data store (embedded performance component - also known as CODA), or into the HP Performance Agent.

If you do not have the HP Performance Agent installed in your environment, the tool creates databases into the data store (CODA). The data store can store the data collected by individual collectors.

If the managed node has both HP PA and CODA installed, then to create the data source in CODA, create an empty nocoda.opt file, and then customize the Create DataSources tool cmdline by adding -CODA option before you start the tool

For more details, see [Data Logging Scenarios](#).



This tool checks for any existing EXSPI datasource. If no datasource exists, it displays an error message. This error message, however, can be ignored as the Create Data Sources tool continues to create a new EXSPI datasource.

- *Register DataCollector*: The Register DataCollector tool registers necessary COM components on the nodes. Run this tool before you start monitoring the nodes.
- *Start PowerShell Collector*

The Start PowerShell Collector tool starts the EXSPI Collector on the Exchange node.



Before you start this tool, run the Edit XPL Configuration File tool. This tool enables the PowerShell Collector tool to run as non-agent user.

Start the PowerShell Collector tool as a user who has the following privileges of an:

- Exchange View-Only Administrator
- Exchange Server Administrator of all mailbox servers
- Local Administrator of all mailbox servers and
- READ+WRITE access to Microsoft Exchange System Object (MESO) of all mailbox servers

To grant READ+WRITE access to MESO to the user:

- a Open Active Directory Users & Computers snap-in on the DC of the domain to which the Microsoft Exchange Server is a member of.
- b Ensure that **View** → **Advanced Features** is selected.
- c Browse to Microsoft Exchange Systems Objects container, right-click, and select **Properties**.
- d Click **Security** tab, and then click **Advanced**.
- e Select **Add** button, type the name of user account to be delegated, and then click **OK**.
- f In the Apply to Drop down list, select **msExchSystemMailbox objects**.
- g Select the **READ PROPERTY & WRITE PROPERTY** check box.
- h Click the consequent **OK** buttons to close all the property sheets.
- i Wait for or force the AD replication.

## Starting PowerShell Collector Tool



Run the Edit XPL Configuration File tool on the managed node before starting the Start Powershell Collector tool. This tool enables the PowerShell Collector tool to run as non-agent user.

- ▶ By default, the Start PowerShell Collector tool is set to run as SYSTEM user. When you run this tool for the first time, configure it to run as a Special user. For more information on the Start PowerShell Collector tool, see [Start PowerShell Collector](#) on page 31.

To start the Start PowerShell Collector tool:

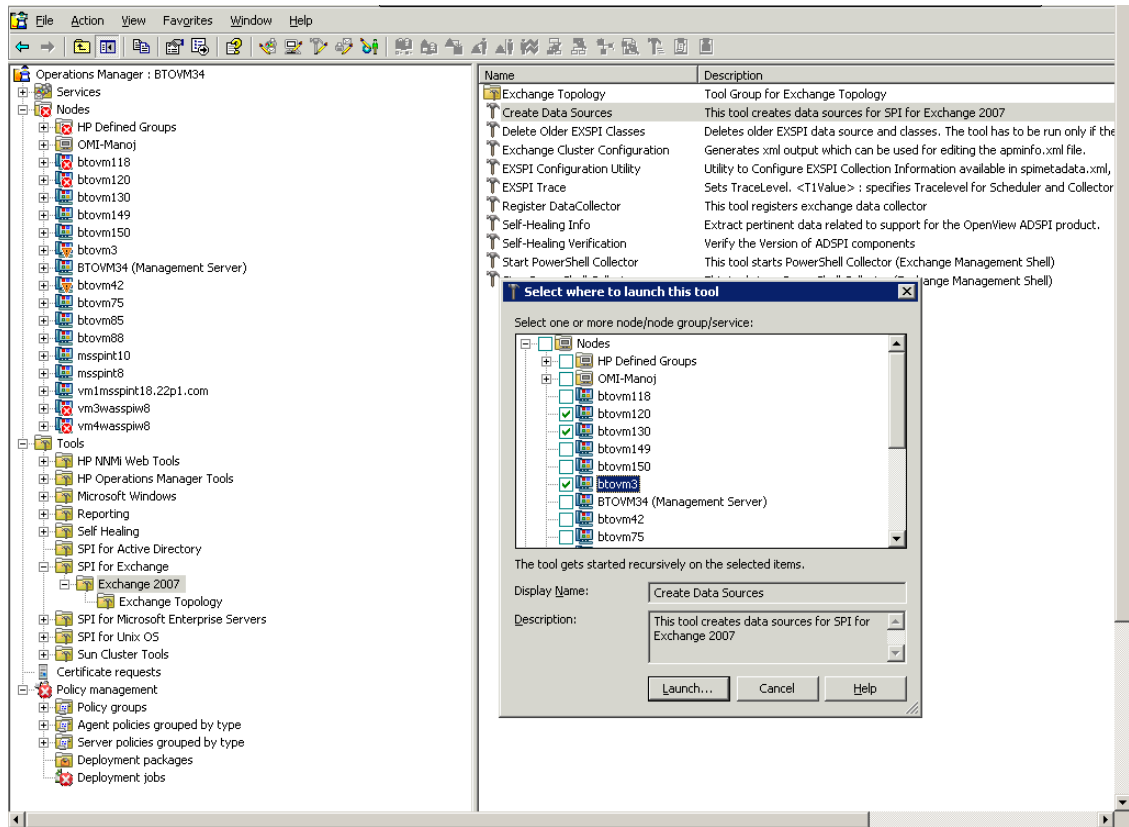
- 1 Expand **Tools** → **SPI for Exchange** → **Exchange 2007**. The tools of the Microsoft Exchange SPI are displayed.
- 2 Double-click the Start PowerShell Collector tool. A window displays all the managed nodes.
- 3 Select the Exchange managed nodes, and then click **Launch...** The Start PowerShell Collector tool starts on the selected nodes.

- ▶ The Start PowerShell Collector tool does not return any output. The status of the tool continues to display *Starting*. To check if the Collector has started, close the tool output and check the Task Manager on the managed node.

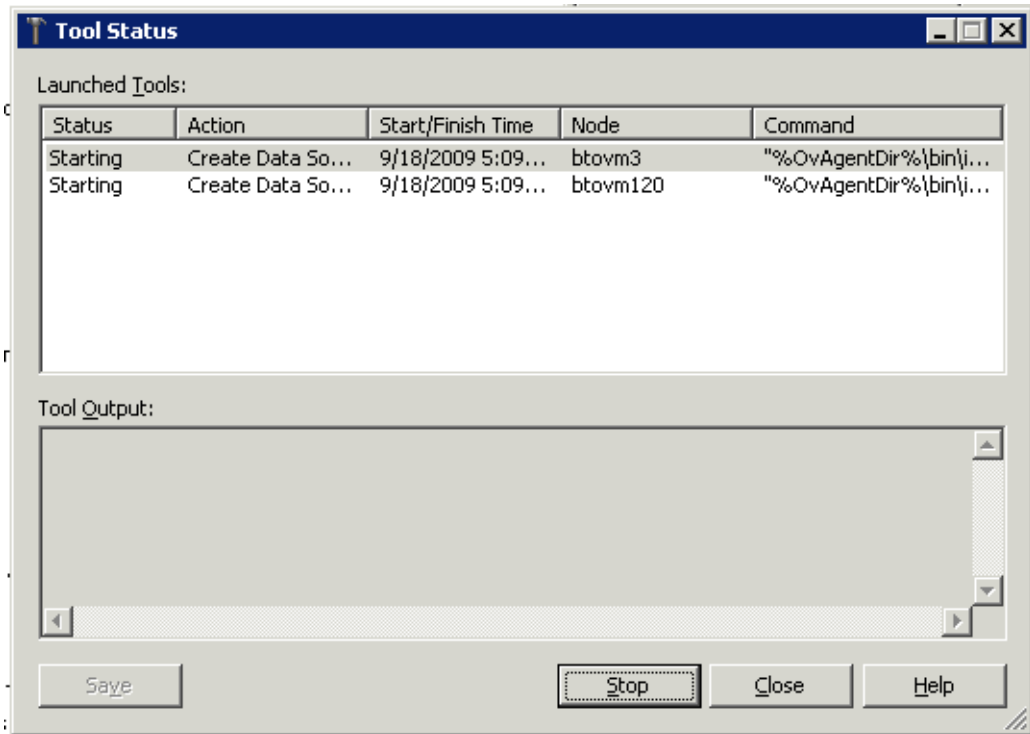


To start Create Data Sources and Register DataCollection tools:

- 1 Expand **Tools** → **SPI for Exchange** → **Exchange 2007**. The tools of the Microsoft Exchange SPI are displayed.
- 2 Double-click the **Create Data Sources** tool. A window displays all the managed nodes.



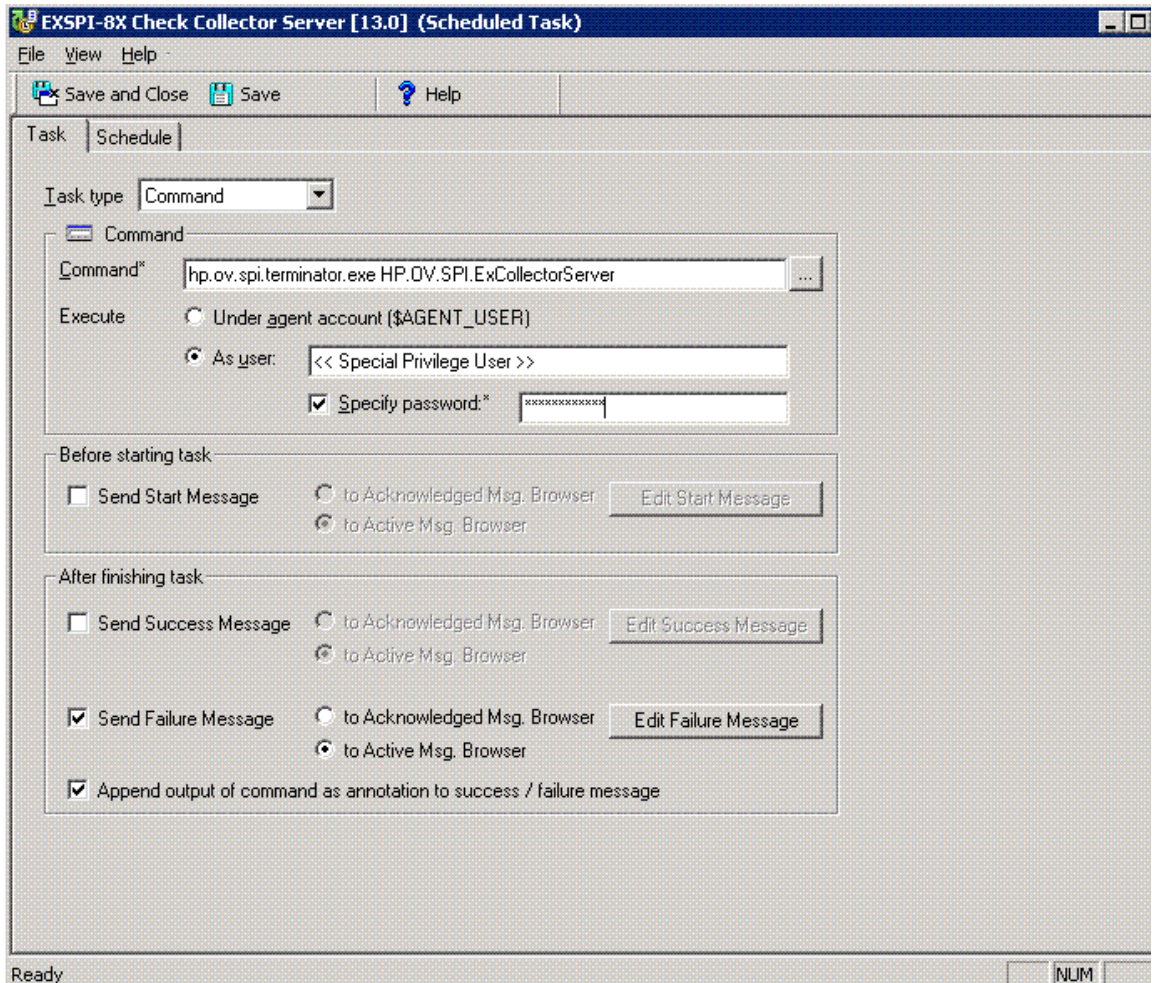
- 3 Select the Microsoft Exchange managed nodes, and then click **Launch...** The Create Data Sources tools starts on the selected nodes.



- 4 Perform steps 1 through 3 for the Register DataCollection tool.

## Specify the Credentials for EXSPI-8X Check Collector Server Policy

Specify the same credentials of the user who starts the Start PowerShell Collector tool for the policy EXSPI-8X Check Collector Server. To know the details of the privileges which the user must have, see [Start PowerShell Collector](#)



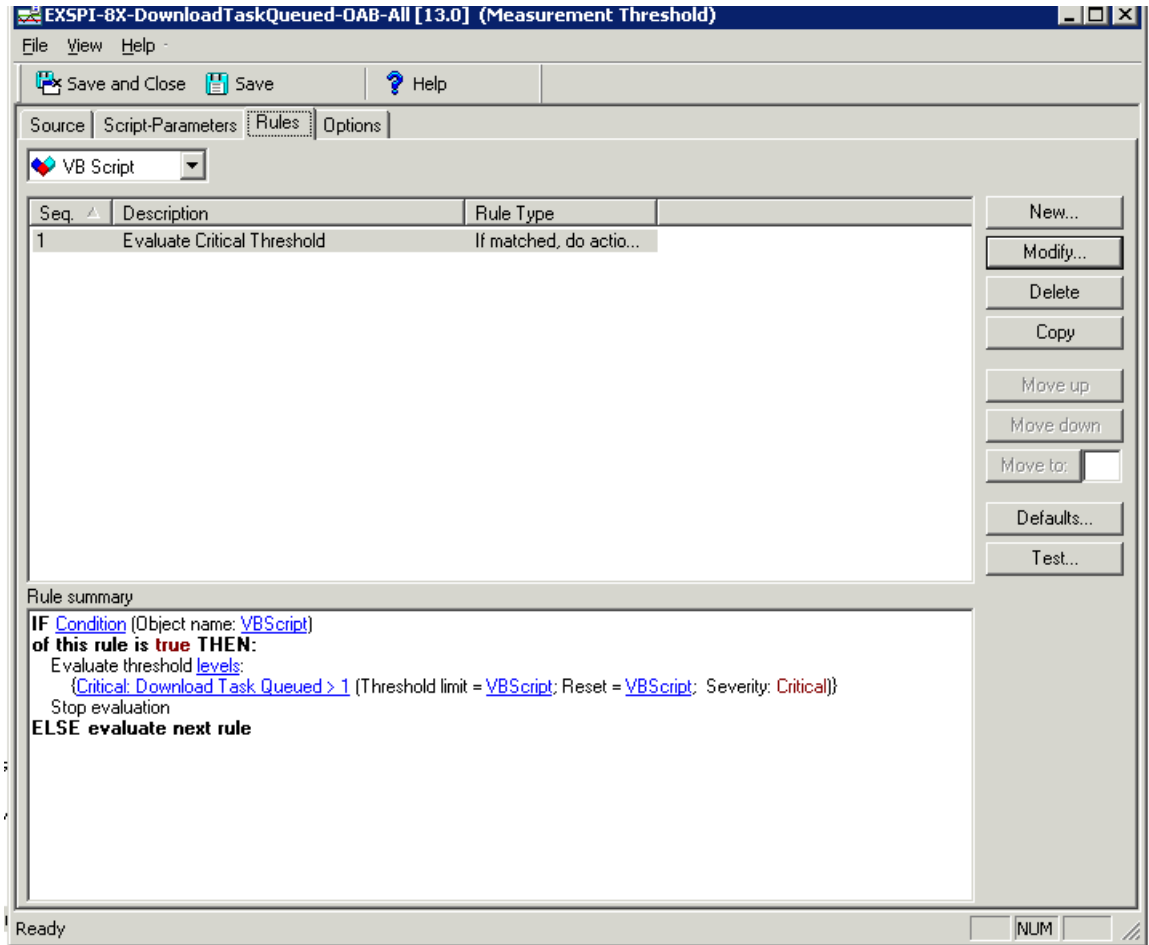
To specify the credentials, select the **As User** button. Specify the credentials of the user and save the policy.

## Customize policies

You can customize the Microsoft Exchange SPI policies, if required. To customize policies:

- 1 Right-click the policy and select **All Tasks**, and then **Edit...**
- 2 Click the **Thresholds level** or **Options** tab or both to customize. Set the required thresholds and other options, if required.

3 Click **Save and Close**.



4 Redeploy the customized policies, if you have customized the policies after deploying them.

- ▶ Use Software Upgrade Tool Kit 2.0 to retain the customization of the earlier versions of the Microsoft Exchange SPI policies. See *HP Operations Smart Plug-in Upgrade Toolkit Windows User Guide* for more details.

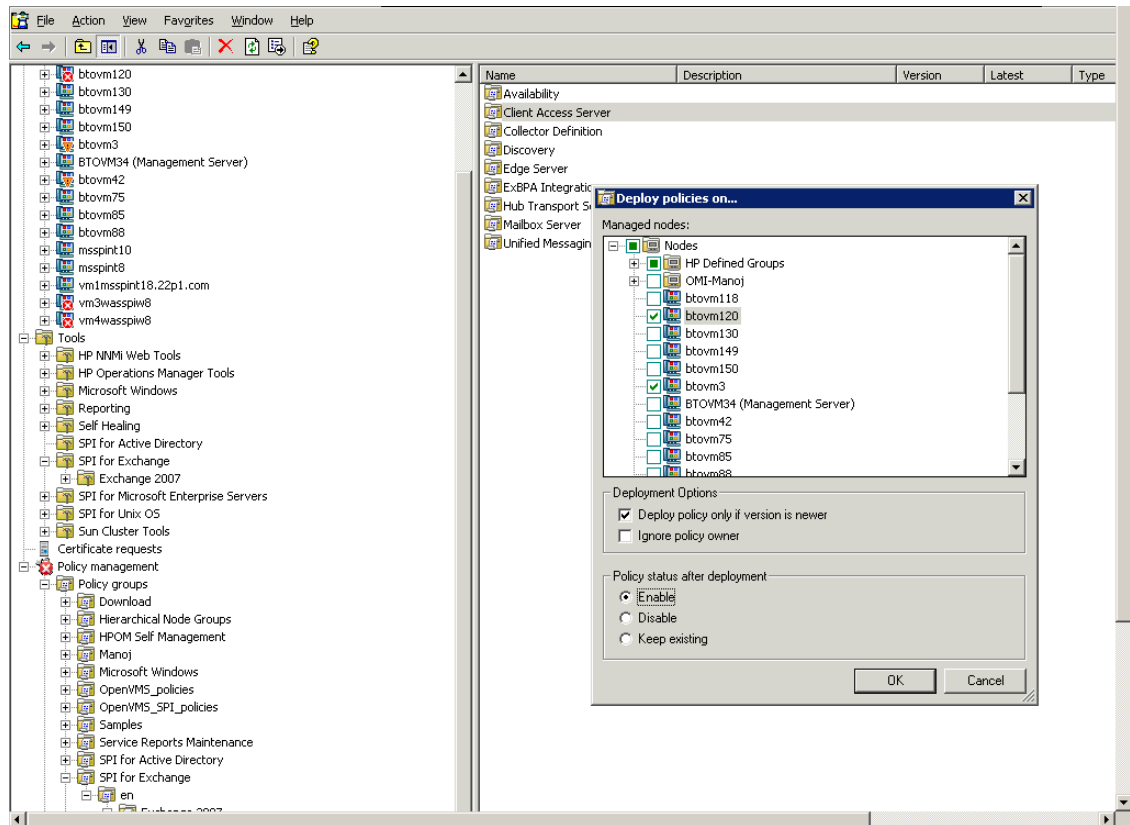
## Deploy Microsoft Exchange SPI policies on Managed Nodes

- ▶ Configuration Deployment fails, if powershell prompt, with EXSPI pssnapin loaded, is kept open on managed node.

If the Microsoft Exchange server nodes run on a cluster environment, perform the steps as described in [Edit Discovery Policy](#) on page 39.

- 1 In the console tree of the HPOM console, expand **Policy Management** → **Policy Groups** → **SPI for Exchange** → **en (ja)** → **Exchange 2007** → **Manual Deploy Groups**.
- 2 Right-click the **<Policy Group>**. Select **All Tasks** → **Deploy on.... Deploy policies on...** Window appears listing all the managed nodes.

- 3 Select one or more Exchange managed nodes on which you want the <Policy Group> to be deployed, and then click **OK**. The <Policy Group> is deployed on the selected nodes which host the appropriate server role.



- 4 Ensure to select the policy status after deployment as **Enable**.



Assign only those policy groups on the managed nodes which host the roles that the policy group is related to. For example if the managed node hosts the Edge Server, deploy only the Edge Server policy group, and so on.

See Table 3 to deploy the specific policy group for the specific Exchange server. Server Role and the Policy Group to be deployed.

**Table 3 Server Role and Policy Group**

<b>Server Role</b>	<b>Policy Group</b>
Mailbox Server	<b>Policy Management → Policy Groups → SPI for Exchange → en (ja) → Exchange 2007 → Manual Deploy Groups → Mailbox Server</b>
Hub Transport Server	<b>Policy Management → Policy Groups → SPI for Exchange → en (ja) → Exchange 2007 → Manual Deploy Groups → Hub Transport Server</b>
Edge Transport Server	<b>Policy Management → Policy Groups → SPI for Exchange → en (ja) → Exchange 2007 → Manual Deploy Groups → Edge Server</b>
Client Access Server	<b>Policy Management → Policy Groups → SPI for Exchange → en (ja) → Exchange 2007 → Manual Deploy Groups → Client Access Server</b>
Unified Messaging Server	<b>Policy Management → Policy Groups → SPI for Exchange → en (ja) → Exchange 2007 → Manual Deploy Groups → Unified Messaging Server</b>

Deploy the following policy groups for *all* the managed nodes irrespective of the specific server role:

- Discovery  
**Policy Management → Policy Groups → SPI for Exchange → en (ja) → Exchange 2007 → Manual Deploy Groups → Discovery**
- Availability  
**Policy Management → Policy Groups → SPI for Exchange → en (ja) → Exchange 2007 → Manual Deploy Groups → Availability**
- Collector Definition  
**Policy Management → Policy Groups → SPI for Exchange → en (ja) → Exchange 2007 → Manual Deploy Groups → Collector Definition**



Edit the EXSPI-8X Check Collector Server policy to run with the same privileges as required to run the Start PowerShell Collector tool. For more details, see the privileges (for the Start PowerShell tool) mentioned in [Run Tools - Create DataSources, Register DataCollector, and Start PowerShell Collector](#).

- ExBPA Integration  
**Policy Management → Policy Groups → SPI for Exchange → en (ja) → Exchange 2007 → Manual Deploy Groups → ExBPA Integration**

## Data Logging Scenarios

If you use Performance Agent as the datastore, data source creation and data logging happens in Performance Agent, by default. There is no configuration required.

To create data sources and to log data into CODA, while Performance Agent is installed, perform the following steps:

- 1 Create a folder `dsi2ddf` in the path `%OvAgentDir%\Conf`, if it does not exist.
- 2 Create an empty file `nocoda.opt`.
- 3 Enter the names of the other data sources *except* `EX2007_DATA`, which are to be created and for which the data logging has to happen in Performance Agent into the file `nocoda.opt`.

The data source `EX2007_DATA` is created and data logging happens in CODA.

For more details on the data store (CODA) metrics and policy logging details, see *HP Operations Smart Plug-in for Microsoft Exchange Server Online Help*.

## Discovery Configuration Scenario

The Microsoft Exchange SPI discovers the services of the Microsoft Exchange 2007 Server and helps you to manage the Microsoft Exchange environment. Perform the tasks in the following sections to discover the Microsoft Exchange services.

### Edit Discovery Policy

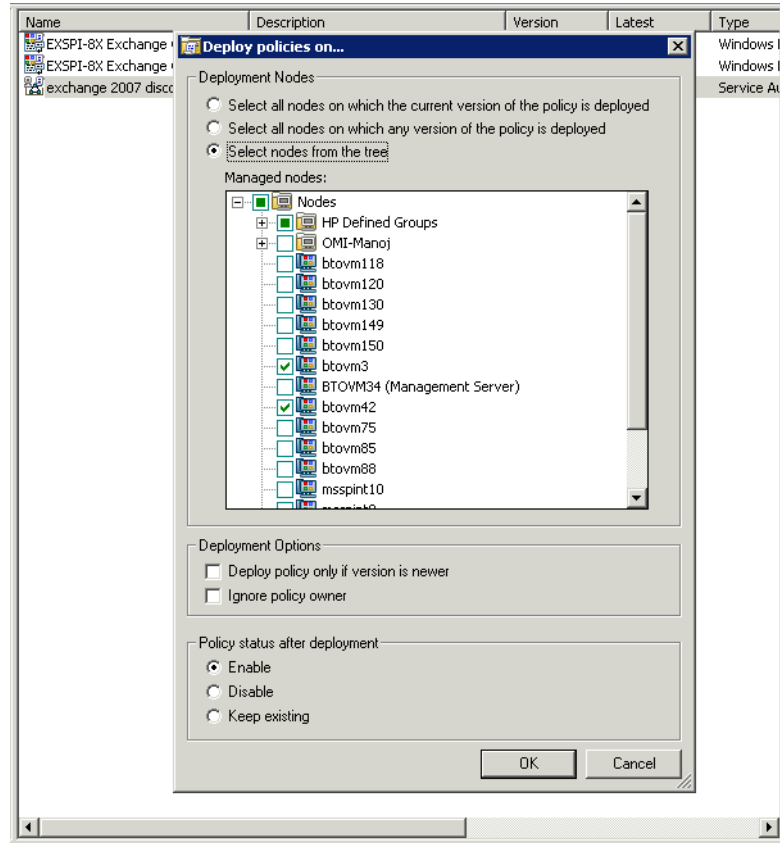


Perform the following steps *only for the clustered Exchange server nodes*.

Edit the Microsoft Exchange SPI Discovery policy by performing the following steps:

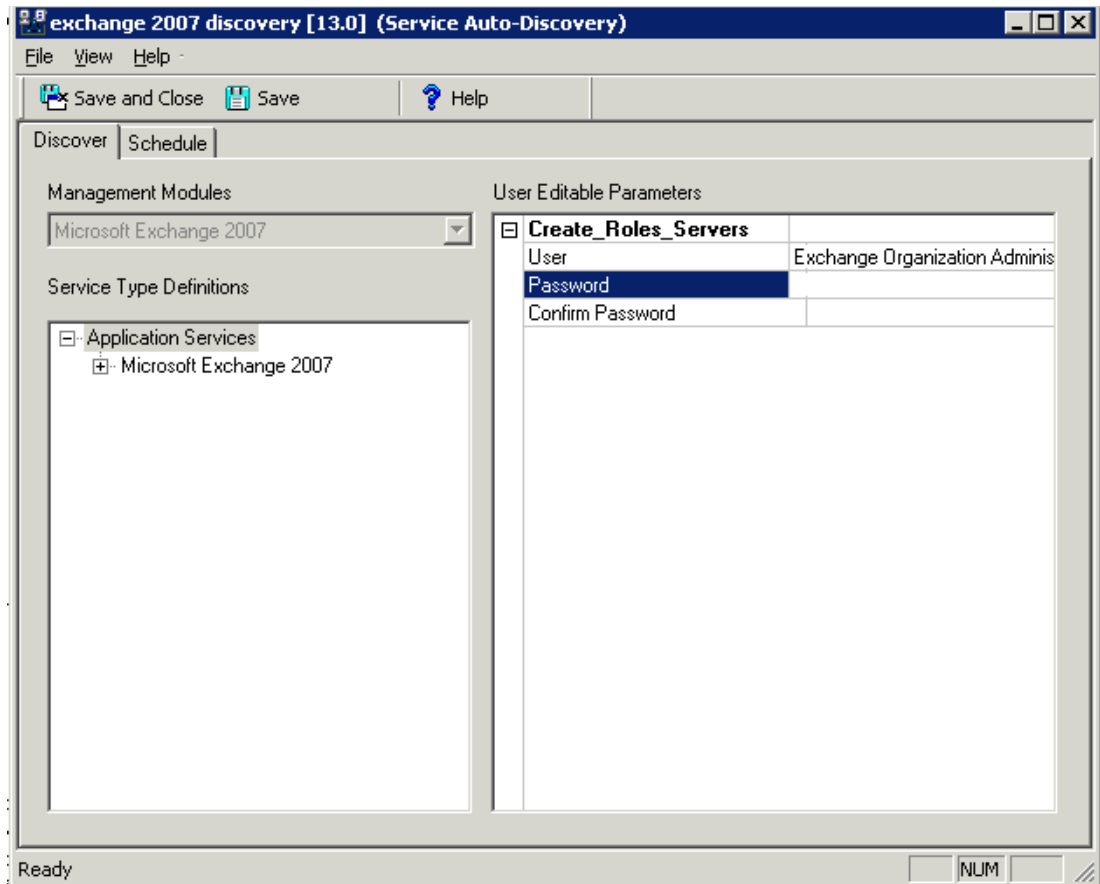
- 1 In the console tree of the HPOM console, expand **Policy Management** → **Policy Groups** → **SPI for Exchange** → **en (ja)** → **Exchange 2007** → **Manual Deploy Groups** → **Discovery**.
- 2 Right-click **exchange 2007 discovery** from the pane.
- 3 Select **All Tasks**, and then click **Edit...** The Discovery tab appears to enable you to enter the required credentials.

- 4 Ensure to select the policy status after deployment as **Enable**.





- 5 Type the credentials of an Exchange Organization Administrator, and click **Save and Close**.

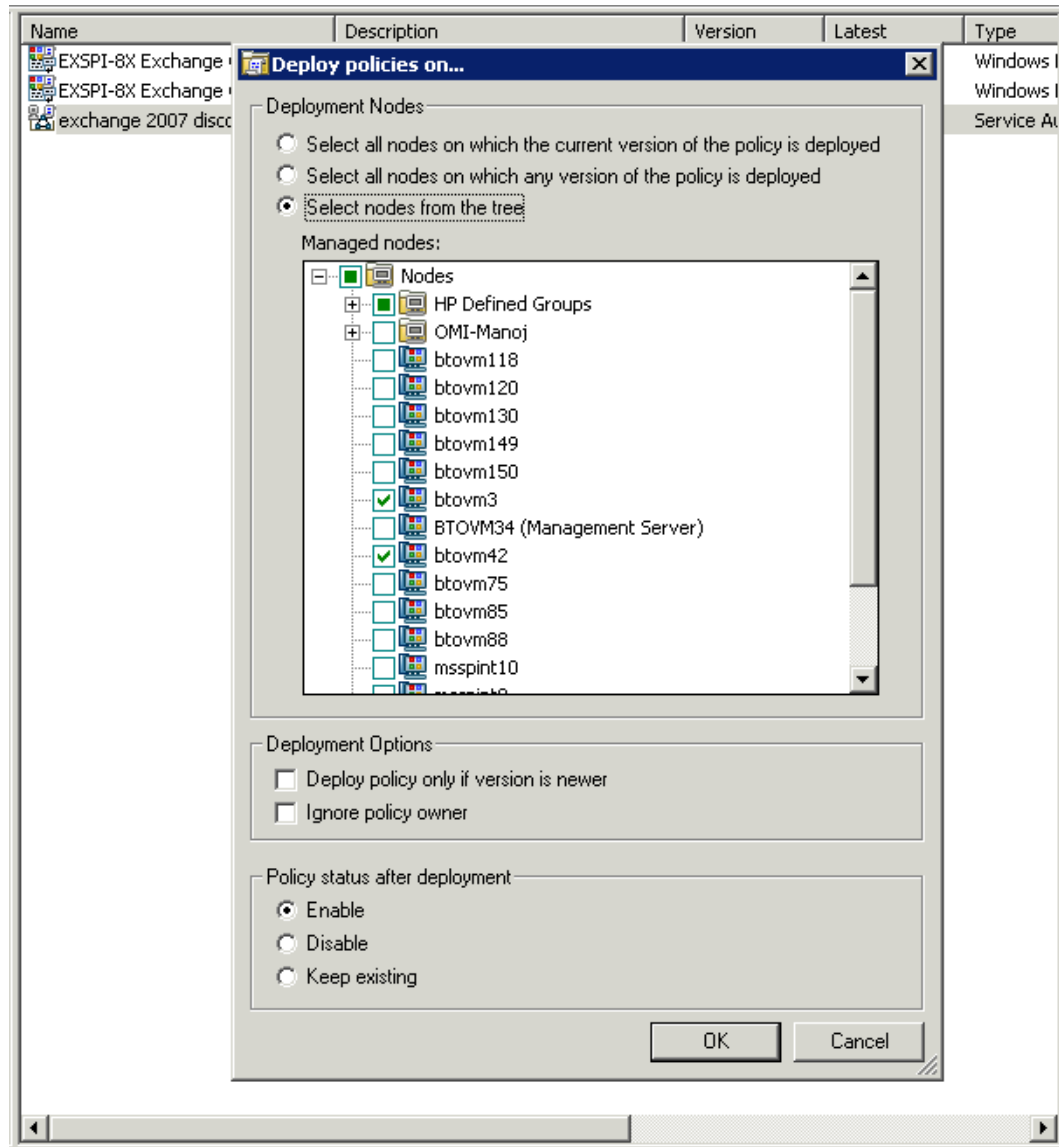


## Deploy Discovery Policy to Managed Nodes

Deploy the Exchange 2007 Discovery policy on the Exchange nodes. To deploy the discovery policy:

- 1 In the console tree of the HPOM console, expand **Policy Management** → **Policy Groups** → **SPI for Exchange** → **en (ja)** → **Exchange 2007** → **Manual Deploy Groups** → **Discovery**.
- 2 Right-click **exchange 2007 discovery** from the pane.
- 3 Select **All Tasks**, and then click **Deploy on....** All the managed nodes are listed.

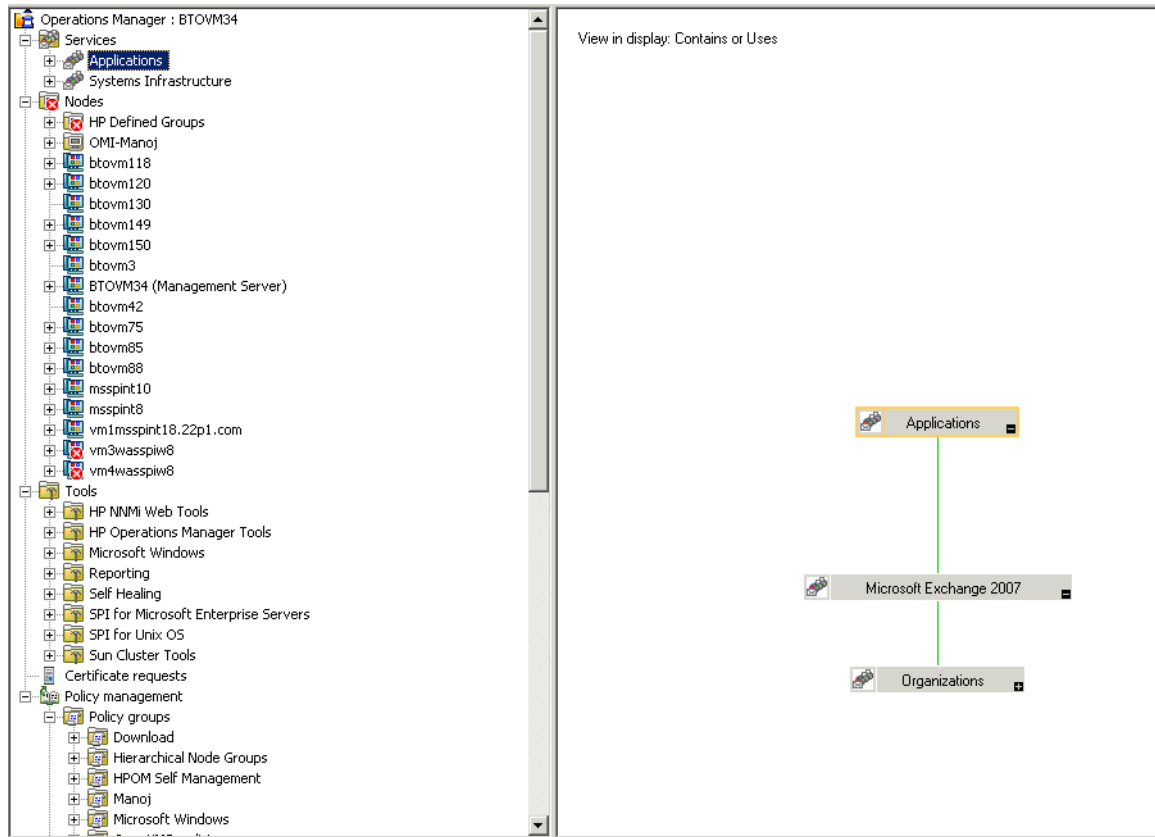
- 4 Select the Exchange nodes where you want to deploy the discovery policy and then click **OK**.



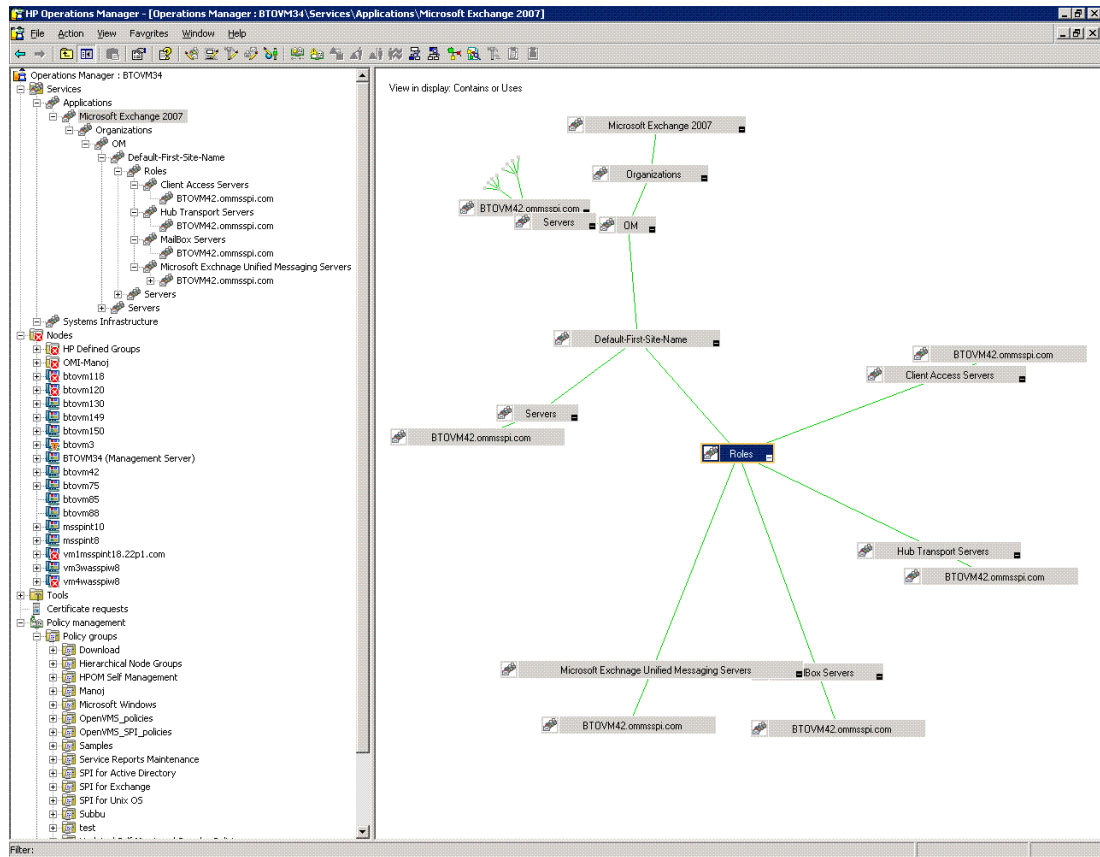
- 5 Ensure to select the policy status after deployment as **Enable**.

## View the Service Map

You can view the service map through the HPOM console. To view the updated services of the Microsoft Exchange 2007 server, expand **Services**, and, then click **Applications**. The map appears on the right pane.



The service map shows the newly discovered services of the Microsoft Exchange Server 2007. Expand the hierarchy to view the specific services and the Exchange managed nodes.



## Additional Configuration Procedure

You can enhance the monitoring capabilities of the Microsoft Exchange SPI on the Microsoft Exchange Server 2007 nodes by customizing the data collection configuration. The Microsoft Exchange SPI data collectors follow a pre-defined data collection configuration to monitor the managed nodes.

Use the pre-defined data collection configuration to monitor the managed nodes. You can add new configuration to the default configuration for the Microsoft Exchange SPI data collector to use. You can create and modify those new data collection configuration.

## Functions of EXSPI Data Collectors

The pre-defined data collection configuration is described in an XML file named as `spimetadata.xml`. Deploy the **EXSPI-8X SPIMetaData Versioning** policy of Collector Definition policy group to use the `spimetadata.xml` file. The EXSPI data collectors follow the data collection configuration as defined in the `spimetadata.xml` file. This file consists of a

component, that is, collection, which determines the data which is to be collected by an EXSPI data collector. The data collection configuration describes the complete workflow of collecting, storing, and alerting.



The EXSPI Data collector can collect *only* the data from Cmdlets available on the managed node.

A data collection configuration consists of the following components or building blocks:

- *MetricSet* — A metric is a measurement that defines a specific operational or performance characteristic of a system or an application. A MetricSet is a group of related metrics.
- *OpCMsg Calls* — An OpCMsg Call generates an alert message when a metric value does not match a pre-set value or range of values.
- *OpCMon Calls* — An OpCMon Call sends the collected data to a measurement threshold policy. The measurement threshold policy checks the data against some upper or lower threshold as defined within the policy and sends alarm to the message browser.
- *Data Store* — A Data Store defines the way in which the collected data can be stored into the data store (CODA or PA).

Each data collection configuration is associated with a scheduled task policy. Each collection is associated with a unique integer value called the collection ID. A request must be sent to the EXSPI Data Collector with the ID as one of the parameters to start the collection process. This is performed by the schedule task policy for each collection which executes a command **HP.OV.SPI.ExScheduler -CID <ID>**.

When you deploy a scheduled task policy on a managed node, the EXSPI data collector retrieves the following details from the data collection configuration:

- The cmdlets to be executed and the metrics to be collected from the Resultset.
- The name of the data store where the collected data is to be logged.
- The name of the monitor policy to which a particular metric has to be passed. This policy performs the threshold on this metric value.
- The set of rules in the `spimetadata.xml` file to be applied on the metrics and if required generate `opcmsg`.

## EXSPI Configuration Utility Tool

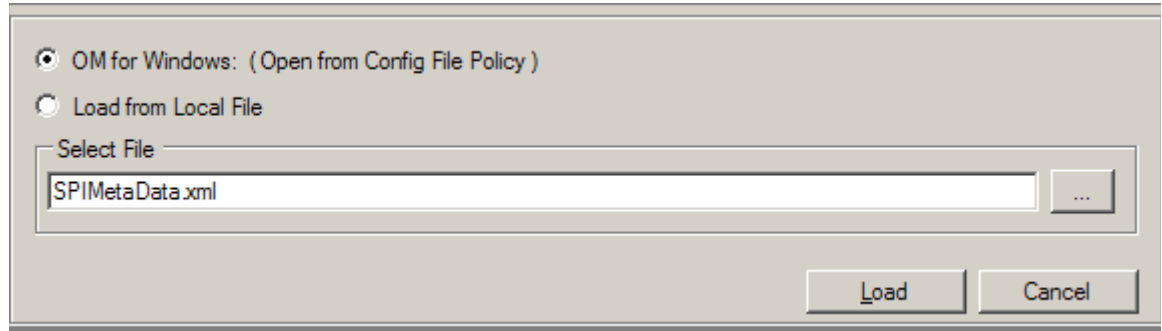
The Microsoft Exchange SPI provides a tool named EXSPI Configuration Utility to modify the default data collection configuration specified in the `spimetadata.xml` file on the Microsoft Exchange Server 2007 nodes by adding new data collection through its graphical user interface. You can add the components of the data collection configuration—MetricSet, OpCMsg Calls, OpCMon Calls, and data store—and modify the newly created collection configuration to monitor the managed nodes.

## Using EXSPI Configuration Utility

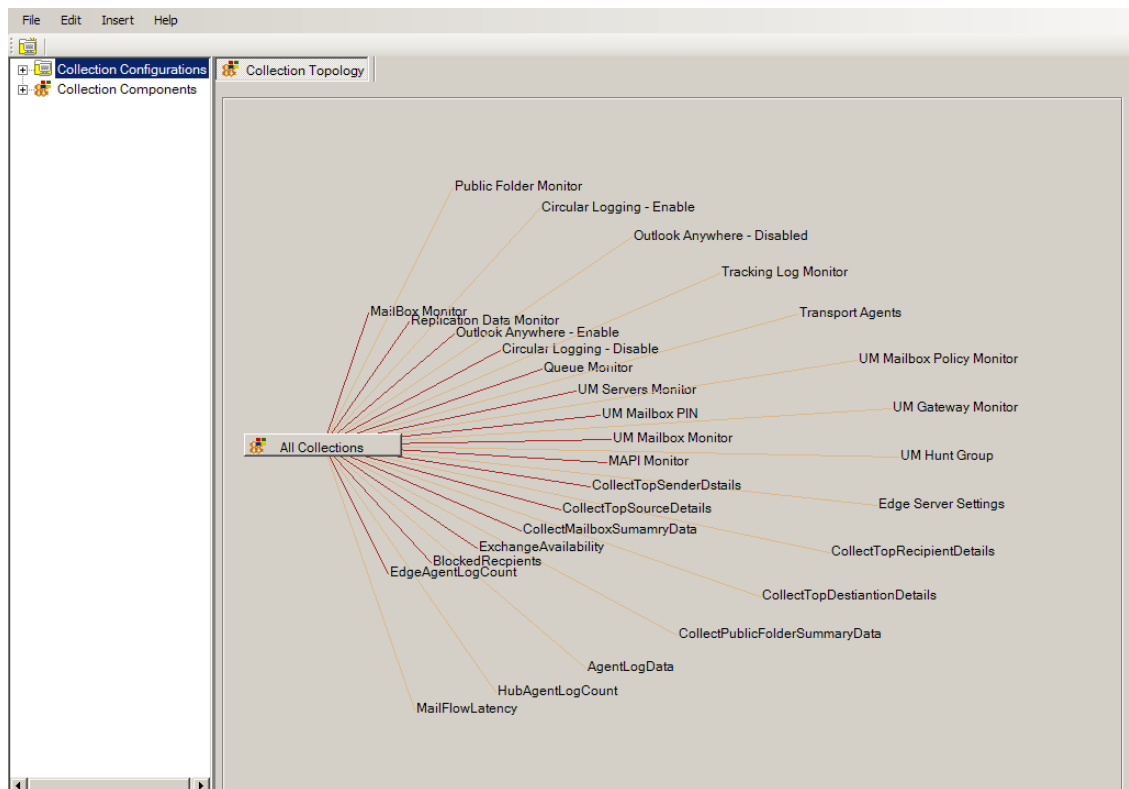
To start the EXSPI Configuration Utility tool:

- 1 In the console tree, expand **Tools** → **SPI for Exchange**, and double-click **Exchange 2007**.
- 2 In the details pane, double-click **EXSPI Configuration Utility**. The Select Server dialog box opens.

- 3 Select the **OM for Windows Server** option, and click **Load**.



- 4 The EXSPI Configuration Utility tool starts displaying the collection topology.



- ▶ **Open from Config File Policy** option cannot be used on a Operations Manager for Windows - Remote Console. Edit the configuration from local SPIMetaData.xml, update the policy EXSPI-8X SPIMetadadata Versioning and re-deploy to managed nodes.

## Viewing the EXSPI Configuration Utility

The EXSPI Configuration Utility provides you with a graphical user interface to perform necessary tasks to create new data collection configuration. The graphical user interface consists of the following elements:

- Menu bar
- Toolbar
- Left pane and right pane

## EXSPI Configuration Utility Menubar

You can use the menu options in the menu bar to perform tasks like adding and removing an element of collection definition. You can also view a preview of every element (in the form of XML markups) by using the Preview menu option.





**Table 4 EXSPI Configuration Utility Menubar**

<b>Menu</b>	<b>Options</b>	<b>Description</b>
File	Save	Saves any changes that you make.
	Save as	Enables you to save the updated <code>spimetadata.xml</code> file on a different location and with a different name.
	Reload/ Cancel All Changes	Reloads the utility, cancels all unsaved changes.
	Exit	Exits the PowerShell collection configuration utility.
Edit	Delete Selected Collection	Deletes the selected collection configuration or component from this menu.
Insert	Add New MetricSet	Adds a new MetricSet to the list of available MetricSets.
	Add New Metric	Adds a new Metric to the list of available metrics in a particular MetricSet. This option is enabled only when you select a MetricSet.
	Add New Collection	Adds a new collection to the list of available collections.
	Add New DataStore	Adds a new DataStore to the list of available DataStores.
	Add New OpCMon Call	Adds a new OpCMon Call to the list of available OpCMon Calls.
	Add New OpCMsg Call	Adds a new OpCMsg Call to the list of available OpCMsg Calls.

## EXSPI Configuration Utility Toolbar

You can use the toolbar to add references to the collection elements—MetricSets, DataStores, OpCMsg Calls, and OpCMon Calls.

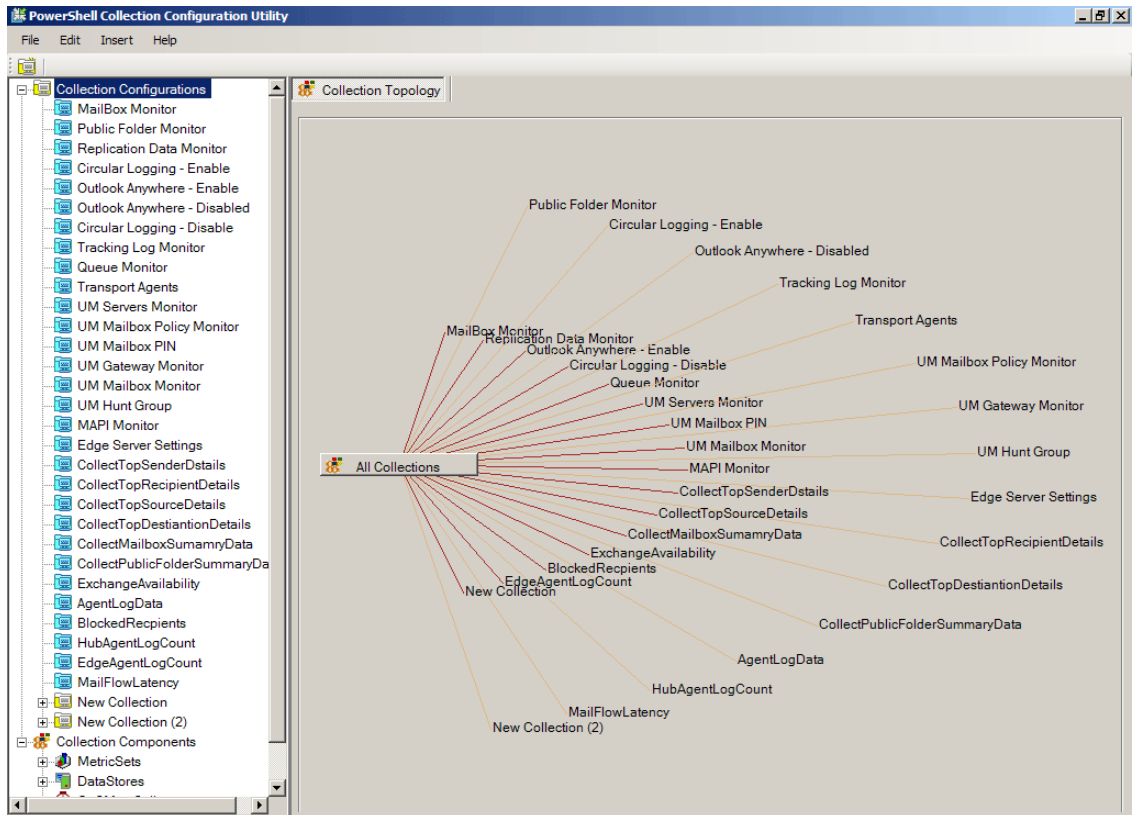
**Table 5** EXSPI Configuration Utility Toolbar

Icon	Tool Name
	Add MetricSet
	Add DataStore
	Add OpCMsg Call
	Add OpCMon Call



## EXSPI Collection Configuration Utility Panes

The left pane lists all available metrics, MetricSets, collections, DataStores, OpCMsg Calls, and OpCMon Calls in a tree like structure. You can navigate to specific collection elements with the help of the left pane. The right pane provides you an interface to view and modify properties and settings for every collection element.



- ▶ If you modify the EXSPI Configuration Utility tool, ensure to deploy the EXSPI-8X SPIMetaData Versioning policy on the managed nodes where the changed data collection mechanism takes effect. Even if you revert to the previous version of the EXSPI-8X SPIMetaData Versioning policy, the GUI shows the latest version.

## Saving Collection Configuration

There are two options for saving the updated collection configuration:

- **File** → **Save**
- **File** → **Save As**

## File and Save Option

When you open the file from the following location:

- From **OM for Windows** option: The configuration is read from the EXSPI-8x SPIMetadata Versioning policy. When you save the updated configuration, the data is written back to the policy. This updates the version of the policy.

To make this configuration available on the node, redeploy the policy.

▶ Since every time you save the file, a new version gets created, avoid saving the file very often to limit the numerous versions of the file.

- From the local disk: No versions are maintained if you save the file from local disk as the latest file overwrites the previous file.

## File and Save As Option

When you click **Save** → **Save As**, the file is saved irrespective of its location in the local disk. The **Save As** option, however, enables you to save only the local copy.

## Adding Collection Data

The EXSPI Configuration utility tool enables you to add the following components:

- MetricSet
- OpCMsg Call
- OpCMon Call
- DataStore
- Collection

▶ Do not modify any default MetricSet or data store or both. You can however modify the newly added MetricSet, the DataStore, OpCMsg Call, and OpCMon Call.

## Adding a MetricSet

A MetricSet is a group of related metrics. The Microsoft Exchange SPI collects these metrics to monitor the health, availability, and performance of Microsoft Exchange Server 2007.

Each MetricSet can execute a Powershell command. The Powershell command can either be a single Cmdlet or a pipeline of Cmdlets. You can use either or all of the following Cmdlets:

- Default Powershell Cmdlets
- Microsoft Exchange Cmdlets
- EXSPI Internal Cmdlets
- User created cmdlets (See [Using Additional Cmdlets](#))

To add a new MetricSet:

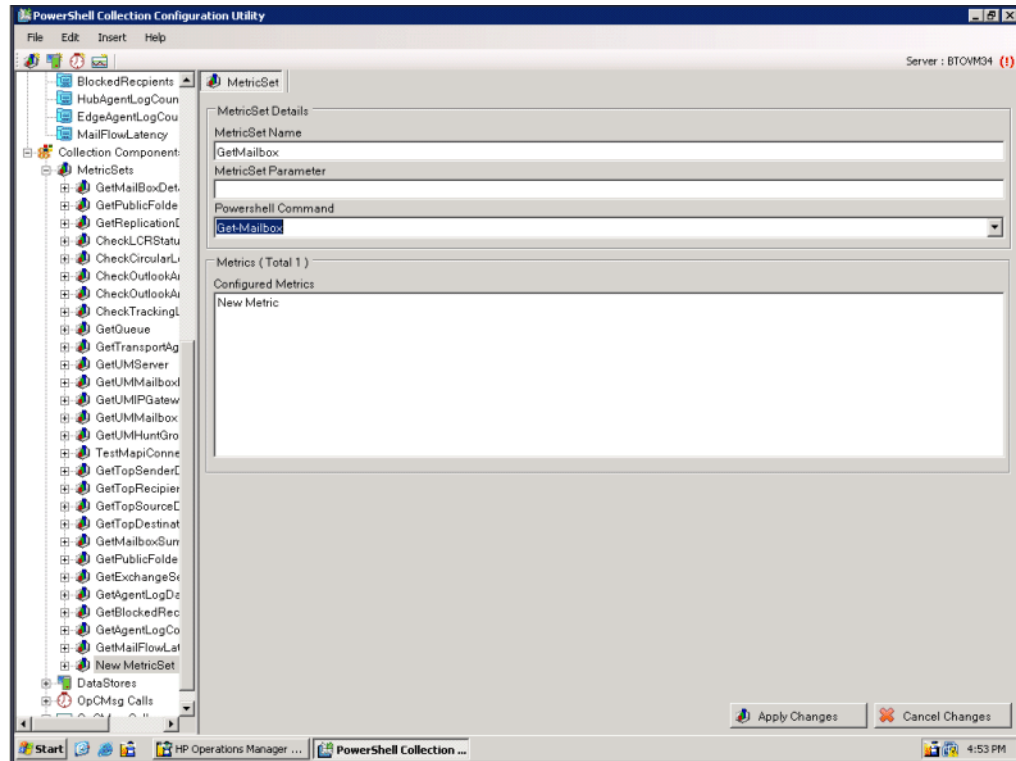
- 1 In the left pane, right-click **MetricSet** from **Collection Components**, and then click **Add New MetricSet** or click **Insert** → **Add New MetricSet** from the menu bar. A new MetricSet (with the name **New MetricSet**) appears in the list of MetricSets.

- In the right pane, specify the MetricSet Name. For example **GetMailBox**. Select the PowerShell command from the drop down.

The list consists of the default Cmdlets available with the Microsoft Exchange Management PowerShell.

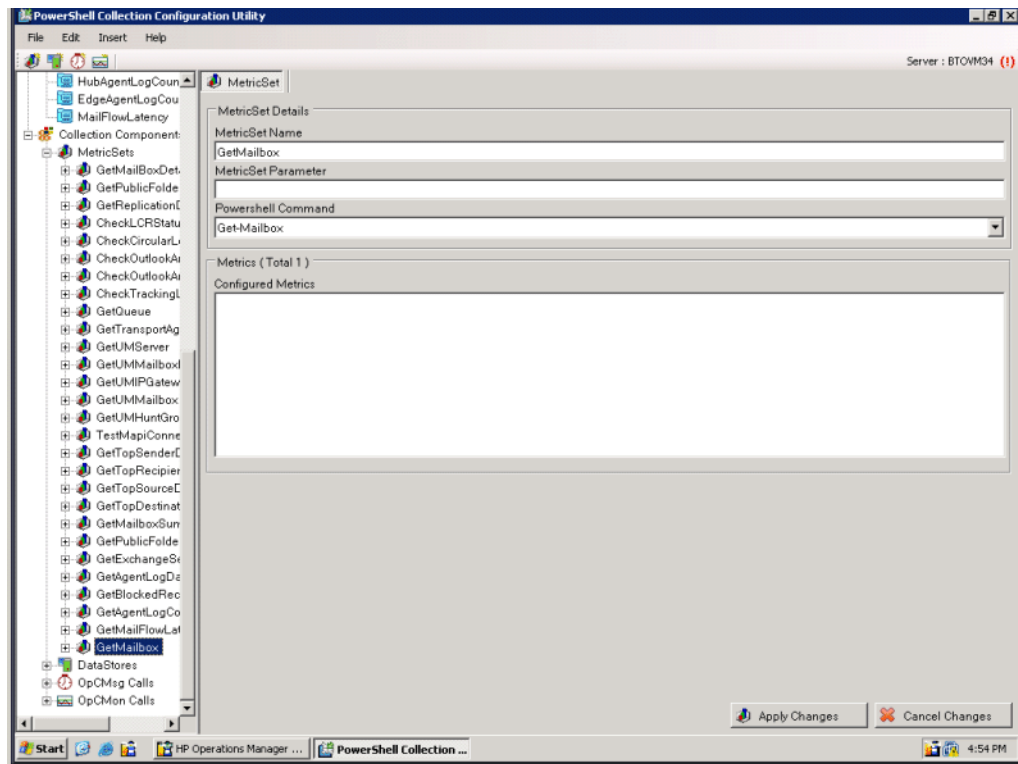


You can use the drop-down option for PowerShell commands *only* for a single command. For more than one PowerShell command (pipelined commands), you must manually type the required commands.



- Click **Apply Changes**.

- 4 Click **File** → **Save**. The added MetricSet (**GetMailBox**) gets listed with the other MetricSets in the left pane.



For the MetricSet GetMailBoxDetails (which is required to collect Mailbox Details), the cmdlet can be Get-Mailbox or if we want to add filter and not want to log System Mailbox Details, it can be "Get-Mailbox | where {\$\_.DisplayName -notlike "SystemMailbox\*" }".

After you add a new MetricSet, the EXSPI Configuration Utility adds a new metric template to the MetricSet. You can create new metrics and add these to the newly created MetricSet.

### Adding a Metric

After you add a MetricSet, you must now add or select metrics from the resultset of the powershell command specified in the MetricSet. If the command is a single Cmdlet, select the metrics from the drop-down list. If the command is pipelined command (more than one cmdlet) type these commands. Then type each metric name from the resultset of the last Cmdlet in the pipeline.

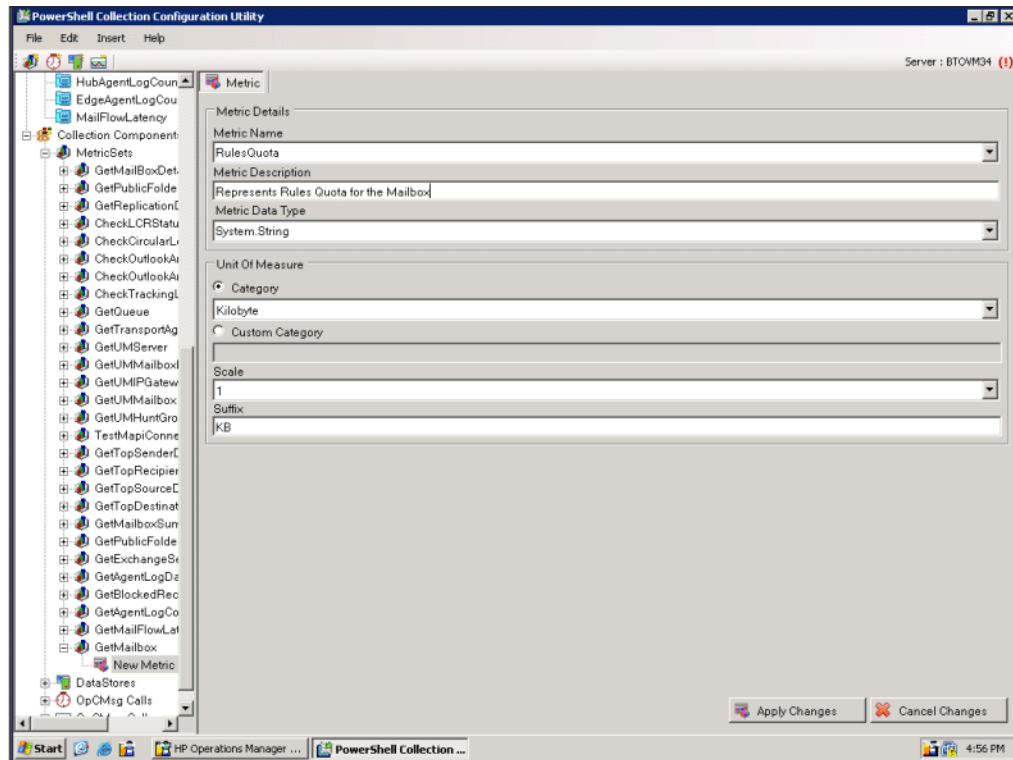
To add a new metric:

- 1 In the left pane, expand **MetricSets** from **Collection Components**.
- 2 Right-click the MetricSet (for example **GetMailbox**), and then click **Add New Metric** or click **Insert** → **Add New Metric** from the menu bar.

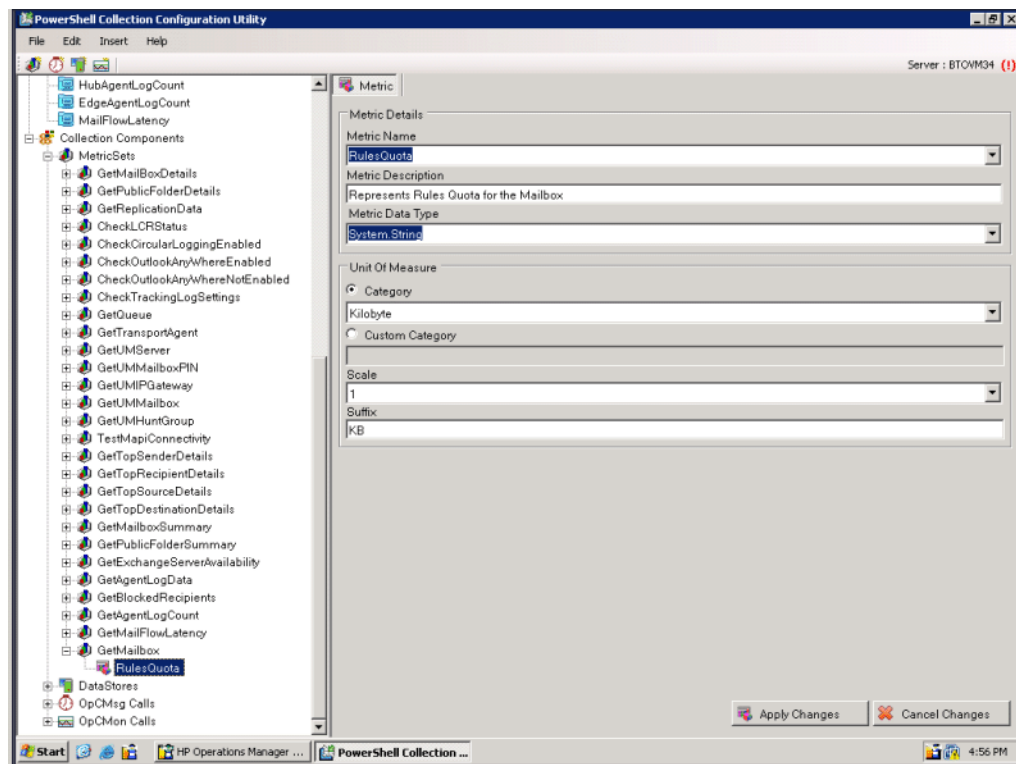
- 3 A new metric (with the name New Metric) appears in the list of metrics under the selected MetricSet enabling you to fill the following options (as shown in the table) on the right pane.

<b>Option</b>	<b>Description</b>
Metric Name	Select a metric name from the drop-down list of the available metrics or type the required metric name if it is not listed in the drop-down list. For example, <b>NextHopDomain</b> .
Metric Description	Type the description of the metric, RulesQuota (Example).
Metric Data Type	After you choose the metric, suitable data type appears by default. Do <i>not</i> change the default setting (RulesQuota). However, if you have typed the metric, then you must type the required metric data type also.

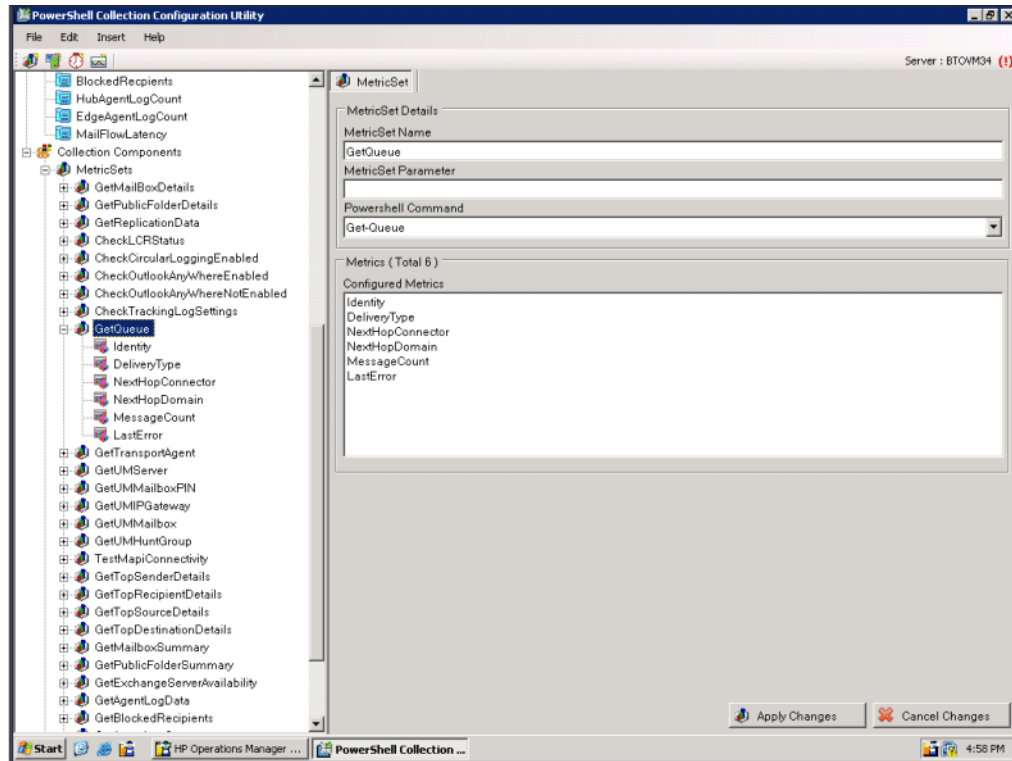
<b>Option</b>	<b>Description</b>
Category	<p>Only in case of metrics which represents bytes/kilobytes you must mention a Category. For Example for the metricset GetMailbox the metric "RulesQuota" returns value in Kilo Bytes (KB). So the category to be selected is KiloByte.</p>
Scale	<p>To convert the metric value to a unit of your choice, specify the multiplying factor. For example, if the metric value is in the form of KB and you want to collect the metric in the form of bytes, specify <b>16</b> (example) in this field. This option is useful for the metrics which are representing the value in Bytes or KB and so on.</p>
Suffix	<p>Specify the element of the metric value that you want to eliminate. For example, if the metric value is appended with the unit B (as in 1200B), you can eliminate B by typing B in the Suffix text box.</p> <p>This option is useful for those metrics which identifies memory size in bytes. Many of the Microsoft Exchange cmdlet metrics which return BYTES/KILOBTYES are suffixed with B/KB. As in the example of "RulesQuota" it is KB. To use the metrics for calculations we must remove the suffix. By mentioning the suffix here the collector removes the suffix from the metric before using it.</p> <p>Specify one suffix for each metric.</p>



- 4 Click **Apply Changes** to save the metric. The added metric RulesQuota is listed in the MetricSet GetMailbox.



- 5 Continue adding the other metrics, if required.



## Adding an OpCMsg Call

If some metric values cross a certain threshold value, you can receive alert messages in the HPOM message browser. The EXSPI Data Collector Configuration enables you to specify the conditions on the metrics of a given metricset to generate alerts through the opcmg call.

An OpCMsg Call is an element of a collection definition, which holds the following information:

- Threshold value (or range of values) for a metric.
- Alert message if the metric does not match the required value or crosses the range of values.
- Severity level (major, minor, normal, warning, and so on) of the event when the metric does not match the limiting value.



You can apply the rules over the metrics for an alert only for a *single* MetricSet.

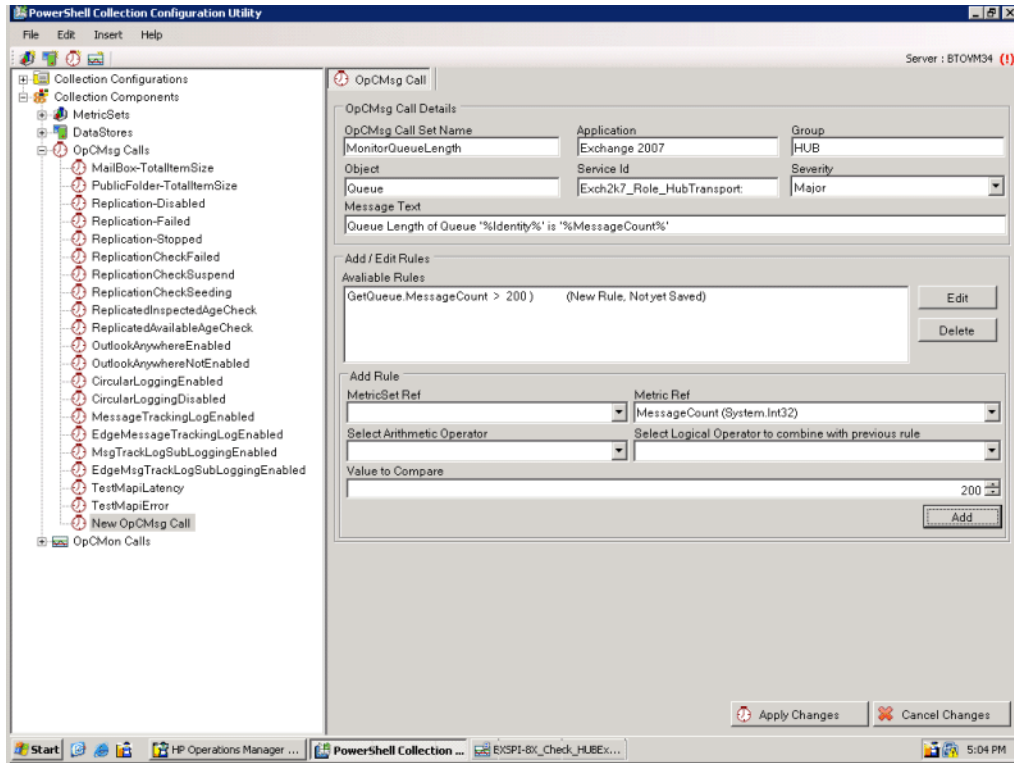


To add a new OpCMsg Call:

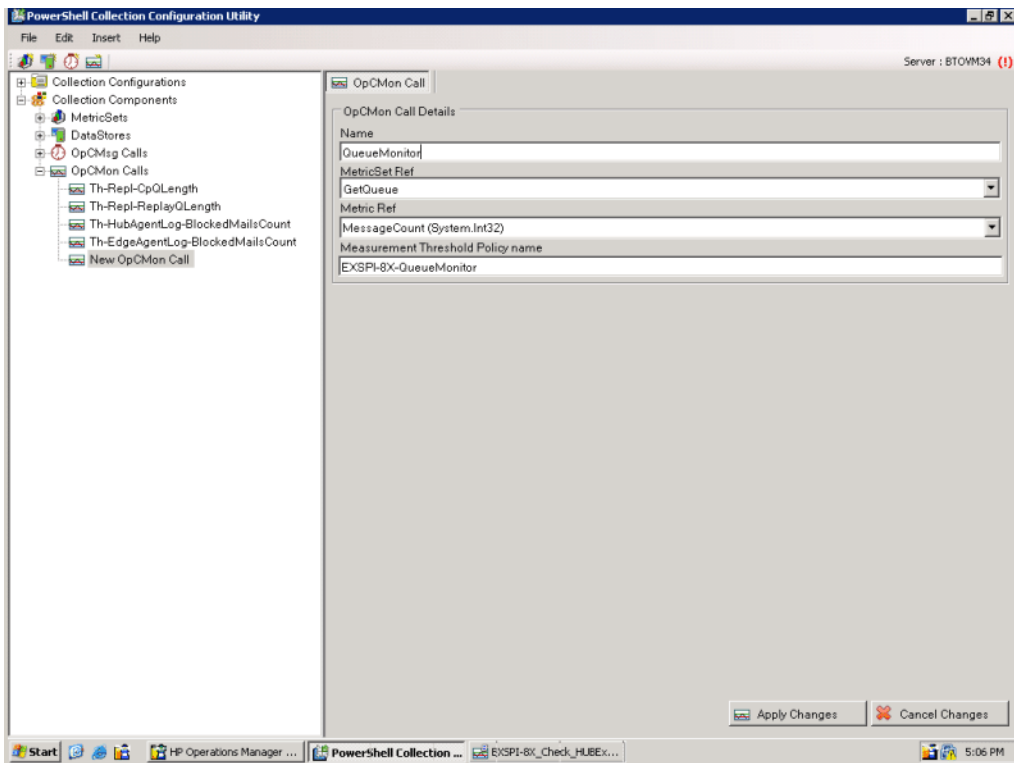
- 1 In the left pane, right-click **OpCMsg Calls** from **Collection Components**, and then click **Add New OpCMsg Call** or click **Insert** → **Add New OpCMsg Call** from the menu bar. A new OpCMsg Call appears in the list in the left pane.
- 2 Fill the following options (as shown in the table) appearing in the right pane.

<b>Option</b>	<b>Description</b>
OpCMsg Call Set Name	Type an appropriate name.
Application	Type an appropriate name of the application that will be affected. You can view this text in the HPOM message browser by opening the Message Properties dialog box. You can leave this field blank.
Object	Type an appropriate name of the object of the application that will be affected. You can view this text in the HPOM message browser by opening the Message Properties dialog box. You can leave this field blank.
Severity	Select the severity level of the event.
Message Text	Type the message that you want to generate.
MetricSet Ref	Select an available MetricSet from the list.
Metric Ref	Select an available metric from the list.
Select Arithmetic Operator	Select an available arithmetic operation from the list.
Select Logical Operator to combine with Previous Rule	This field is enabled only when you choose more than one limiting value or condition for the chosen metrics. Select AND or OR to combine the rules that you create based on the available arithmetic operators.
Value to compare	Select the limiting (threshold) value of the selected metric.

- 3 Click **Add** to add the rules.



- 4 Click **Apply Changes** to save the OpCMsg Call. The added OpCMsg Call GetQueue is listed with the other OpCMsg Calls.



## Adding an OpCMon Call

An OpCMon Call sets a limiting value for metric data through a measurement threshold policy. The Microsoft Exchange SPI retrieves the details like message text and severity from the measurement threshold policy.

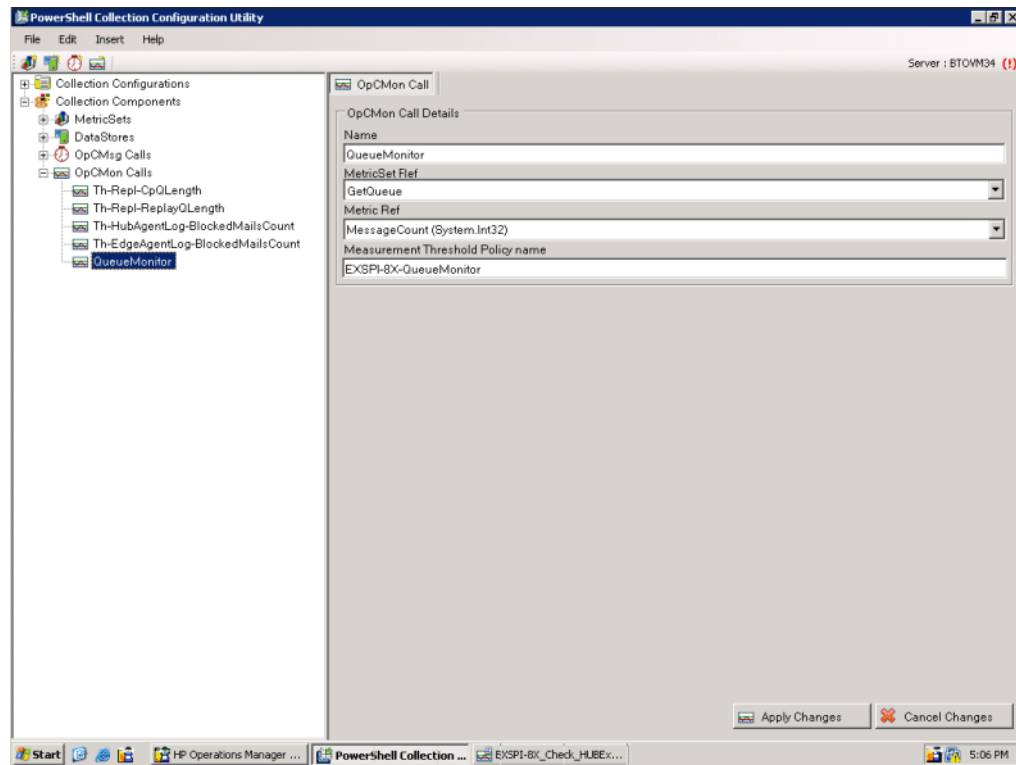


You can use OpCMon Calls only for numeric metric values.

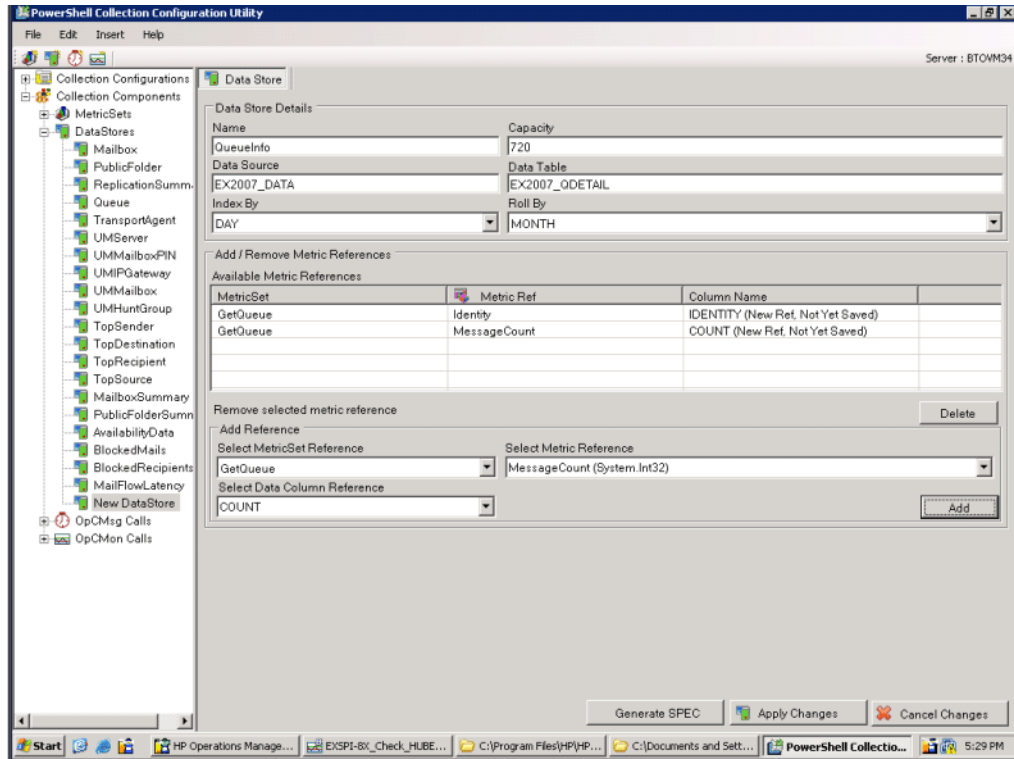
To add a new OpCMon Call:

- 1 In the left pane, right-click **OpCMon Calls** from **Collection Components**, and then click **Add New OpCMon Call** or click **Insert** → **Add New OpCMon Call** from the menu bar. A new OpCMon Call appears in the list in the left pane.
- 2 Fill the following options (as shown in the table) appearing in the right pane.

Option	Description
Name	Type an appropriate name for the OpCMon Call.
MetricSet Ref	Select an available MetricSet.
Metric Ref	Select the metric name for which you want to set the OpCMon Call.
Measurement Threshold Policy Name	Type the name of a measurement threshold policy to which you want to associate this OpCMon Call.



- Click **Apply Changes** to save the OpCMon Call. The added OpCMon Call **TransportQueueCount** is listed with the other OpCMon Calls.



## Adding a DataStore

Data Stores define the way in which you can store metric data. After the Microsoft Exchange SPI collects metric data by using collectors, you can store the collected data either in the HP Operations agent's data store (CODA) or in the HP Performance Agent (PA, if you have it installed in the HPOM environment).

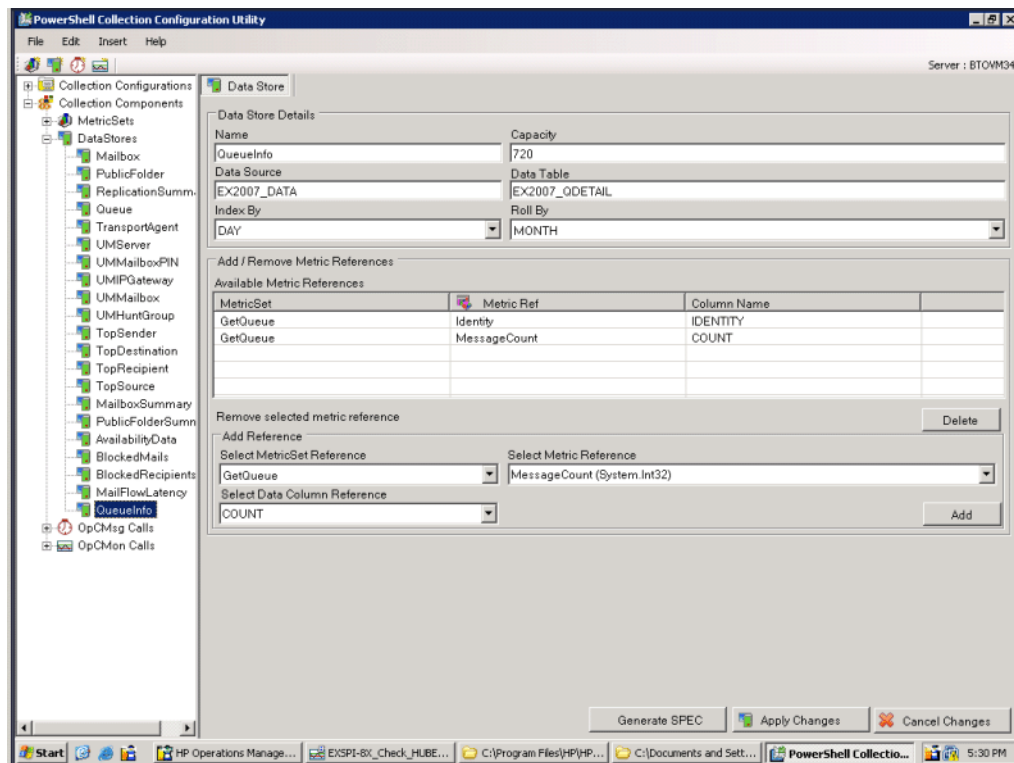
To add a new DataStore:

- In the left pane, right-click **DataStores** from **Collection Components**, and then click **Add New DataStore** or click **Insert** → **Add New DataStore** from the menu bar. A new DataStore appears in the list in the left pane.
- Fill the following options (as shown in the table) appearing in the right pane.

Option	Description
Name	Type an appropriate name for the DataStore.
Capacity	Type the number of rows for the DataStore.
Data Source	Type EX2007_DATA.

Option	Description
Data Table	Type EX2007_<table name>, where <table name> is an appropriate name for the table.
Index By	Set the index on daily, weekly, or monthly schedules.
Roll By	Type the interval at which the data should be flushed out of the data store. You can specify DAY, WEEK, or MONTH. You cannot store data for more than a month.

- From the Select MetricSet reference drop-down list, select the appropriate **MetricSet**.
- From the Select Metric reference drop-down list, select the one or more appropriate metrics.
- In the Select Data column reference box, type a name for the data column in which the DataStore will store the selected metrics. Do not leave this field blank if you want to add more than one metric.
- Click **Add**. You can add only one MetricSet whereas more than one metrics can be added but all the metrics should belong to the same MetricSet.
- Click **Apply Changes** to save the DataStore. The added DataStore QueueInfo is listed with the other DataStores.



After you create a new Data Store, you must add it to an existing collection configuration. See [Adding a Collection Configuration](#) to add a collection configuration. After adding the newly created Data Store to an existing collection configuration, perform the following steps:

- 1 Go to the newly created DataStore.
- 2 In the right pane, click **Generate SPEC**. The Spec File Generator dialog box opens.
- 3 In the Spec File Generator dialog box, type an appropriate label name in the Table Label text box, and then click **Create**. The details of the SPEC file appear in the Preview of the SPEC File section.
- 4 Click **Save**. A pop-up box opens to confirm the successful creation of the spec file.
- 5 Close the Spec File Generator dialog box.



If you create a new DataStore and generate a spec file by using the PowerShell collection configuration utility, ensure that the spec file is made available at the instrumentation directory of the managed node. This can be done by saving the spec file in `Instrumentation Category` folder of the Microsoft Exchange SPI. Save the spec file in `%ovsharedir%\Instrumentation\Categories\Exchange2k7_Core` on the HPOM Server. Then deploy the `Exchange2k7_Core` category on the node. After this launch the Create Data Source tool on that node to add the datastore. Launch the Create Data Source tool on the nodes before you deploy the EXSPI-8X SPIMetaData Versioning policy.

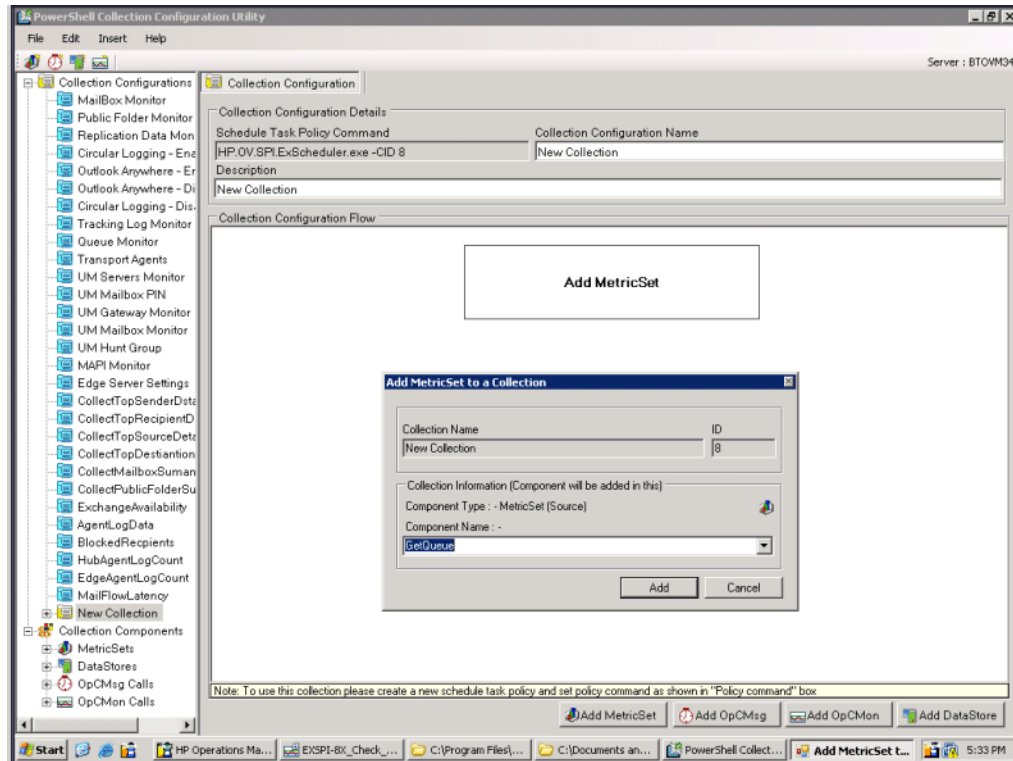
## Adding a Collection Configuration

A collection defines the complete mechanism of metric data collection. A collector can collect metric data, log it to a data store, or send a message to the HPOM message browser if a threshold is violated. A collection configuration consists of all the elements that collectively describe the complete lifecycle of the collection mechanism for a MetricSet.

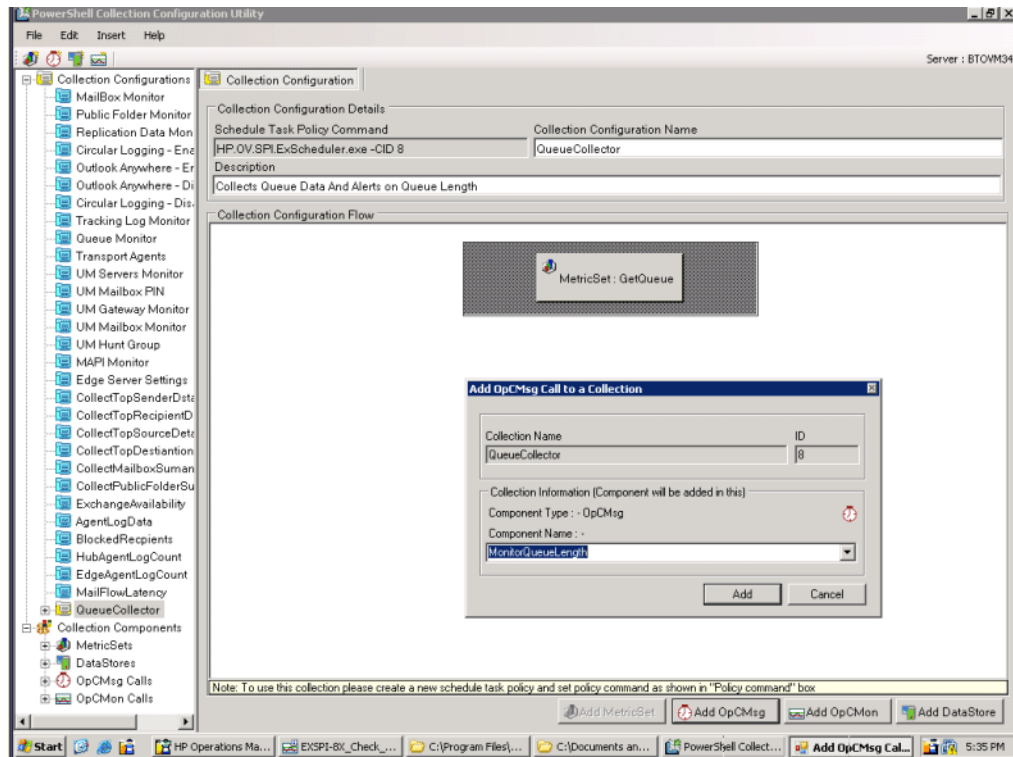
To add a new collection configuration:

- 1 In the left pane, right-click **Collection Configurations**, and then click **Add New Collection** or click **Insert** → **Add New Collection**. A window appears to add MetricSet to the new collection.
- 2 Select the MetricSet from the Component Name box from the drop-down menu list.

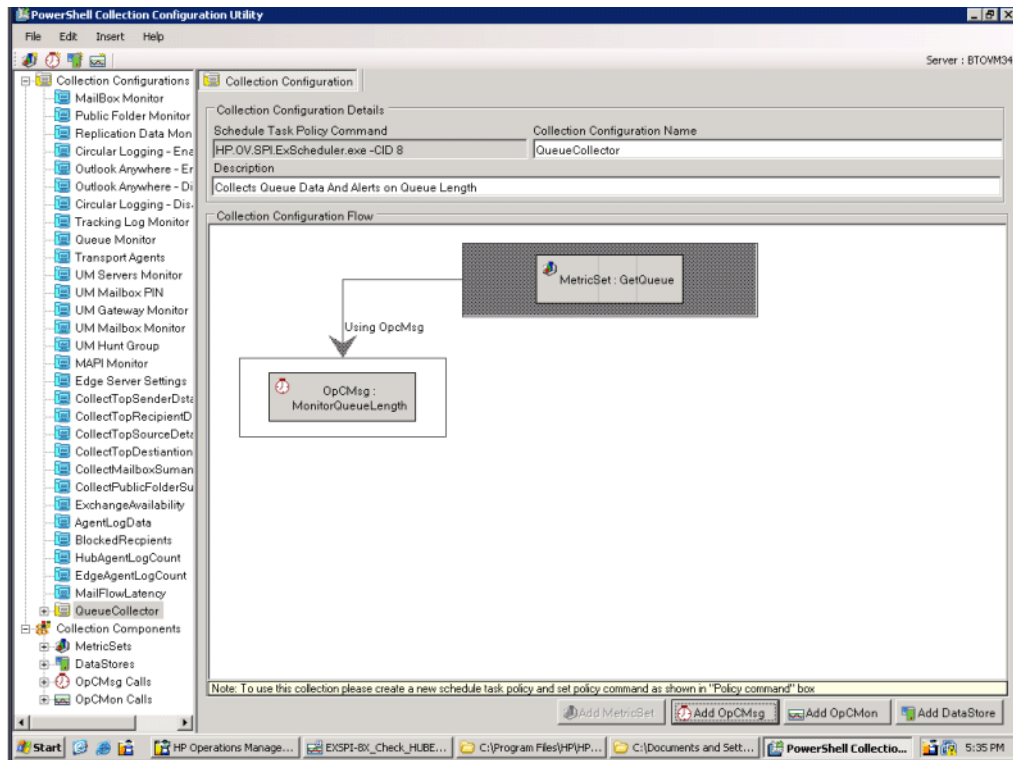
4. For example, The MetricSet is added to the collection.



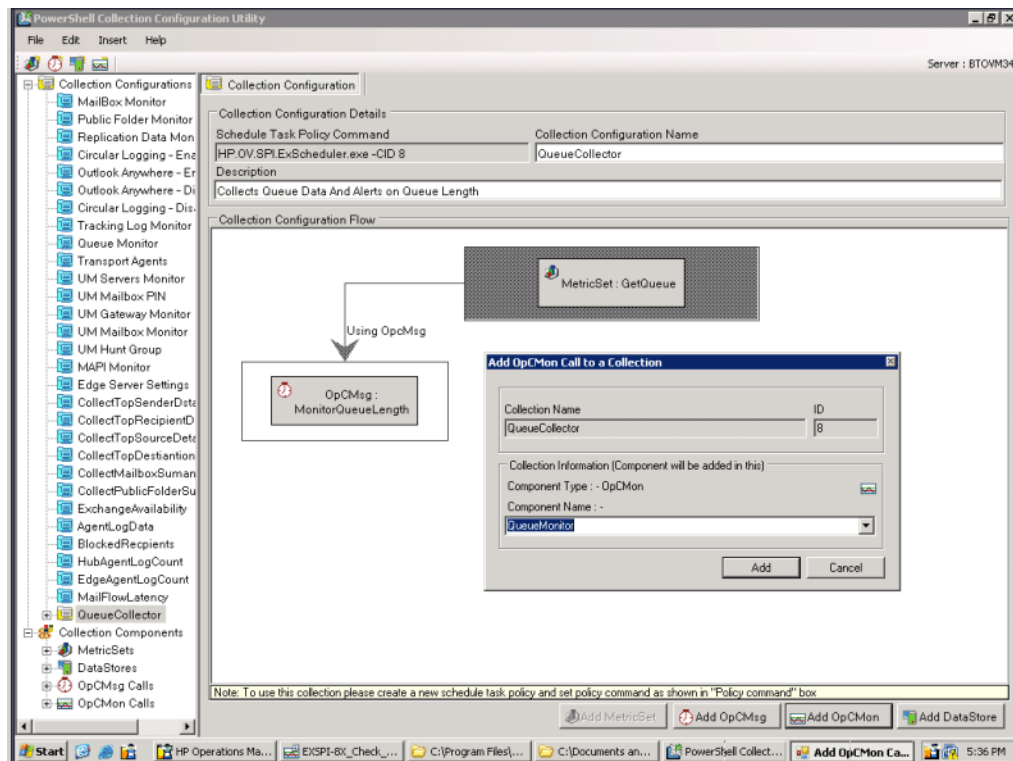
- 3 To add an OpCMsg Call to this collection, click **Add OpCMsg** in the right pane. A window appears to add the OpCMsg Call to the new collection.
- 4 Select an OpCMsg Call from the Component Name box from the drop-down list, and then click **Add**. The OpCMsg Call is added to the collection.



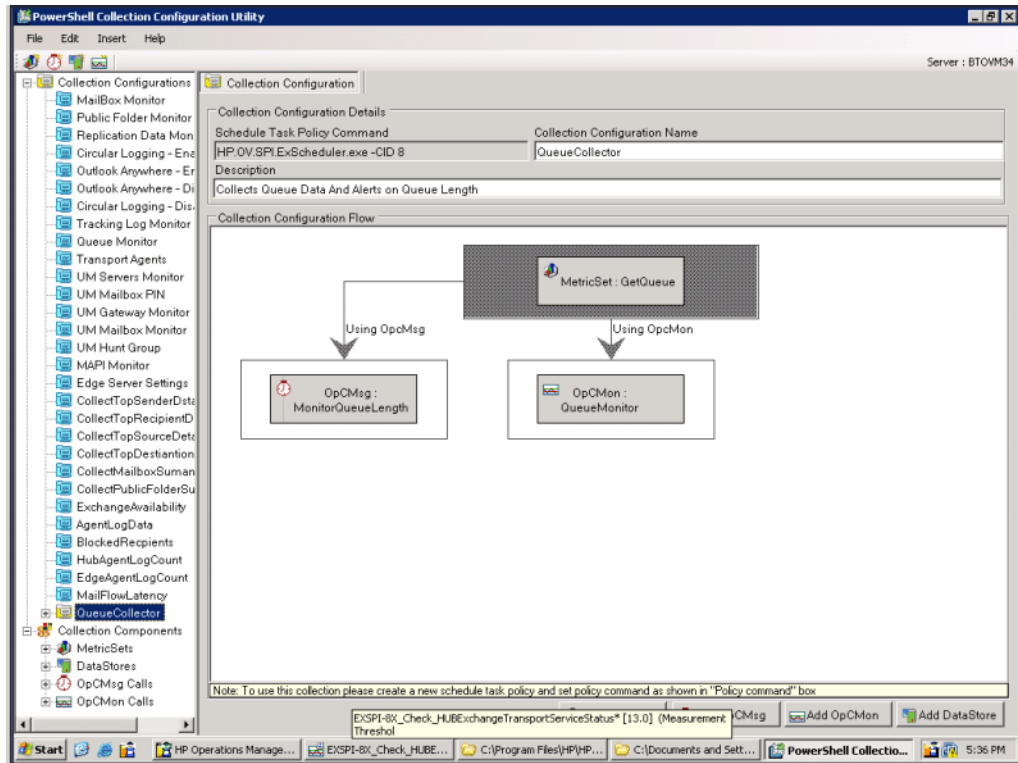




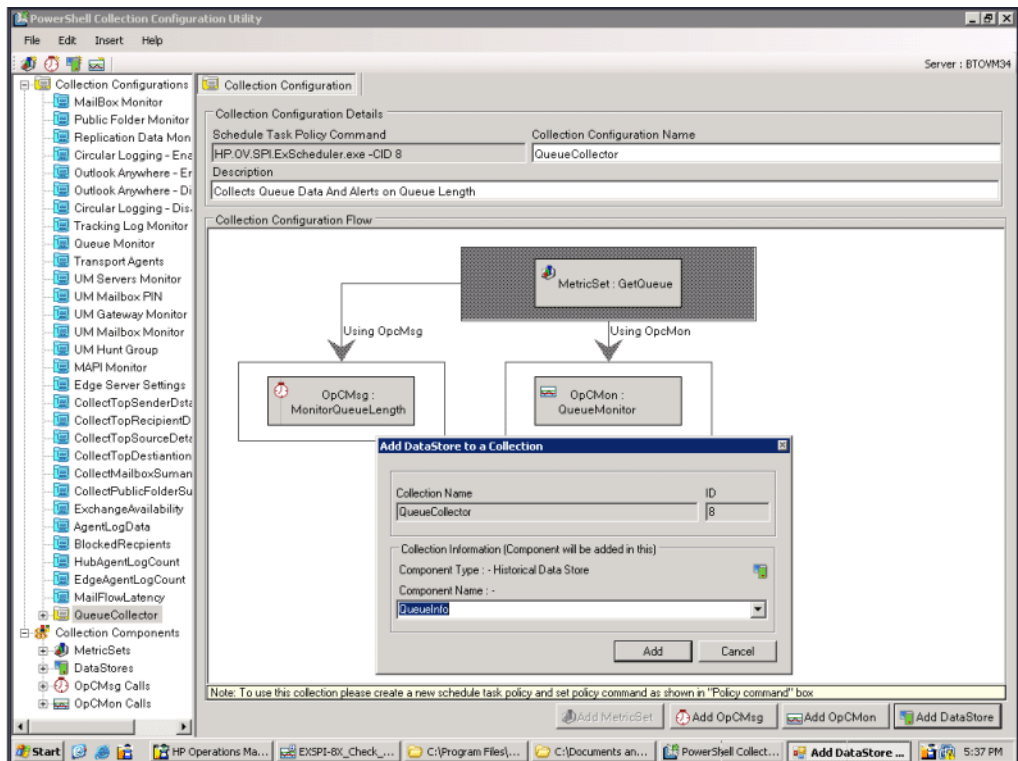
- 5 To add an OpCMon Call to this collection, click **Add OpCMon** in the right pane. A window appears to add the OpCMon Call to the new collection.
- 6 Select an OpCMon Call from the Component Name box from the drop-down list, and then click **Add**. The OpCMon Call is added to the collection.

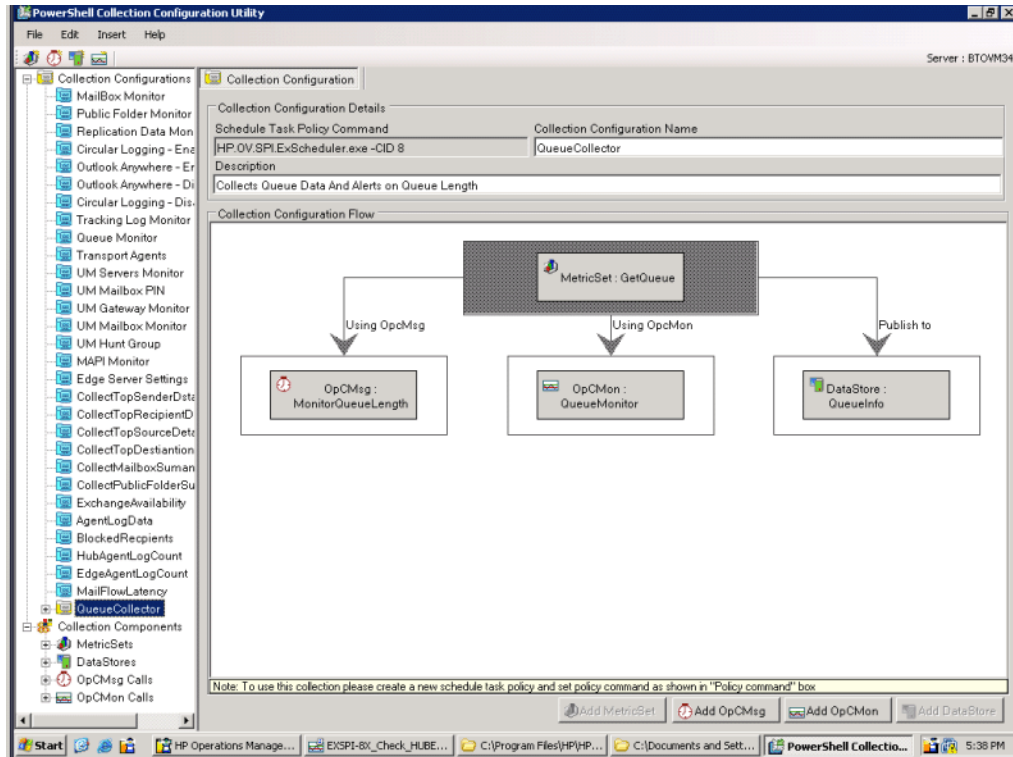








- 7 To add a DataStore, click **Add DataStore** in the right pane. A window appears to add the DataStore to the new collection.
- 8 Select the appropriate DataStore from the Component Name box from the drop-down list, and then click **Add**. The DataStore is added to the collection.





- 9 In the right pane, type an appropriate name in the Collection Configuration Name text box.
- 10 Click **File** → **Save**. The new collection configuration  is listed with the default configurations .
- 11 Note the command displayed in the Schedule Task Policy Command text box.
- 12 After you add a new collection configuration, you must perform the following tasks:
  - a Create a new scheduled task policy.
  - b In the newly created scheduled task policy, specify the command that you have noted down.



You must deploy the newly created scheduled task policy (along with the EXSPI-8X SPIMetaData Versioning policy) on the nodes where you want the changed data collection mechanism to take effect.

## Modifying a Collection

The EXSPI Configuration utility tool enables you to modify the newly added configuration collections:

- MetricSet
- OpCMsg Call
- OpCMon Call
- DataStore
- Collection configuration



Do not modify any default MetricSet or data store or both.

## Modifying a MetricSet

To modify the MetricSet, perform the following:

- 1 Click the MetricSet (for example, GetQueue) which requires changes. The MetricSet details are displayed in the right pane.
- 2 Change one or more of the following options (as shown in the table) appearing in the right pane.

Option	Description
MetricSet Name	Change to an appropriate name.
Powershell Command	Select a command from the list of available commands.

- 3 Click **Apply Changes** to save the change.



If you change the PowerShell command, all the previously added metrics will be removed.

*Do not delete any default MetricSet that is present in the EXSPI Configuration Utility. To delete a MetricSet that you have added to the EXSPI Configuration Utility, right-click the MetricSet in the left pane, and then click **Delete Selected MetricSet**.*

## Modifying a Metric

To modify an existing metric:



Do not modify the metric order in the existing default MetricSets. You can modify the order of metrics only in the MetricSets that you have added to the EXSPI Configuration Utility.

- 1 In the left pane, click the metric that you want to modify.

- Change one or more of the following options (as shown in the table) appearing in the right pane.

Option	Description
Metric Name	Select a metric name from the list of available metrics.
Metric Description	Type a description of the metric.
Metric Data Type	After you choose the metric, suitable data type appears by default. Do not change the default setting.
Category	Select this option to specify the unit of measure of the metric.
Scale	To convert the metric value to a unit of your choice, specify the multiplying factor. For example, if the metric value is in the form of KB and you want to collect the metric in the form of bytes, specify 1024 in this field.
Suffix	Specify the element of the metric value that you want to eliminate. For example, if the metric value is appended with the unit B (as in 1200B), you can eliminate B by typing B in the Suffix text box.

- Click **Apply Changes**.

*Do not delete any default metric that is present in the EXSPI Configuration Utility. To delete a metric that you have added to the EXSPI Configuration Utility, right-click the metric in the left pane, and then click **Remove this....***

- Click **Apply Changes**.
- Click **File** → **Save**.

## Modifying OpCMsg Call

To modify an existing OpCMsg Call:

- In the left pane, expand **Collection Components**, and then click the OpCMsg Call that you want to modify.
- Change one or more of the following options (shown in the table) appearing in the right pane.

Option	Description
OpCMsg Call Set Name	Type an appropriate name.

Option	Description
Application	If necessary, modify the name of the application that will be affected. You can view this text in the HPOM message browser when you open the Message Properties dialog box. You can leave this field blank.
Object	If necessary, modify the name of the object of the application that will be affected. You can view this text in the HPOM message browser when you open the Message Properties dialog box. You can leave this field blank.
Severity	Select the severity level of the event.
Message Text	Type the message that you want to generate.
MetricSet Ref	Select an available MetricSet from the list.
Metric Ref	Select an available metric from the list.
Select Arithmetic Operator	Select an available arithmetic operation from the list.
Select Logical Operator to combine with Previous Rule	This field is enabled only when you choose more than one limiting value or condition for the chosen metrics. Select AND or OR to combine the rules that you create based on the available arithmetic operators.
Value to compare	Select the limiting (threshold) value of the selected metric.

### 3 Click **Apply Changes**.

To delete an existing OpCMsg Call, right-click the OpCMsg Call in the left pane, and then click **Remove from Collection**.

### Editing Existing Rules

You can edit the existing rules of OpCMsgCall. To edit the rules, perform the following:

- 1 Click **Edit**.
- 2 In the section Update Rule, change one or more of the following options:
  - Metric Ref
  - Arithmetic Operator

To delete any existing rule, select the rule in the Available Rules box, and then click **Delete**.

## Modifying OpCMon Call

To modify an existing OpCMon Call:

- 1 In the left pane, click the OpCMon Call that you want to modify.
- 2 Change one or more of the following options (as shown in the table) appearing in the right pane.

Option	Description
Name	Type an appropriate name for the OpCMon Call.
Metric Ref	Select the metric name for which you want to set the OpCMon Call.

- 3 In the Measurement Threshold Policy name text box, type the name of a measurement threshold policy to which you want to associate this OpCMon Call.
- 4 Click **Apply Changes**.
- 5 To delete an existing OpCMon Call, right-click the **OpCMon Call** in the left pane, and then click **Remove from Collection**.

## Modifying a Data Store

To modify an existing DataStore:

- 1 In the left pane, click the DataStore that you want to modify.
- 2 Change one or more of the following options (as shown in the table) appearing in the right pane.

Option	Description
Name	Type an appropriate name for the DataStore.
Capacity	Type the number of rows for the DataStore.
Data Source	Type EX2007_DATA.
Data Table	Type EX2007_<table name>, where <table name> is an appropriate name for the table.
Index By	Type DAY.
Roll By	Type the interval at which the data should be flushed out of the data store. You can specify DAY, WEEK, or MONTH. You cannot store data for more than a month.

- 3 From the **Select MetricSet Reference** drop-down list, select a MetricSet.
- 4 From the **Select Metric Reference** drop-down list, select a metric.

- 5 In the **Select Data Column Reference** box, type a name for the data column in which the DataStore will store the metric selected.  
Do *not* leave this field blank if you want to add more than one metric.
- 6 Click **Add**. You cannot add more than one MetricSet. You can however add more metrics in that MetricSet.
- 7 To add a new MetricSet and a new metric to this DataStore, in the Add Reference section, select new MetricSet and metric, and then click **Add**.
- 8 To delete existing MetricSets and metrics from this DataStore, select an entry from the Available Metric References list, and then click **Delete**.
- 9 Click **Apply Changes**.

### Regenerating the Spec File

After you modify an existing DataStore, you must re-generate the spec file. To re-generate the spec file for the modified DataStore, perform the following steps:

- 1 Go to the modified DataStore.
- 2 In the right pane, click **Generate SPEC**. The Spec File Generator dialog box opens.
- 3 In the Spec File Generator dialog box, type an appropriate label name in the Table Label text box, and then click **Create**. The details of the SPEC file appear in the Preview of the SPEC File section.
- 4 Click **Save**. A pop-up box opens to confirm the successful creation of the spec file.
- 5 Close the Spec File Generator dialog box..



If you create a new DataStore and generate a spec file by using the PowerShell collection configuration utility, ensure that the spec file is made available at the instrumentation directory of the managed node. This can be done by saving the spec file in `Instrumentation Category` folder of the Microsoft Exchange SPI. Save the spec file in `%ovsharedir%\Instrumentation\Categories\Exchange2k7_Core` on the HPOM Server. Then deploy the `Exchange2k7_Core` category on the node. After this launch the Create Data Source tool on that node to add the datastore. Launch the Create Data Source tool on the nodes before you deploy the EXSPI-8X SPIMetaData Versioning policy.

Do *not* delete any default Data Store that is present in the EXSPI Configuration Utility. To delete a DataStore that you have added to the EXSPI Configuration Utility, right-click the DataStore in the left pane, and then click **Remove from Collection**. If the DataStore is associated with an existing collection configuration, the utility removes the DataStore from the collection.

### Modifying Collection Configuration

To modify an existing collection configuration:



Do *not* modify the existing default collection configurations. You can modify a collection configuration that you have added.

- 1 In the left pane, click the collection configuration that you want to modify.
- 2 In the right pane, right-click the collection configuration block or any other component block to edit.
- 3 After making changes, click **File** → **Save**.

Do not delete any default collection configuration that is present in the EXSPI Configuration Utility. To delete a collection configuration that you have added to the EXSPI Configuration Utility, right-click the collection in the left pane, and then click **Remove Collection**.

## Using Additional Cmdlets

You can create customized cmdlets and use those cmdlets to monitor metric data on a managed node. You can create customized cmdlets to return additional metrics, and configure the Microsoft Exchange SPI to monitor these additional metrics. Perform the following tasks to achieve this:

### Task 1: Identify the Microsoft Exchange Server 2007 Node

Identify the Microsoft Exchange Server 2007 node on which you want to add customized cmdlets to observe additional metric data.

### Task 2: Create Cmdlets

Create customized cmdlets on the identified nodes.

### Task 3: Install Snap-ins

Install customized snap-ins for the newly created cmdlets on the nodes on which you have created new cmdlets.

### Task 4: Update the Exspi-exshell.psc1 File

To update the `Exspi-exshell.psc1` file with the new snap-in information, perform these steps:

- 1 Open the `Exspi-exshell.psc1` file by using a text editor from the location `%OvAgentDir%/bin/instrumentation`.
- 2 Add the following within the `PSSnapin` tag:  

```
<PSSnapIn Name="new_snap-in_name" />
```

where `new_snap-in_name` is the name of newly added snap-in.



Perform this change on the managed node where the snapin is installed. If the snapin is installed on all managed nodes then the `Exspi-exshell.psc1` can be updated at the management server itself.

- 3 Save the file.

### Task 5: Create New Collection Definitions for New Cmdlets

Use the EXSPI Collection Configuration utility and create new collections with the newly added cmdlets. While creating the new collection configuration, note the command displayed in the Schedule Task Policy Command text box.

### Task 6: Create a New Scheduled Task Policy

After creating a new collection configuration, perform these steps:

- 1 Create a new scheduled task policy.
- 2 In the newly created scheduled task policy, specify the command as mentioned in [Task 5](#).



#### Task 7: [Deploy the EXSPI-8X SPIMetaData Versioning Policy on Nodes](#)

Deploy the EXSPI-8X SPIMetaData Versioning policy on the nodes where you have created the new cmdlets.

#### Task 8: [Deploy the Scheduled Task Policy](#)

Deploy the created scheduled task policy on the nodes where you have created the new cmdlets.

## Configuring Microsoft Exchange SPI for Exchange Server Cluster Environment

You can use Microsoft Exchange Server 2007 in a cluster environment where the fail-over capability of Exchange Servers ensures uninterrupted Exchange availability. In the event of a cluster node failure, the Microsoft Exchange SPI automatically switches monitoring activity from the failed node to the active node.

The Microsoft Exchange SPI recognizes Exchange instances in an Exchange cluster by using XML configuration files (`apminfo.xml` and `msexchange.apm.xml`). In the event of failure, these XML files enable the HP Operations agent to automatically perform the following functions:

- Disable instance monitoring on the inactive node
- Enable instance monitoring on the currently active node

To configure the Microsoft Exchange SPI for a cluster environment, perform the following tasks in the order given.

#### Task 1: [Add the Exchange Cluster Nodes to HPOM Console](#)

Identify the cluster nodes of your Exchange environment, and then add those nodes to HPOM console.

If policy autodeployment is disabled, you must launch the necessary policies on newly added cluster nodes.

Edit the Discovery policy to run it with the special user privileges. See [Edit Discovery Policy](#). Deploy the policy groups depending on the Server role hosted by the managed node. See [Table 3](#) on page 38 for the specific policy group.

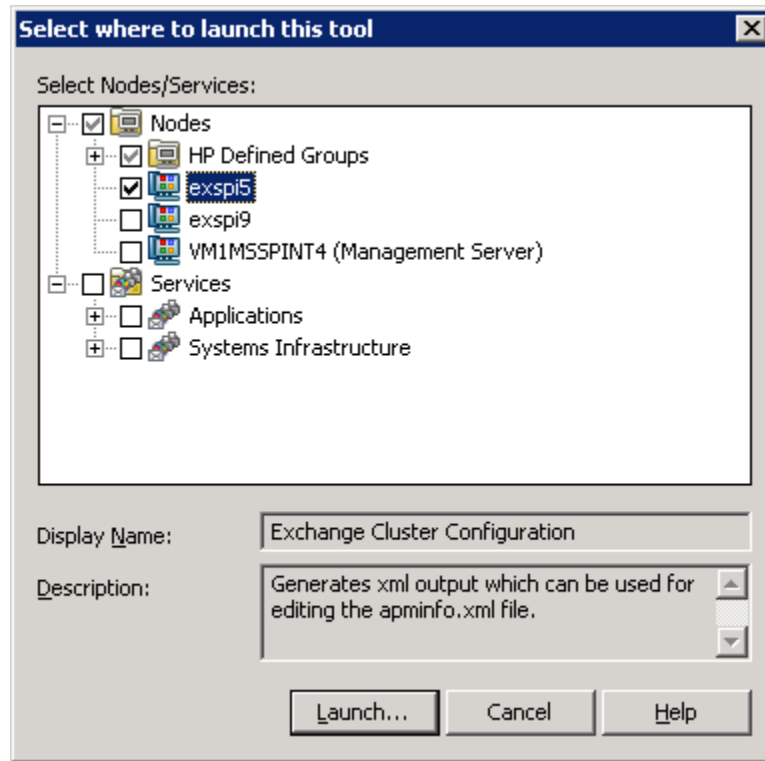
The discovery policy discovers the Exchange cluster and updates the map with cluster topology.

#### Task 2: [Generate Cluster Application Configuration File](#)

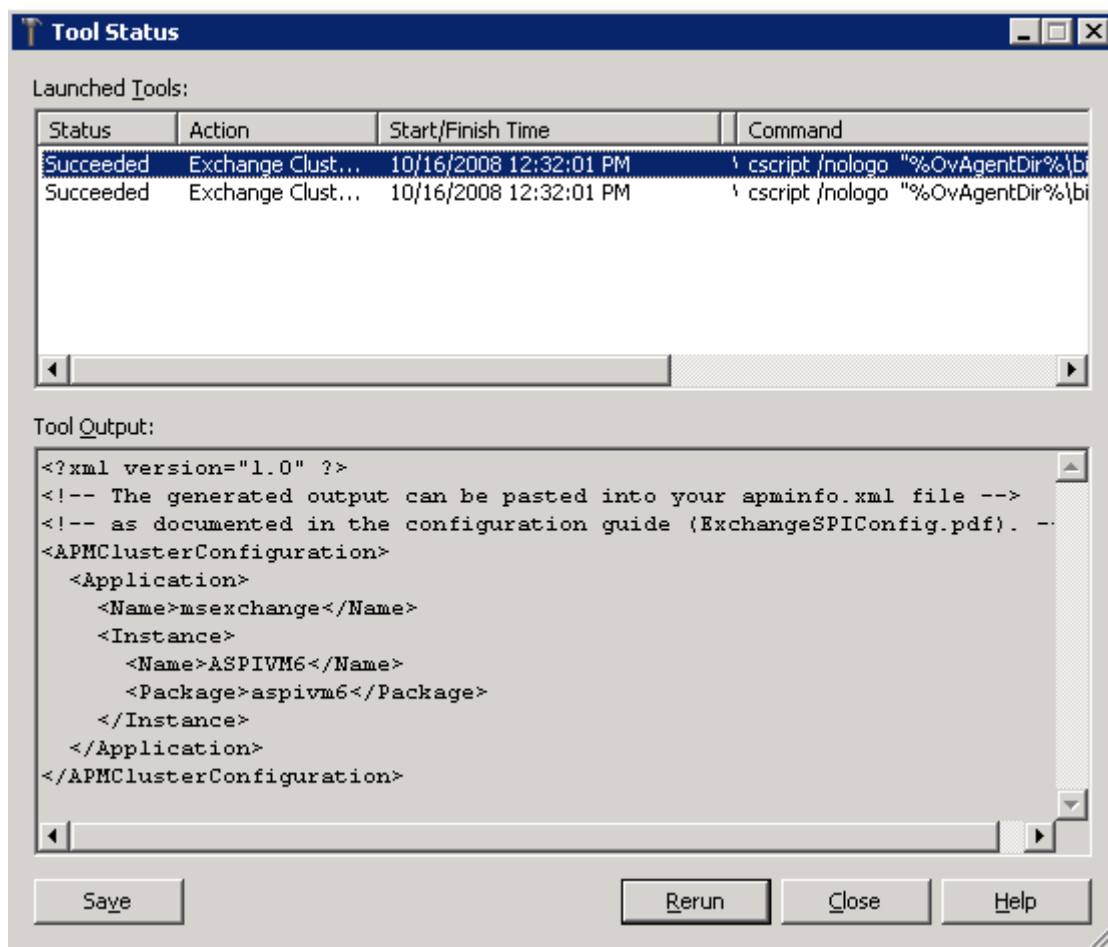
You must generate the `apminfo.xml` file to describe the cluster instances (Exchange virtual servers). For this, start the Cluster Configuration tool:

- 1 Expand **Tools** → **SPI for Exchange** → **Exchange 2007**.

- 2 In the details pane, double-click **Exchange Cluster Configuration**. The Select where to launch this tool dialog box opens.



- 3 Click **Launch....** The tool Status window appears and displays the output under the Tool Output section.



- 4 Remove any content above `<?xml version="1.0"?>`.
- 5 Select the text content under the Tool Output section, and then copy it to a text editor.
- 6 Save the text as `apminfo.xml` in the `%OvAgentDir%\conf\conf\` location on cluster nodes.



Before copying the `apminfo.xml` file, you must manually create the `%OvAgentDir%\conf\conf\` folder if it does not exist.

- 7 Stop and start the agents on the nodes by using the following commands:

```

opcagt -kill
opcagt -start

```

#### Example `apminfo.xml` File

In the following example, `aspivm6` is the names of the Exchange resource groups corresponding to the `aspivm6` instance (virtual server):

```

<?xml version="1.0" ?>
<APMClusterConfiguration>
  <Application>
    <Name>msexchange</Name>

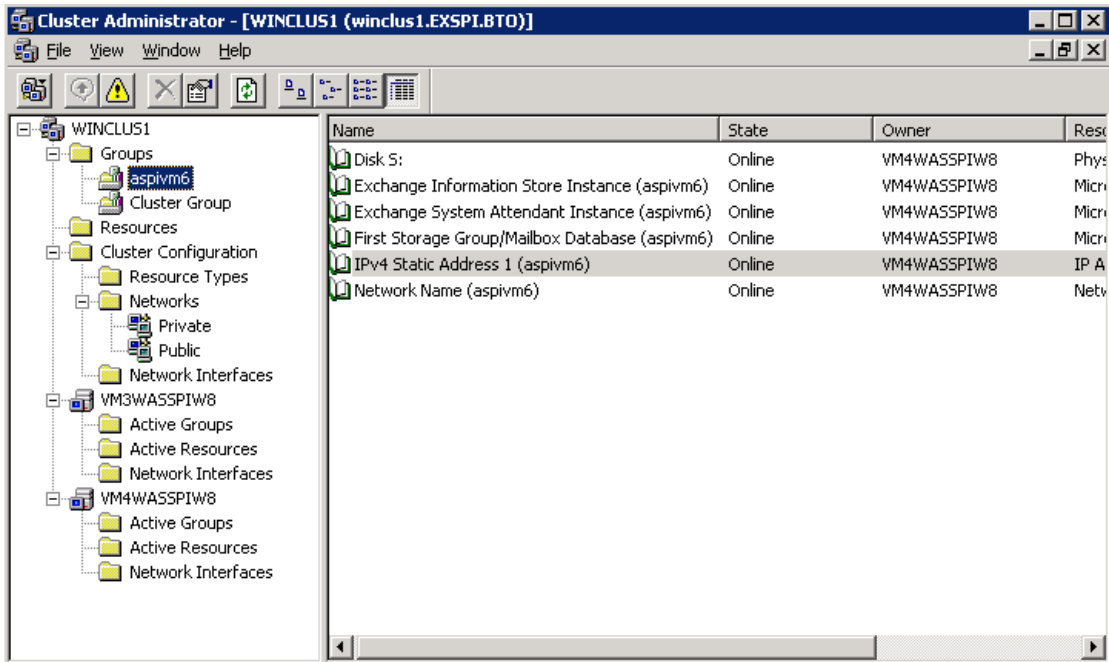
```

```

<Instance>
  <Name>ASPIVM6</Name>
  <Package>aspivm6</Package>
</Instance>
</Application>
</APMClusterConfiguration>

```

**Figure 4 Example of Exchange Resource Group**



### Task 3: Copy the Cluster-Aware Policy XML File

Perform the following steps:

- 1 Deploy the SPI for Exchange instrumentation on the node.
- 2 Create the `\conf\` folder under `%OvAgentDir%\bin\instrumentation\`.
- 3 Copy the `msexchange.apm.xml` file from the `%OvAgentDir%\bin\instrumentation\` folder to `%OvAgentDir%\bin\instrumentation\conf\`.
- 4 Restart the agent.
- 5 Repeat [step 1](#) through [step 4](#) for all the Exchange nodes.



Make sure to deploy the policy EXSPI-8X Exchange Cluster Discovery SysLog on Windows Server 2003 cluster nodes and the policy EXSPI-8X Exchange Cluster Discovery AppLog 2K8 on Windows Server 2008 cluster nodes, to handle failovers.

## Additional Configuration for Policy Name Change

The Microsoft Exchange SPI disables all policies from a cluster node if the node fails, and then enables all policies on the active cluster node. While switching its operation from disabled node to active node, the Microsoft Exchange SPI retrieves policy information from the `msexchange.apm.xml` file. If you change any policy name (or add a new policy) and deploy the changed policy on a managed cluster node, you must reflect the change in the `msexchange.apm.xml` file as well. To update the `msexchange.apm.xml` file with changed policy information, follow these steps:

- 1 On the management server, open the `msexchange.apm.xml` file from the `%OvShareDir%\Instrumentation\Categories\SPI for Exchange\Windows\6.0\X64` location by using a text editor.
- 2 Edit the changed policy names in this file. Add new policy names (within the `Template` markup), if required.
- 3 For the managed nodes, follow these steps:
  - a Redeploy the SPI for Exchange instrumentation on the node.
  - b Create the `\conf\` folder under `%OvAgentDir%\bin\instrumentation\`.
  - c Copy the `msexchange.apm.xml` file from the `%OvAgentDir%\bin\instrumentation\` folder to `%OvAgentDir%\bin\instrumentation\conf\`.
  - d Restart the agent.
  - e Repeat [step a](#) through [step d](#) for all nodes.

While redeploying the instrumentation on Microsoft Exchange Server 2007 nodes, see [Deploy the Instrumentation Categories on the Managed Nodes](#).

## Map View for Exchange Cluster Services

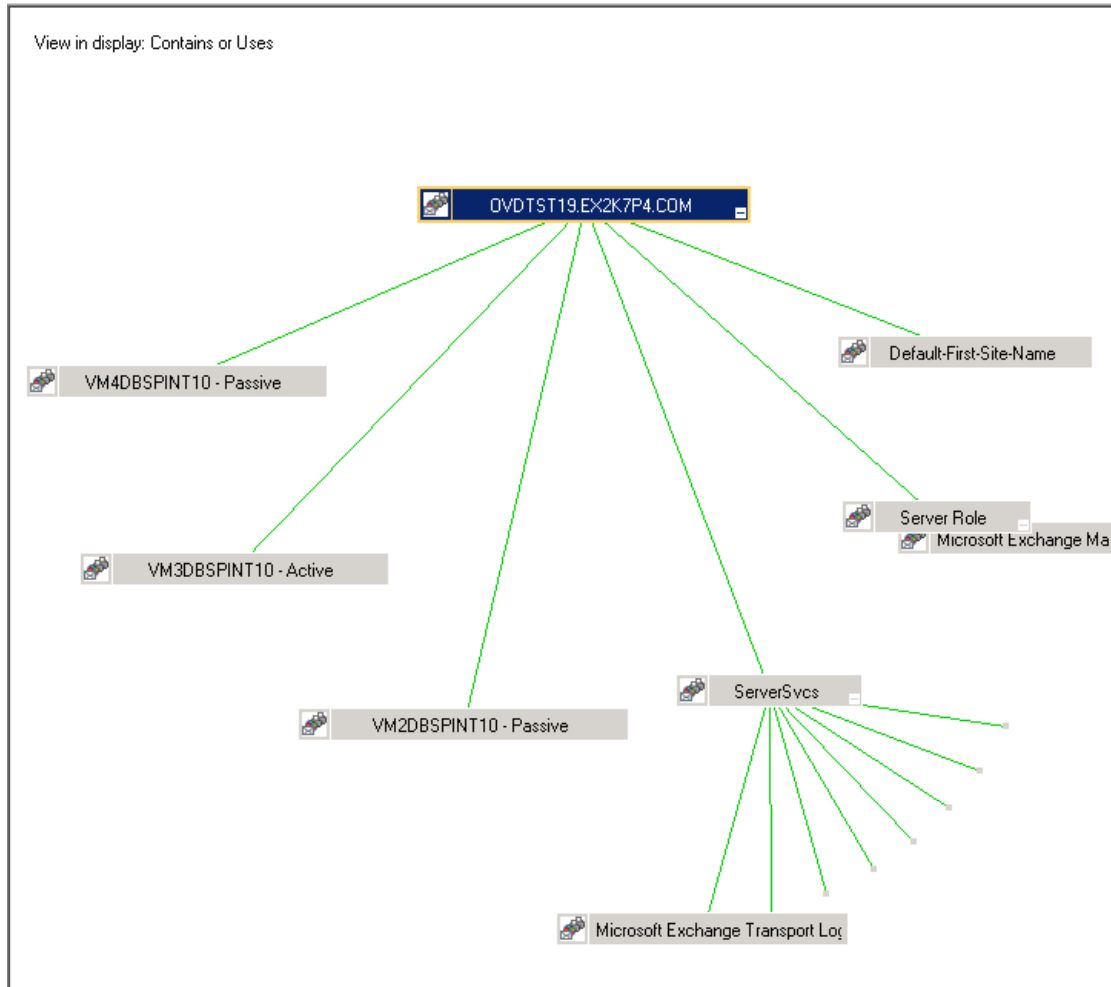
The Microsoft Exchange SPI represents Exchange clusters in the map view. Map view creates one node for each virtual server in the cluster. Because the cluster is properly modeled in the service map, Microsoft Exchange SPI instrumentation and Quick Start policies are auto-deployed to all managed Exchange cluster nodes.

Messages for the Exchange virtual server show up under the Exchange virtual server name in the maps.

For the Exchange Virtual server an EXSPI service discovery hosted-on hierarchy is created within a Clusters container. This allows messages to be sent to the hosted-on hierarchy.

This same hierarchy is also created as virtual nodes under the Exchange Virtual Server. A dependency is created from each Virtual Exchange Server virtual node to its corresponding Cluster hosted-on node. Messages and status will then propagate to the correct Virtual Exchange Server virtual node.

**Figure 5 Service Map in Clustered Environment**



When a fail-over happens, dependencies to the failed node will be removed and replaced with new dependencies to the newly active node.



When a failover happens, messages that occurred before the failover will not be propagated to the virtual node.

---

## 4 Using Policies

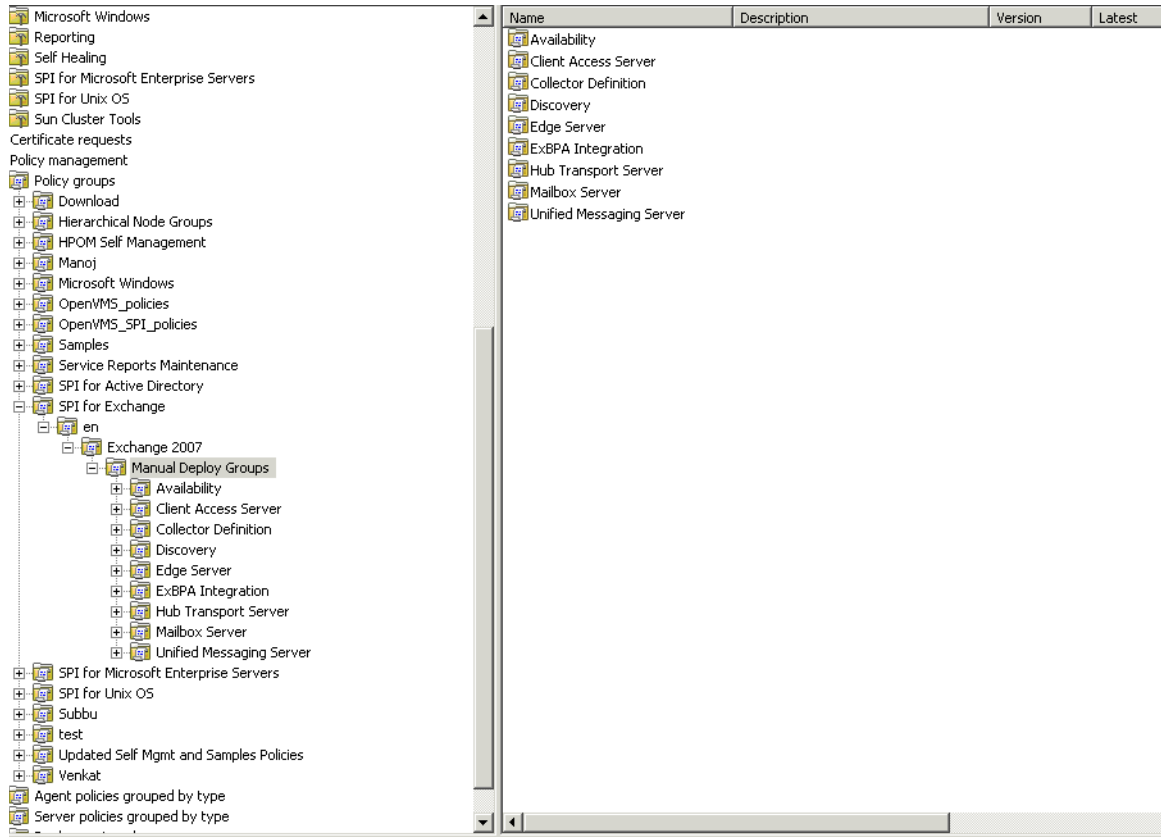
Policies monitor the Microsoft Exchange 2007 Server environment and run according to rules and schedule specifications. Scheduled Tasks policies contain the rules for interpreting Microsoft Exchange Server 2007 states or conditions. See *HP Operations Smart Plug-in for Microsoft Exchange Online Help* or *HP Operations Smart Plug-in for Microsoft Exchange Online Help PDF* for detailed description of all policies.

### Policy Group and Policy Type

The policies of the Microsoft Exchange SPI in the HPOM console are available in two ways—policy group and policy type.

#### Policy Group

A policy group organizes policies according to the deployment method and area to be targeted for discovery or monitoring. Deployment in Microsoft Exchange SPI is manual. To view the manually deployed policies in the Microsoft Exchange SPI, in the console tree of the HPOM console, expand **Policy Management** → **Policy Groups** → **SPI for Exchange** → **en (ja)** → **Exchange 2007** → **Manual Deploy Groups**. The policies are displayed in each sub-groups of the Microsoft Exchange SPI.



You can customize the threshold of Microsoft Exchange SPI policy. See [Customize policies](#) for more details.

To customize policies, see [Customize policies](#) on page 35.

The Microsoft Exchange SPI has the following policy groups depending on the Exchange server roles:

- Availability
- Client Access Server
- Collector Definition
- Discovery
- Edge Server
- ExBPA Integration
- Hub Transport Server
- Mailbox Server
- Unified Messaging Server

## Policy Type

Agent policies grouped by type organize policies according to type. The Microsoft Exchange SPI has the following policy types:



- Service Auto-Discovery
- Scheduled Task
- Measurement Threshold
- Windows Event Log
- Windows Management Interface
- ConfigFile
- Open Message Interface
- LogFile Entry



To know the policies in each policy group and their policy type in detail, see *HP Operations Smart Plug-in for Microsoft Exchange Online Help* or *HP Operations Smart Plug-in for Microsoft Exchange Online Help PDF*.



# 5 Using Tools

The Microsoft Exchange SPI uses different tools to monitor the Microsoft Exchange Server 2007 environment. For more information on the functioning of each tool, see the *Microsoft Exchange SPI Online Help*.

## Launching Microsoft Exchange Tools

To launch a tool of Microsoft Exchange SPI:

- 1 Expand **Tools** → **SPI for Exchange** → **Exchange 2007**. The tools of the Microsoft Exchange SPI are displayed.
- 2 Double-click the tool to be launched. A window displays all the managed nodes.
- 3 Select the Exchange managed nodes, and then click **Launch....** The tool starts on the selected nodes.

## HP Operations Topology Viewer

The HP Operations Topology Viewer provides a quick means to seeing an Exchange environment, providing a hierarchical view in a tree (left pane), and a topological view in a map (right pane). The left pane shows the organization/admin groups/Microsoft Exchange servers/connectors/routing groups components, while the map in the right pane graphically represents servers/routing groups/connectors links and connections.

After you launch the HP Operations Topology Viewer and enter domain controller access information, the tool gathers data from the domain controller and Microsoft Exchange servers. From this information a map is created, displaying servers, connectors, and routing groups.



The Topology Viewer provides a view that reflects the Active Directory site/server replication information/Exchange organization information at the time you connect to a server. The view remains static until you refresh it. To update the view, select from the menu **File** → **Refresh Data**. The map is then updated.

In the Topology Viewer window right pane, the map initially shows Routing group connectors, external mail connectors. You can display the server labels and modify the display by selecting **View** → **Properties**. The Properties page allows you many options for how to display the map: you can show or hide connectors between routing groups, server labels and roles, DC Roles.

## Using the HP Operations Topology Viewer

After you complete steps mentioned to connect to a Microsoft Active Directory domain controller, the Topology Viewer tool can gather information. This information is organized into a tree, showing Microsoft Exchange Server components on the left and a map graphically representing the Microsoft Exchange Server organization on the right.










You can modify the default display by using the **View** menu and selecting **Properties...** The Properties page has three tabbed pages that show additional information and allow you to change the display (**Visibility** and **Colors and Lines**).






- ▶ If the logged-in user account has proper access to the DC to which you are attempting to connect, no alternate credentials are necessary.

## HP Operations Topology Viewer Toolbar

The following table lists the HP Operations Topology Viewer toolbar functions and the icons.

**Table 6 HP Operations Topology Viewer Toolbar**

Icon	Function
	Starts a new file, which appears as an empty grid; you can then click the Add Forest button to populate the empty view. The "New" button allows you to transition to a new view (for example, an Add a Forest), without adding to or changing the current view if the current view has been saved.
	Allows you to open a file of a previously saved view.
	Saves the current view to a file.
	Exports the current view and saves it to a graphic format of your choice, such as .png or .bmp. (The default format is .png.
	Allows you to add a forest by opening the Add Forest dialog, where you enter server connection information.
	Refreshes the data by checking information on the current connection.
	Zooms out the map view to the maximum degree.
	Zooms out the map view incrementally.
	Resets the map view to the default.

<b>Icon</b>	<b>Function</b>
	Zooms in the map view incrementally.
	Zooms in the map view to the maximum degree.
	Shows the next available top-level view in the forest.
	Displays the navigator, which shows a thumbnail of the entire map, surrounding the area of focus with a blue square. You can change the map focus by repositioning the blue square in the Navigator.
	Displays the Topology Viewer online Help.

## HP Operations Topology Viewer Menus

The following table lists the HP Operations Topology Viewer menu commands.

**Table 7 HP Operations Topology Viewer Menus**

<b>Menu</b>	<b>Command</b>	<b>Function</b>
File	New...	Opens a new file (empty grid); allows you to transition from the current view to a new view.
	Open...	Opens a selected, saved file that shows the layout as it was saved.
	Save	Saves the layout as the default layout.
	Save as...	Saves the layout to a file so that you can load it when desired.
	Export View...	Saves the currently displayed map in a graphical format of your choice.
	Add Forest...	Opens the Add Forest dialog, where successful connection to a server generates the replicated information within that forest and displays the information in the HP Operations Topology Viewer tree and map.
	Refresh Data	Reconnects to the server and updates the view with changes, if any, since the last connection.

<b>Menu</b>	<b>Command</b>	<b>Function</b>
View	Zoom	Allows you to zoom-in closer for greatest magnification or zoom-out farther for overall view. Minimum is at greatest degree zoomed out. Maximum is at greatest degree zoomed in.
	Next View	Shows the next view available in the right pane.
	Navigator	Shows a thumbnail of the entire map (including any area outside the current display) with a blue box indicating the current visible display.
	Legend	Displays the legend, which explains the meaning of the symbols used in the map located next to each server.
	Clear Find	When enabled, means that a server or site in the tree or the map has been right-clicked and Find in View or Find in Tree selected, resulting in selecting the corresponding item; clicking Clear Find returns the display to its default status with no elements selected.

<b>Menu</b>	<b>Command</b>	<b>Function</b>
View	Toolbar	Toggles on/off the display of the Topology Viewer toolbar buttons.
	Status Bar	Toggles on/off the display of the Topology Viewer status bar (located at the bottom of the Topology Viewer window).
	Properties...	Opens the Site Topology Properties dialog, which allows you to hide/show elements in the map and to modify the map appearance.
Window	Title Page	Displays the HP Operations Topology Viewer title page.
	Site Topology	Displays the Active Directory topology of the current forest.
	Exchange Topology	Displays the Exchange messaging view (with routing groups) of the current forest.
Help	HP Operations Topology Viewer Help	Displays online Help for HP Operations Topology Viewer.
	About HP Operations Topology Viewer...	Displays the HP Operations Topology Viewer version number.



## HP Operations Topology Viewer Map

Map connection lines labels: You can choose which connection lines to display and whether to display server, routing group, and external mail connector labels by right-clicking the map, selecting **View** → **Properties...** In the Exchange Topology View Properties page, select the Colors and Lines tabbed page. The connections are represented in default colors as follows:

- Routing Group (Represented in green): This acts as a connector that connects one routing group to the other logically. The Routing Group shows a logical routing of mail within the organization
- External Mail Connectors (Represented in blue): This represents the different send connectors which are configured in an organization having a Microsoft Exchange setup. An external connector shows the logical connection between a source server and a destination server. These connectors describe the way the nodes are running in a Microsoft Exchange 2007 environment and how the nodes which have the Edge Transport server or the Hub Transport server installed communicate:
  - With each other
  - With the Internet
  - With servers that are running Exchange 2000 or Exchange 2003
  - With other messaging systems

The Send connectors send outbound messages. To enable communication, set one or more source servers on a Send connector. The source servers act as transport servers which are responsible to handle message delivery along with that connector. When a Microsoft Exchange Server 2007 receives messages for a remote destination, they are sent to the source server of a Send connector. This Send connector is configured to send the e-mail to the destination domain. Send connectors are not applied to a single source.

- Routing Groups (Represented in green): This represents the logical grouping of different components which play a role a routing a message to the recipients. These components control the flow of the messages between various servers like Hub Transport servers, Edge Transport servers, servers which are running on Microsoft Exchange 2000 or 2003, and other SMTP servers. You can control the flow of the messages between these servers by configuring the settings of these components.



The Topology Viewer provides a view that reflects the Active Directory site/server replication information/Exchange organization information at the time you connect to a server. The view remains static until you refresh it. To update the view, select from the menu **File** → **Refresh Data**. The map is then updated.



---

## 6 Integrating Microsoft Exchange SPI with Reporting and Graphing Solutions

Reports and graphs provide you with a complete view of the performance of the components of the Microsoft Exchange Server 2007.

### Using Reports and Graphs

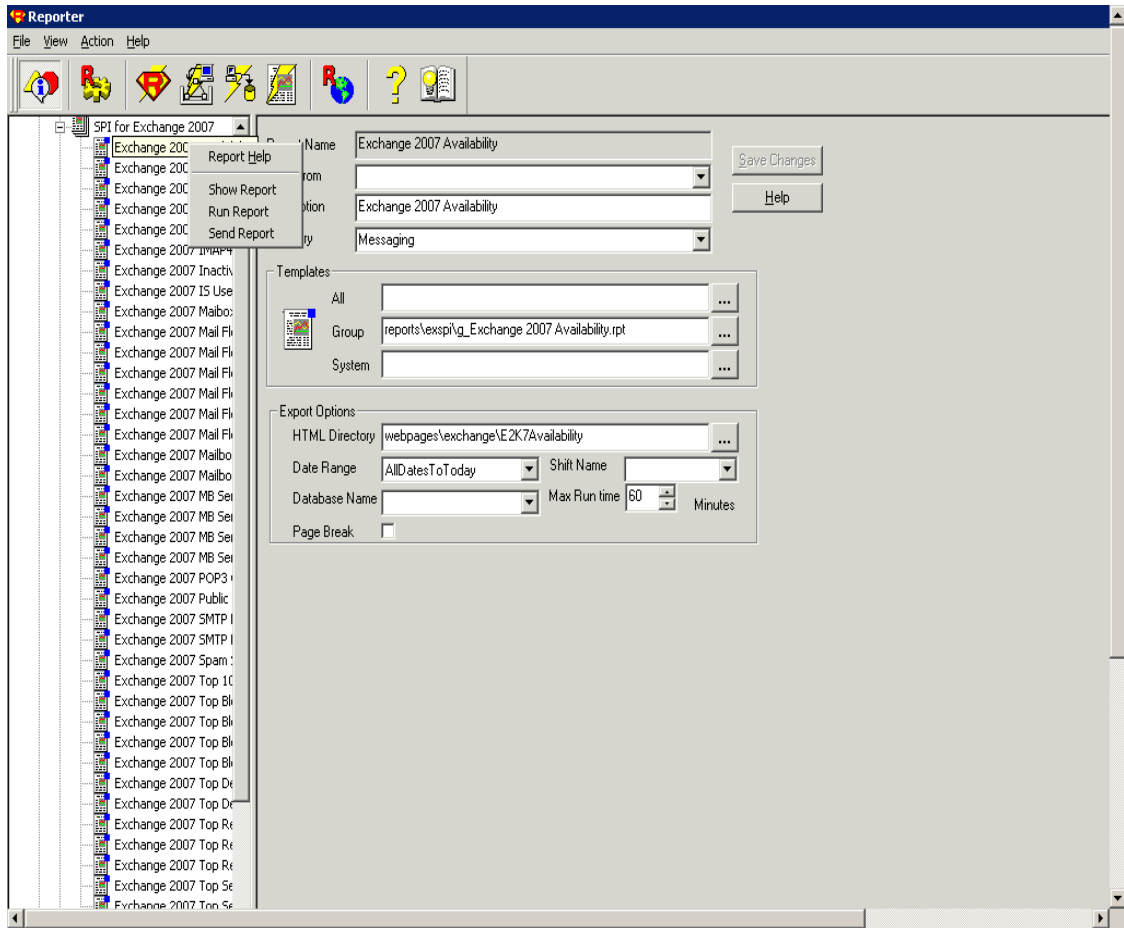
Report- and graph-generating templates are installed after you install the Microsoft Exchange SPI. They cover updates on the availability or the activity or both in Microsoft Exchange Server 2007 such as SMTP, MTA, processes for activity and status, and IS Public or Private Mailbox.

 **Time Interval for Exchange SPI Reports or Graphs**

The Microsoft Exchange SPI reports and graphs are not available until data has been gathered to the management server from the managed nodes. This occurs each night, so at least one day of activity is needed for the reports to populate. Where a report or graph type requires data from a Sat/Sun collection, those reports or graphs or both require a weekend to pass.

### Integrating Microsoft Exchange SPI with HP Reporter

You must install EXSPI Reporter package on HP Reporter Server to use the Microsoft Exchange SPI reports. For this, run `Setup.exe`. This setup installs the Microsoft Exchange SPI Report Package within the Reporter server. After you complete the installation, configure the Reporter to generate reports.



## Installing and/or Upgrading Report Package

- ▶ Complete the steps mentioned in [step 6](#) on page 23 in [Upgrading Microsoft Exchange SPI on a Standalone Management Server](#) on page 23 before installing the Report package.

To install and/or upgrade the Microsoft Exchange SPI Report Package on a stand-alone Reporter server:

- 1 Insert the HP Operations Smart Plug-ins DVD.
- 2 Double-click the file `Setup.exe`. (See and follow the steps of installation on Management Server for Windows.) A dialog box opens.
- 3 Click **Finish** to complete the installation.

## Configuring Report Package

To configure the Microsoft Exchange SPI Report Package:

- 1 Open the Reporter main window and check the status pane to note the changes to the Reporter configuration, which include uploading the Microsoft Exchange SPI reports.  
The Microsoft Exchange SPI Reports are automatically assigned to the **ALL** group in the Reporter main window. (See for HPOM Report list.)

2 Add group and single system reports by assigning reports as desired.

Reports are available for viewing the following day.

- ▶ Identify the Microsoft Exchange SPI reports of group and single systems by their full name; for example, **abc.xyz.com** is acceptable while **abc** is not.

Instructions are available in the HP Reporter Help for assigning Microsoft Exchange SPI reports to the targeted nodes. To access Help, select **Reports** or **Discovered Systems** in the left panel of the HP Reporter main window and right-click it. Select **Report Help** or **Discovered Systems Help** from the sub-menu that appears. See the topic “To assign a report definition to a Discovered Systems Group.” Reporter also includes two online documents: the *Concepts Guide* and the *Installation / Special Configurations Guide* for further information.

## Generating Reports

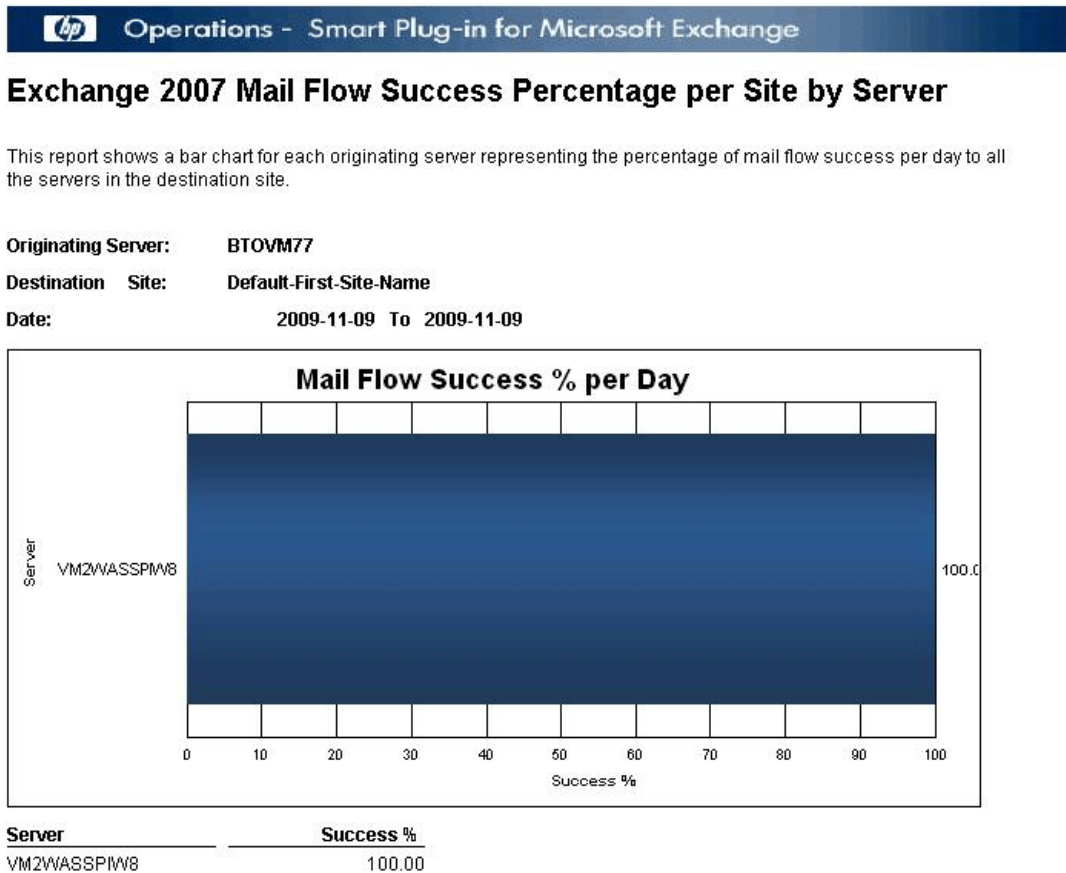
After you install the Microsoft Exchange SPI, the HPOM generates reports using the SPI-collected data for Microsoft Exchange Server 2007. HPOM runs the reports regularly on a nightly schedule. You can see the updated reports every day because the HPOM, by default, re-generates reports every night with the day’s data.

- ▶ If you want to customize your reports you must install HP Reporter. The documentation on HP Reporter on modifying the reports is available in *Concepts Guide*, *Installation Guide* and *Special Configuration Guide*, Online Help, and Release Notes.

The report data of Microsoft Exchange SPI is collected based on metrics used for each report. The HP Reporter identifies the data through metric variables. This data is stored in the MS SQL Reporter database.

You can access the reports of Microsoft Exchange SPI from the **Reports** area of the HPOM console. You can find complete description of all the reports in *Microsoft Exchange SPI Online Help*.

**Figure 6 Generating Reports**



## Integrating Microsoft Exchange SPI with HP Performance Manager

The Microsoft Exchange SPI comes with a set of preconfigured graph templates. Ensure that these graph templates are installed on an HP Performance Manager system, and that the data store (CODA or HP Performance Agent) runs on the managed node.

To integrate the Microsoft Exchange SPI with HP Performance Manager, follow these steps:

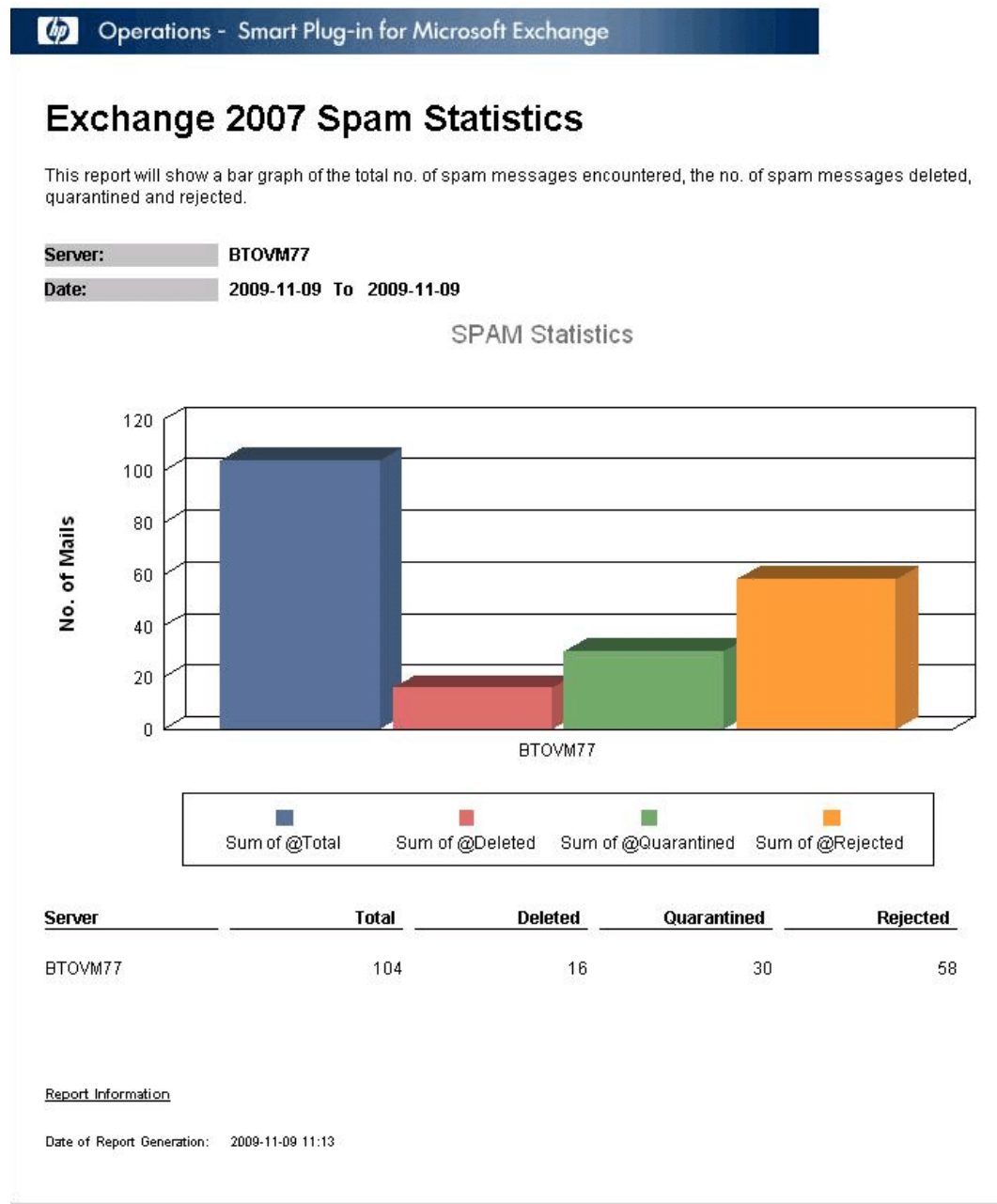
- 1 Install and configure the Microsoft Exchange SPI.
- 2 Install the graph package. To install the graph package:
  - a Insert the HP Operations Smart Plug-ins DVD.
  - b Double-click the `Setup.exe` file and follow the steps of [Installing SPI on a Standalone Management Server](#) on page 20.
  - c Select **Finish** to complete the installation.

For information see the HP Performance Manager documentation.

## Generating Graphs

You can generate the Microsoft Exchange SPI graphs on OVPM on a stand-alone Windows Server.

**Figure 7 Generating Graphs**







# 7 Troubleshooting

This chapter includes troubleshooting some areas of the Microsoft Exchange SPI and provides solutions thereof. The methods described may or may not require support assistance.

## Troubleshooting Discovery

The following sections describe the possible cause and suggested action for the failed discovery of the Microsoft Exchange Server services.

### Insufficient Privilege

In some cases the Microsoft Exchange SPI fails to discover the Microsoft Exchange Server services. The possible cause and suggested action is as follows:

- *Possible cause:* The account with which the Discovery policy (**Policy Management** → **Policy Groups** → **SPI for Exchange** → **en (ja)** → **Exchange 2007** → **Manual Deploy Groups** → **Discovery**) is run by the HP Operations agent does not have the privileges to connect to the Microsoft Exchange Server and retrieve data.
- *Suggested action:* Ensure that an administrator credentials are provided in the Discovery policy and then redeploy the policy.

### Failed Binary on the Managed Node

In some cases the HP Operations agent fails to update the discovered services to the HPOM management server. The possible cause and suggested action is as follows:

- *Possible cause:* The output of the Microsoft Exchange SPI discovery policy is not a properly formatted `xml` file.
- *Suggested action:* Run the Microsoft Exchange SPI discovery binary on the managed node. To do this:
  - a Login to the managed node as an administrator.
  - b From the command prompt, open the instrumentation directory.
  - c Run the `Exchange_discovery.exe > out.xml` command.
  - d Check the `out.xml` is in the required `xml` format by opening it in the web browser.

## Discovery Binary times-out on Managed Node

Sometimes, the Microsoft Exchange SPI discovery binary takes a lot of time to complete. In such cases, the discovery agent (agtrep) forcefully terminates the Microsoft Exchange SPI discovery binary before it completes. This causes the Microsoft Exchange SPI discovery failure.

You can identify the Microsoft Exchange SPI discovery binary termination by agtrep through the following statements in the `System.txt` of the managed node:

- 0: ERR: Thu Nov 12 10:52:01 2009: agtrep (4732/5412): (agtrep-151) Timeout occurred when executing action "C:\Windows\system32\cmd.exe /C ""C:/ProgramData/HP/HP BTO Software/bin/instrumentation/Exchange\_Discovery.exe"" - will be terminated.
- 0: ERR: Thu Nov 12 10:52:01 2009: agtrep (4732/5412): (agtrep-133) No output received from discovery policy action

The possible cause and suggested action for discovery failure are as follows:

- *Probable cause:* The Microsoft Exchange SPI discovery binary does not complete within the ACTION\_TIMEOUT period of agtrep.
- *Suggested Action:* Increase the ACTION\_TIMEOUT of agtrep to give sufficient time for the Microsoft Exchange SPI discovery binary to complete.

To increase ACTION\_TIMEOUT of agtrep:

- a Open the command prompt on managed node.
- b Run the command `ovconfchg -edit` to edit the agent configuration file. The default value is ACTION\_TIMEOUT=3
- c Increase the value of the ACTION\_TIMEOUT. For Example, ACTION\_TIMEOUT=10
- d Save and close the file.
- e Re-run the Microsoft Exchange SPI discovery.

## Troubleshooting through Tracing

With the help of the EXSPI Trace tool, you can obtain troubleshooting information from managed nodes. The Microsoft Exchange SPI stores the troubleshooting information as trace files in the `%OvDataDir%\bin\exspi\log` location on a managed node.

This tool enables you to set two trace levels:

- <T1Value> specifies trace level for Scheduler and CollectorServer. The value is either 0 or 1.
- <T2Value> specifies trace level for power shell script file. The value ranges from 0 to 2, where 2 is the maximum possible value.

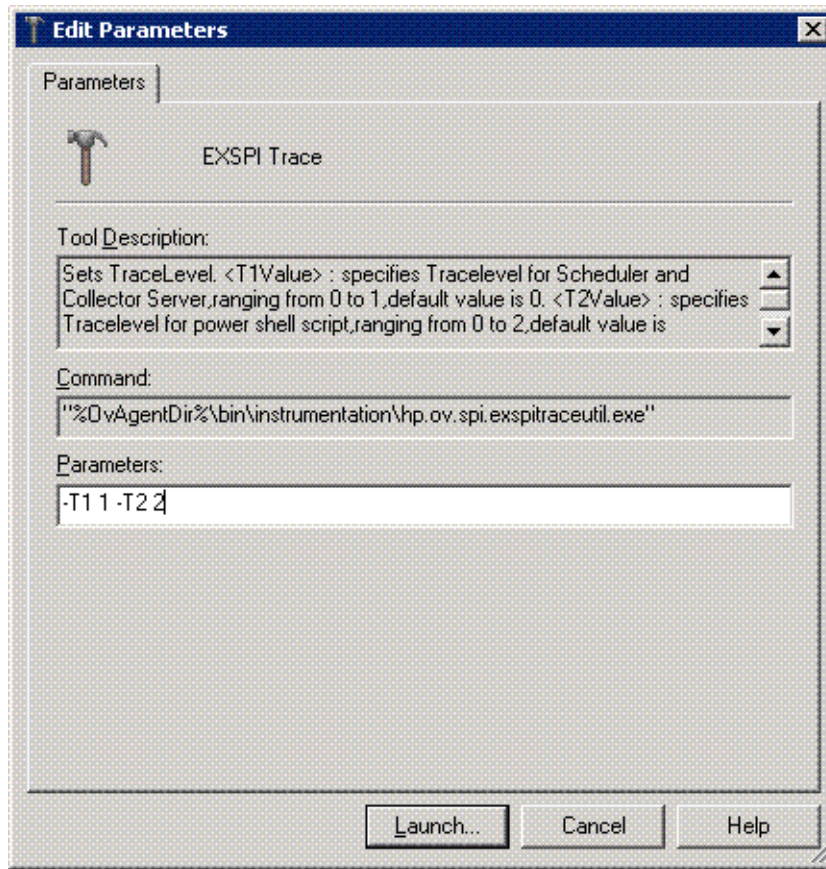


Each trace statement proceeds with a unique ID to distinguish between the different instances of the same collection which run simultaneously.

To launch the EXSPI Trace tool on a managed node, perform the following steps:

- 1 In the console tree, expand **Tools** → **SPI for Exchange**, and then double-click **Exchange 2007**.

- 2 In the details pane, double-click **EXSPI Trace**. The Select where to launch this tool dialog box opens.
- 3 Select a node, and then click **Launch**. The Edit Parameters dialog box opens. The Edit Parameters box contains values as -T1 0 -T2 0. You can replace the value with 0. For -T1 replace with 0 or 1 while with -T2 replace the value with 0, 1, or 2. This sets the trace value.
- 4 Click **Launch**.



## Troubleshooting Reports and Graphs

The following sections describe the possible cause and suggested action for the failed generation of data in Microsoft Exchange SPI reports and graphs.

### Reports and Graphs are not generated

In some cases, the reports and graphs are not generated. The possible cause and suggested action are as follows:

- *Possible cause:* The appropriate policies are not deployed to the respective Microsoft Exchange SPI reports and graphs. The policy, therefore, fails to collect the data which the HP Reporter generates as report. Failure to deploy the appropriate policy also disables the HP PM to generate graphs.

- *Suggested action:* See Appendix B Report, Report Table, Data Store, and Policy Mapping Details in *HP Operations Smart Plug-in for Microsoft Exchange Server Reference Guide* to know the appropriate policy for each Microsoft Exchange SPI report. See also Graphs, Data Store, and Policy Mapping Details in *HP Operations Smart Plug-in for Microsoft Exchange Server Reference Guide* to know the appropriate policy for each Microsoft Exchange SPI graph. Deploy the policy accordingly.

For troubleshooting reports see *Troubleshooting Microsoft Exchange SPI Reports* in *HP Operations Smart Plug-in for Microsoft Exchange Server Online Help*.

## Data Logging Policies cannot log Data

In some cases the data logging policies cannot log data. The possible cause and the suggested action are as follows:

- *Possible cause:* The data source is not created in the datastores—CODA or OVPA.
- *Suggested action:* Check if the datasource EX2007\_DATA is created. To do this:
  - a Login to the managed node as an administrator.
  - b From the command prompt run the `ovcodutil -obj > out.txt` command.
  - c Check the `out.txt` file to ensure that the datasource EX2007\_DATA is created.

## Browser Crashes while Viewing HTML Report

While viewing the reports in HTML format, the browser crashes. The possible cause and the suggested action are as follows:

- *Possible cause:* The browser cannot handle huge amount of data.
- *Suggested action:* View the reports in PDF format.

## Reports Fails with Oracle Database

Some of the reports fail due to invalid Reporter ODBC driver.

- *Possible cause:* The versions of Oracle client to access Oracle database do not match.
- *Suggested action:* Use Oracle client 9.2.0 to access Oracle 9.2.0 database and 10gR2 client to access 10gR2 database.

## Modifying Policy Names

If you change the default name of the following Microsoft Exchange SPI policies, ensure to change the SPIMetaData.xml also:

- EXSPI-8X\_ReplicationCopyQueueLength
- EXSPI-8X\_ReplicationReplayQueueLength
- EXSPI-8X-HubMonitorBlockedMails
- EXSPI-8X-EdgeMonitorBlockedMails
- EXSPI-8X\_Check\_IMAP4ServiceStatus
- EXSPI-8X\_Check\_POP3ServiceStatus
- EXSPI-8X\_Check\_ADTopologyServiceStatus
- EXSPI-8X\_Check\_CASFileDistributionServiceStatus



Change all references to these policies to new policy names in the policy command line and in the SPIMetaData.xml.

For details on each Microsoft Exchange SPI policy, see *HP Operations Smart Plug-in for Microsoft Exchange Server Online Help* or *HP Operations Smart Plug-in for Microsoft Exchange Server Online Help PDF*.



## 8 Removing Microsoft Exchange SPI

You can remove the Microsoft Exchange SPI in the following ways:

- Using DVD
- Using Windows Control Panel - Add/Remove Programs

To remove Microsoft Exchange SPI remove all the policies and policy groups from the managed nodes, and then from the management server.

▶ Undeploy all Microsoft Exchange SPI policies from all managed nodes before uninstalling.

### Using DVD

You must remove SPI components manually before removing SPI from the management server using a DVD.

### Removing Microsoft Exchange SPI Components

The Microsoft Exchange SPI components include policies, reporting package, and graphing package.

**Task 1:** Remove the Microsoft Exchange SPI policies from all managed nodes

- 1 At the console expand the folder **Policy Management**.
- 2 Right-click **SPI for Exchange**, and select **All tasks** → **Uninstall from...**
- 3 In the **Uninstall on...** window, select each check box next to one or more nodes from which you want to remove the policies.
- 4 Click **OK**.

▶ To verify policies have been removed, at the HPOM console expand the **Nodes**, right-click a node, and then select **View** → **Policy Inventory**.

**Task 2:** Remove Microsoft Exchange SPI programs from the HPOM management server

- 1 Insert the *HP Operations Smart Plug-ins* DVD.
- 2 Follow the instructions as they appear on the screen and start the uninstall procedure by selecting the **Remove products**.
- 3 In the **Product Selection Uninstall** window, select **Microsoft Exchange (SPI)**, and click **Next**.
- 4 In the next window select **Remove**.

▶ Each window updates you with the status of uninstalling the Microsoft Exchange SPI.

- 5 Click **Finish** to complete.

### Task 3: Remove the Microsoft Exchange SPI Policies from the Management Server

- 1 Expand the Agent Policies grouped by type.
- 2 From each policy type, delete all versions of the policies which start with the name **EXSPI**.

## Using Windows Control Panel

Remove SPI components before removing the Microsoft Exchange SPI from the management server. To remove SPI components manually, perform the tasks in [Removing Microsoft Exchange SPI Components](#).

### Removing Microsoft Exchange from Management Server

To remove SPI from the management server, perform the following steps:

- 1 From the Start menu, select **Settings** → **Control Panel**, and open **Add/Remove Programs**.



When you use the Windows Control Panel to remove any SPI, you have two options: (1) to remove selected SPIs or (2) to remove HPOM for Windows. If you want to remove both HPOM and SPIs, you must first remove all Smart Plug-ins from managed nodes then from the management server. You can then remove SPI from HPOM.

- 2 Select **HP Operations Smart Plug-ins**, and then click **Change**.
- 3 Click **Next** on the Welcome screen.
- 4 Select **Remove Programs**, and select **HP Operations Smart Plug-ins**.
- 5 Select **EXSPI**.
- 6 Complete the instructions until a message appears which shows that Microsoft Exchange SPI is removed.

### Removing Reporting package

To remove reporting package, perform the following steps:

- 1 From the Start menu, select **Settings** → **Control Panel**, and open **Add/Remove Programs**.
- 2 Select the reporting package, and then click **Change**.
- 3 Complete the instructions until a message appears which shows that HP Reporter has been removed.

### Removing Graphing package

To remove graphing package, perform the following steps:

- 1 From the Start menu, select **Settings** → **Control Panel**, and open **Add/Remove Programs**.
- 2 Select the graphing package, and then click **Change**.



- 3 Complete the instructions until a message appears which shows that HP performance Manager has been removed.

## Removing Reporting and Graphing Package using .msi File

You can also remove the reporting and graphing package by using .msi file.

### Removing Reporting Package using .msi file

To remove the reporting package using .msi file, perform the following steps:

- 1 Browse to:  
`<SPI DVD>\SPIS\Exchange SPI Reporter Package\EXSPI-Reporter.msi`
- 2 Right-click EXSPI-Reporter.msi, and then click **Uninstall**.
- 3 Confirm the removal of the reporting package by clicking **Yes**.

### Removing Graphing Package using .msi File

To remove the graphing package using the .msi file, perform the following steps:

- 1 Browse to:  
`<SPI DVD>\SPIS\EX SPI OVPM ConfigurationPackage\HPOvSpiExGc.msi`
- 2 Right-click HPOvSpiExGc.msi, and then click **Uninstall**.
- 3 Confirm the removal of the graphing package by clicking **Yes**.



# A List of Microsoft Exchange SPI Instrumentation Files

Appendix A provides instrumentation category details of the Microsoft Exchange SPI in the following tables.

## Exchange2k7\_Collector

**Table 8 Instrumentation Category Details - Exchange2k7\_Collector**

Category	Description
HP.OV.SPI.ExCollectorServer.exe	Daemon which runs on the node and starts the powershell script (exspi2007.ps1) for each collection.
HP.OV.SPI.ExCollectorServer.exe.config	Configuration file for HP.OV.SPI.ExCollectorServer.exe
HP.OV.SPI.EXCustomCmdlets.dll	Defines the Microsoft Exchange SPI custom cmdlets
exspi2007.ps1	PowerShell script which formulates and executes the Microsoft Exchange cmdlets and logs data or sends alerts, or does both.

## Exchange 2k7\_Core

**Table 9 Instrumentation Category Details - Exchange 2k7\_Core**

Category	Description
HP.OV.SPI.ExspiTraceUtility.exe	Sets the trace levels for the scheduler and the collector server.
HP.OV.SPI.ExScheduler.exe	Requests the collector server to launch a collection with the required parameters.
HP.OV.SPI.ExScheduler.exe.config	Configuration file for HP.OV.SPI.ExScheduler.exe
HP.OV.SPI.Terminator.exe	Stops the collector server
HP.OV.SPI.ExBPAScheduler.exe	Calls the ExBPA (Exchange Best Practices Analyzer) command line utility
CheckServiceState.exe	Returns the state of a particular service
exspidatasource.exe	Creates the datasource for Microsoft Exchange SPI and sets certain registry entries which are utilized by the collector server.

<b>Category</b>	<b>Description</b>
EX2007_AVAILABILITY.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass EX2007_AVAILABILITY
ex2007_senderid.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_senderid
ex2007_fdsum.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_fdsum
ex2007_isperf.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_isperf
ex2007_mbsummary.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_mbsummary
ex2007_pfsummary.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_pfsummary
ex2007_mbdetail.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_mbdetail
ex2007_pfdetail.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_pfdetail
ex2007_isclient.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_isclient
ex2007_umipgway.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_umipgway
ex2007_pfperf.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_pfperf
ex2007_pop3perf.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_pop3perf
ex2007_mbperf.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_mbperf
ex2007_umhunt.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_umhunt

<b>Category</b>	<b>Description</b>
ex2007_ummbox.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_ummbox
ex2007_imap4perf.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_imap4perf
ex2007_replsumm.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_replsumm
ex2007_umpin.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_umpin
ex2007_smtprecv.spec	Specifies the column names and data types for the EXSPI dataclass ex2007_smtprecv
ex2007_umsrv.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_umsrv
ex2007_qinfo.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_qinfo
ex2007_smtpsend.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_smtpsend
ex2007_agcfg.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_agcfg
ex2007_umply.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_umply
EX2007_DEST.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass EX2007_DEST
EX2007_RECP.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass EX2007_RECP
EX2007_SENDER.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass EX2007_SENDER
EX2007_SOURCE.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass EX2007_SOURCE

<b>Category</b>	<b>Description</b>
ex2007_transq.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_transq
ex2007_umautoattendent.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_umautoattendent
ex2007_umavailability.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_umavailability
ex2007_umcallanswer.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_umcallanswer
ex2007_umfax.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_umfax
ex2007_umgeneral.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_umgeneral
ex2007_umsubaccess.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_umsubaccess
ex2007_blockedmails.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_blockedmails
ex2007_blockedrcpts.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_blockedrcpts
ex2007_spamstats.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass ex2007_spamstats
ex2007_MailFlowLatency.spec	Specifies the column names and data types for the Microsoft Exchange SPI dataclass EX2007_MFLAT
CmdletCommands.xml	Lists the datatypes of the properties of all the Microsoft Exchange cmdlets used in the Microsoft Exchange SPI.
spimetadata.xml	Defines the various default and user-defined Microsoft Exchange SPI collections.
spi_msexch.xml	Defines the various modes under which SHS collector can run.
spi_msexch_chkexch.vbs	Checks the operating system and Microsoft Exchange server information for use by SHS collector.

<b>Category</b>	<b>Description</b>
spi_msexch.cmd	Calls shs_collector.pl which launches the SHS collector.
spi_msexch_runSHSCollector.cmd	Used by the self-healing client to run the SHS collector.
spi_msexch_shs_install.xml	Contains the Microsoft Exchange SPI installation folder details.
spi_msexch_shs_input.xml	Contains the input parameters for spi_msexch.cmd
register.bat	Registers HP.OV.SPI.EXCustomCmdllets.dll
Exspi_exshell.psc1	Defines the Microsoft Exchange SPI custom PS snap-in.
exbpa_wrapper.vbs	Wrapper script which calls ExBPACmd.exe
exspi_e2k7_clust_config.js	Generates the apminfo.xml file which describes the cluster instances
ovosysdetect_exspi.pl	Checks whether the Microsoft Exchange SPI is installed
license.vbs	Checks the license validity of the Microsoft Exchange SPI

## Exchange2k7\_Discovery

**Table 10 Instrumentation Category Details - Exchange2k7\_Discovery**

<b>Category</b>	<b>Description</b>
interop.opcautolib.dll	dll used in the Microsoft Exchange SPI discovery
Exchange_Discovery.exe.config	Configuration file for Exchange_Discovery.exe
discoverresult.dll	Used by Exchange_Discovery.exe to create the Microsoft Exchange SPI service discovery tree.
Exchange_Discovery.exe	Discovers the Microsoft Exchange topology and services.
msexchange.apm.xml	Contains the list of the Microsoft Exchange SPI policies that are to be disabled on a passive cluster node
ex2k7_rundiscovery.js	Runs the Microsoft Exchange SPI discovery policy (Exchange 2007 Discovery) on a cluster node after a cluster failover happens.





# Index

## E

Edit XPL Configuration File, 31  
EXSPI Data collector, 45

## F

Flowchart, 15

## G

Graphs, 91

## H

HP Operations Manager, 9  
HP Operations Topology Viewer, 84  
HP Operations Topology Viewer Tool, 13  
HP Performance Manager, 94  
HP Reporter, 91

## I

Installation Environments, 18  
    Standalone HP Reporter or HP Performance  
    Manager, 19  
    Standard Installation, 18  
    Standard Installation on Remote Consoles, 19

## L

Legends, 15

## M

Managed node, 28  
Message Alerts, 13  
Microsoft Exchange Server 2007, 10

## P

Policy Group, 38, 79  
Policy Type, 80

## R

READ+WRITE access, 31

Report Package, 92

Reports, 91

## S

SAN environment, 14  
Servicemap View, 12  
Severity levels, 12  
Smart Plug-in for Microsoft Exchange Server, 10  
Software Upgrade Tool Kit, 24



## 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:**

