User Guide:

HP OpenView SPI For Antigen

Sybari

TRADEMARK NOTICES
ANTIGEN, EVER VIGILANT PROTECTION, LIVENOTES, SYBARI, ADVANCED SPAM DEFENSE, SPAM MANAGER, ADVANCED SPAM MANAGER, SYBARI ENTERPRISE MANAGER, WORMPURGE, ANTIGEN FILE FILTERING, ANTIGEN WORM PURGE, AND ANTIGEN CENTRAL MANAGER and the logo forms of the foregoing marks, are trademarks and/or service marks of Sybari Software, Inc. or its subsidiaries and may be registered in the United States or in other jurisdictions including internationally. Sybari Software, Inc.'s trademarks, service marks and trade dress may not be used in connection with any product or service that is not affiliated with Sybari Software, Inc., in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Sybari Software, Inc. All other trademarks not owned by Sybari Software, Inc. or its subsidiaries that appear in this publication are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Sybari Software, Inc. or its subsidiaries.

FEEDBACK
Sybari appreciates your comments and reserves the right to use any information you supply in any way it believes appropriate without incurring any obligations whatsoever. Please address your feedback to: Sybari Software, Inc., 353 Larkfield Road, East Northport, NY 11731, or send email to info@sybari.com.

Contents

Index

Chapter 1 – Introducing OpenView SPI

Sybari's Smart Plug-In (SPI) for Antigen is a powerful new module that enables Sybari's Antigen for Microsoft Exchange, Antigen for SMTP Gateways, and Advanced Spam Manager to provide critical security management data to HP OpenView Operations Manager for Windows (OVOW).

Sybari's OpenView SPI for Antigen allows you to monitor the status of Antigen servers and engine updates and monitor virus and spam alerts. Events (such as a concentrated virus attack) are propagated to the OpenView console, which immediately alerts administrators and can be programmed to take a custom action that uses an Antigen tool or a custom script. The Antigen SPI can also be used to launch the Sybari client on remote Antigen servers to view additional reporting or centrally modify Antigen's security configurations.

Sybari's OpenView SPI scripts include UI integration into several support tools that perform simple actions, such as on-demand signature updates.

What Is A Smart Plug-In?

A Smart Plug-In (SPI) for OpenView Operations For Windows is an addition to the OVOW product that provides extended or incremental system or application management capabilities on top of the capabilities provided by the out-of-the-box OVOW product.

For it to function, an SPI requires that OVOW be installed and running. Further, an SPI for OVOW is a product that is created for a specific management capability, such as managing a multi-tier software system (like SAP/R3) or a database environment (like Oracle).

Definitions

These are terms that you will find throughout this User Guide.

OVOW
: OpenView Operations For Windows, a third party product for software monitoring provided by Hewlett-Packard.

OVO Policy
: A set of rules and actions that helps to automate network, system, and application administration.

SPI
: A Smart Plug-In, a Hewlett-Packard OpenView term for product plug-ins used to manage and monitor remote systems.

Functionality

The OpenView SPI For Antigen provides monitoring functionality in the following areas:

Command Line Tool Integration
A component of SPI used to provide access to command line utilities, such as engine updates from the OVOW console menus.

Alert Management Tools
A component of SPI used to enable, disable, and configure thresholds on Antigen WMI events for Virus Outbreaks, Spam, etc.

OpenView Operations Policies
Policies are the parts of SPIs that instruct OVO agents how to monitor remote antigen products and indicate which logs to monitor. For Antigen, the program log, event log, and WMI events will be the main source of information.

OpenView Node Group Installation
The SPI install creates an “Antigen Servers” group in the node section of the OVO console. Node groups provide an association between the Antigen SPI’s policies/tools and the servers being monitored. Servers running antigen need to be manually added to this group.

How To Contact Us

Customer Service

To order products or obtain product information, please contact the sales office in your region.

[For Pre-Sales Technical Support, please contact our Pre-Sales Support department in the US at 1-631-630-8500 (press option 2 for our Support Menu and then press option 2) or in Spain at +34 91 296 2600]

In North America:
Sybari Software, Inc.
353 Larkfield Road
East Northport, NY 11731-1429
U.S.A.
Tel: 1-631-630-8500

and

Sybari Software California
1299 Del Mar Avenue, Suite 110
San Jose, CA 95128 U.S.A.
Tel: 1-408-938-9050

In France:
Sybari Software France
La Grande Arche. Paroi Nord
92044 Paris-La Defense, France
Tel: +33 1 4090 3022
sales-fr@sybari.com

In Germany:
Sybari Software GmbH
Mühlweg 2 B
D-82054 Sauerlach (bei München)
Tel: +49 (0) 8104 6493 0
sales-de@sybari.com

In Italy:
Sybari Software Italy
Viale America 93
00144 Rome, Italy
Tel +39 06 591 5591
sales-it@sybari.com

In the Netherlands:
Sybari Software Benelux
“Het Poortgebouw”
Beech Avenue 54-80
1119 PW Schiphol Rijk
The Netherlands
Tel: +31 0 20-6586952
sales-nl@sybari.com

In the UK:
Sybari Software UK
188-192 Sutton Court Road
Chiswick
London W4 3HR, U.K.
Tel: +44 0 20 8987 3280
sales-uk@sybari.com

In Spain and other EU Countries:
Sybari Software S.A.
C/General Yagüe, 6
28020 Madrid, Spain
Tel: +34 91 296 2600
Fax: +34 91 296 2601
sales-eu@sybari.com

In the Middle East and Africa:
Sybari Software Mid-East
Dubai Internet City Building, 9, Office 209
PO Box 500154
Dubai, UAE
Tel: +971 4 391 3711
sales-mea@sybari.com

In Asia/Pacific:
Sybari Software APAC
Penthouse Level, Suntec Tower Three
8 Temasek Blvd.
Singapore, 038988
Tel: +65 8663 767

In China:
Sybari Software
Rm. 612, Beijing Towercrest Plaza,
No. 3 Mai Zi Dian West Road,
Chao Yan District, Beijing, 100016
China
Tel: +86 10 64606127

In Australia and New Zealand:
Sybari Software Australia Pty Ltd
Unit 21, Building 7
49 Frenchs Forest Rd
Frenchs Forest, NSW, 2086
Australia
Tel: +61 2 9454 8000
Fax: +61 2 9454 8070

You can also visit us at our web site: http://www.sybari.com/

Technical Support

Sybari is famous for its dedication to customer satisfaction. Sybari has continued this tradition by investing considerable time and effort to make our website a valuable resource for updating Sybari software and obtaining the latest news and information. For technical support information, we encourage you to visit our website first:

http://www.sybari.com/

Contacting Our Technical Support Team

- In North America and Latin America:
  - **East Northport, NY Office:**
    1-631-630-8500 option #2
    8 am - 8 pm EST
  - **San Jose, CA Office:**
    1-408-938-9050 option #6
    8 am - 6 pm PST

    support@sybari.com
- In the Europe/Africa region:

  Madrid, Spain Office:
  +34 91 296 2600
  9 am - 7 pm ECT

  support.eu@sybari.com
- In the Asia/Pacific region:

  Singapore Office:
  +65 6533 3018 Ext. 16
  9 am - 6 pm Singapore Time (GMT +8)

  support.eu@sybari.com
- In Australia and New Zealand:

  Sydney, Australia Office:
  +61 2 9454 8000
  9 am - 6 pm Sydney Time (GMT +11)

  support.eu@sybari.com

Chapter 2 – Installation

The Sybari SPI For Antigen is easy to install on servers running HP OpenView Operations Manager. The steps to install and uninstall the SPI For Antigen are described below.

Requirements

Please Note: User customizations will not be retained in new SPI-installed versions of the same policies. Such customizations will need to be merged to the newer version installed. This is especially important if you have removed policies prior to the upgrade

Operating System

Sybari's SPI For Antigen can be installed under any of these operating systems:

- Windows 2000
- Windows XP
- Windows Server 2003

Operations Manager Server Requirements

HP integration requires that OpenView SPIs run on the same system as OpenView Operations Manager (version 7.*x* or later). Operations Manager Server requires the following:

- Windows 2000 Server/Advanced Server Edition (SP3 or higher) or Windows 2003 Standard/Enterprise/Data Center Server.
- 500MHz Intel Pentium III (or compatible) processor, 1 GHz recommended.
- 512 MB physical memory, with at least 512 MB virtual memory (page file)
- Minimum 10 GB hard drive. 1.2 GB disk space is required for installation (depending on selected product options.)
- We recommend at least 4 GB free disk space for event and performance databases. Hard drives with at least 20 GB are recommended.
- CD Rom Drive
- 17 Inch monitor with 1024x768 resolution and at least 256 colors.

Managed Node Requirements

- Windows 2000, Windows NT 4.0, Windows XP Professional, or Windows Server 2003.
- 15 MB memory for agent processes
- 40 MB hard disk space for installation, and databases. Actual size may vary depending on what policies are installed, and how much data is collected.

Before You Start

Prior to the installation of SPI For Antigen, ensure that both the Antigen client and HP OpenView Operations For Windows are installed on the server where you plan to install the product.

Installation

Once you've downloaded the product from the Sybari site, simply double-click SETUP.EXE and the product will install itself. There are no parameters to be entered or questions to be answered. All components are installed into existing HP OpenView folders.

Installation creates the following groups within the OVOW Console:

- Antigen Servers node group. This node group contains the managed nodes that are running Antigen.
- SPI For Antigen group within Tools. This has the following subgroups:
  - Alert Management
  - Engine Management
- SPI For Antigen policy group.

Uninstalling

To remove the SPI For Antigen, follow these steps:

1. All policies within the SPI For Antigen group currently deployed to managed nodes must be uninstalled. If they are not, they will not be automatically removed from the management console.

   Please Note: If you have modified any policies, the uninstall will not automatically remove them. They will have to be manually removed through the OVOW Console.

2. Remove SPI for Antigen by using Add/Remove Programs in the Windows Control Panel.
3. In the OpenView console, manually delete the Antigen Servers node group, the SPI For Antigen tools group, and the SPI For Antigen policy group.

Upgrading From An Earlier Version

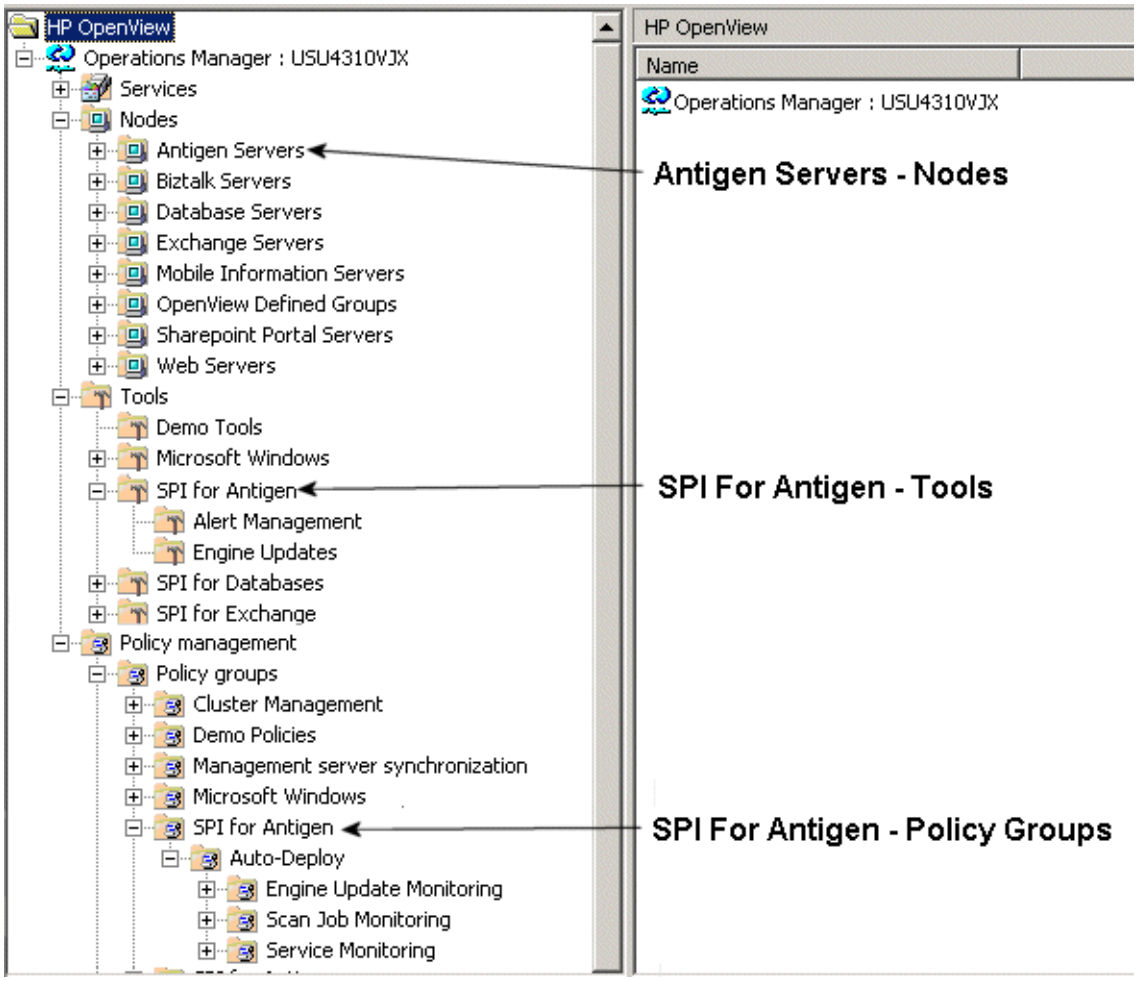
If a previous version of the Sybari Smart Plug-In (SPI) For Antigen is installed, that version must be removed before installing the latest version. Please see Uninstalling, above for more information on uninstalling the product.

Chapter 3 – Using The OpenView SPI For Antigen

Once you have installed SPI For Antigen, you can immediately use it to see alerts on the Console and to manage the criteria for triggering those alerts. The Console is also used to configure new nodes, connect to the Antigen client, and update scanning engines.

The HP OpenView Operations Console

This is what the HP OpenView Operations Console looks like after the SPI For Antigen has been installed:



The install creates three new items in the Operations Console:

1. In Nodes, there is a new Antigen Servers node group. Add managed nodes to this group to associate them with Antigen tools and policies (see Adding Nodes, below).
2. In Tools, there is a new SPI For Antigen group. It has two subgroups:
   - Alert Management – tools to handle and configure alerts sent from Antigen (see Alert Management, below).
   - Engine Updates – tools to allow you to update any of Antigen's installed scanning engines at any time (see Engine Updates, below).
3. In Policy Management, there is a new SPI For Antigen group. This contains policies that are deployed to a managed node to watch logs for incidents. If an incident is found, an alert is displayed on the OpenView console. (See both Policy Management and Alert Management, below.)

   Please Note: When a new Antigen server is added to the Antigen Servers node group, all policies are automatically deployed to it.

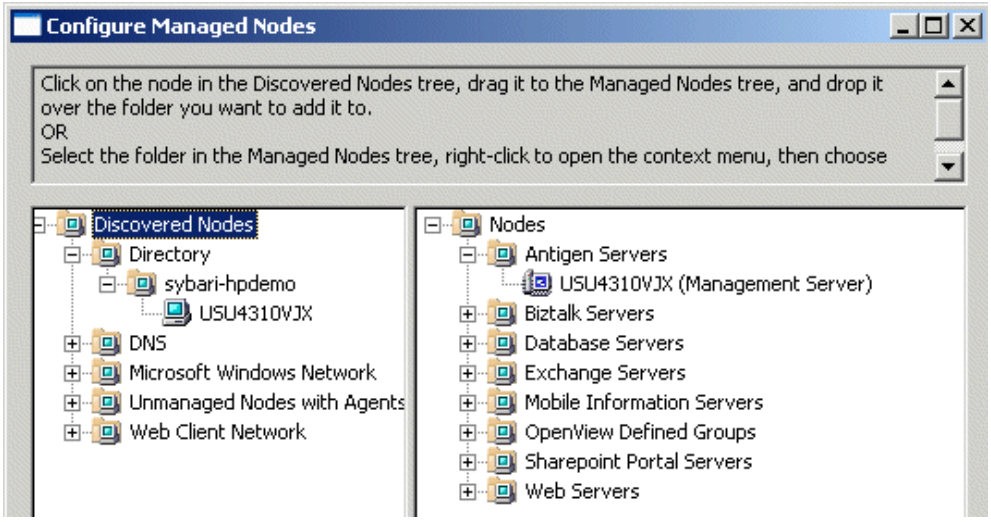
Antigen Servers Node Group

This node group contains the managed nodes that are running Antigen.

Adding Nodes

The Antigen Servers node group is empty when the SPI For Antigen is installed. To populate it, follow these steps to add a node for each server running Antigen:

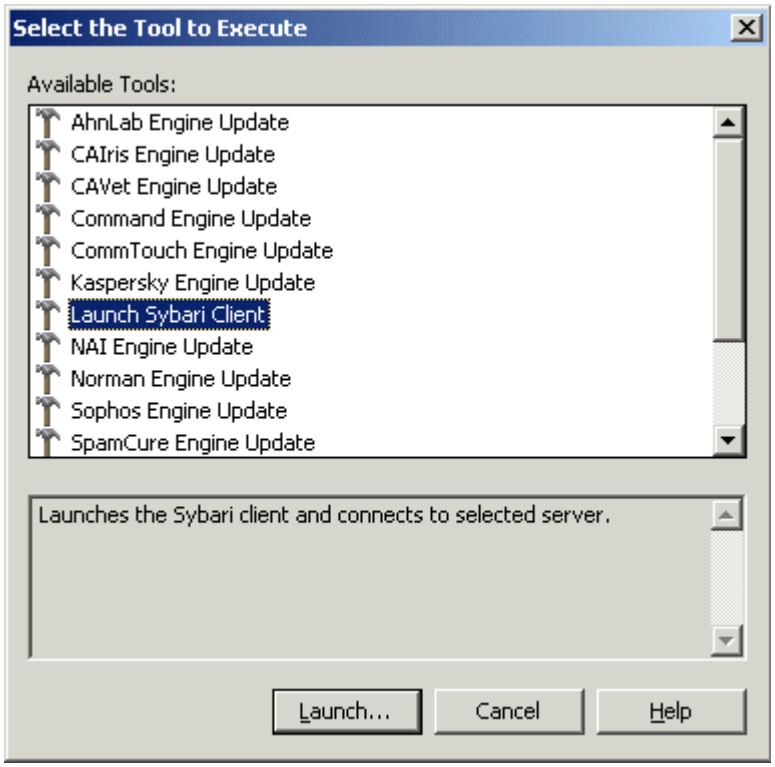
1. Right-click on the Nodes group to get the context-sensitive menu.
2. Select Configure Nodes. The *Configure Managed Nodes* dialog appears. All the nodes that OpenView has discovered on the network are shown in the left pane.



3. Select a node on the left side and drag it to the right side, dropping it onto the Antigen Servers node group.
4. Once you have added all the desired nodes, click OK to return to the Console. All the nodes will appear under the Antigen Servers node group.

Launching Antigen Tools

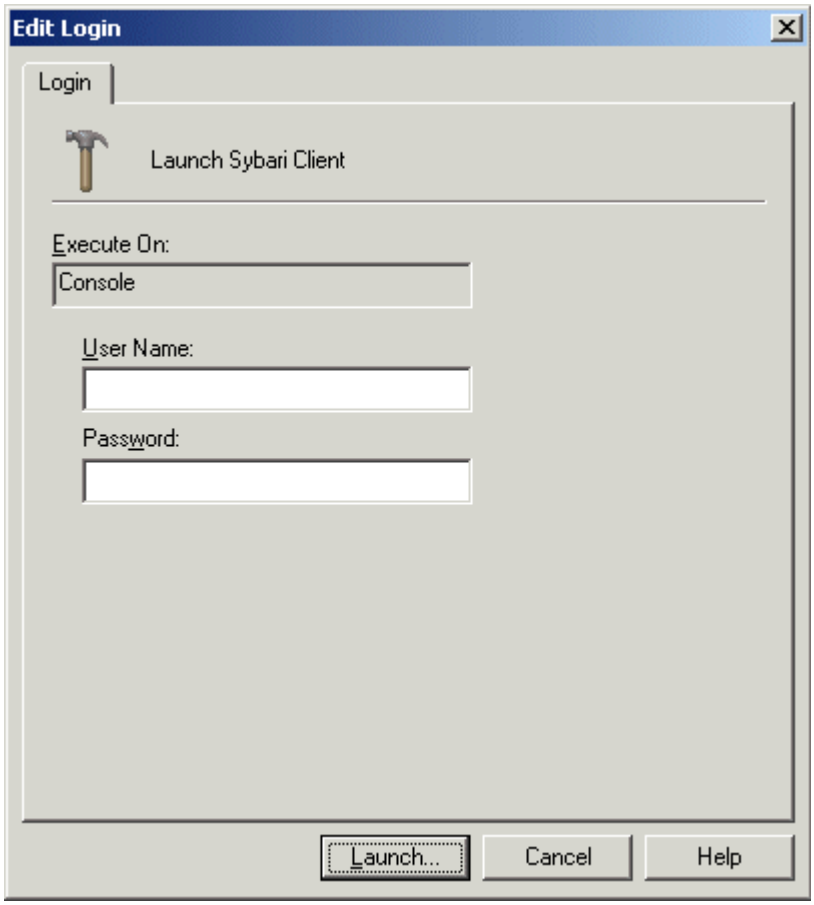
To launch either an engine update or to connect the Sybari client to a specific node, select that node from the Antigen Servers node group. Right-click it and, from the context menu, select All Tasks, and then Launch Tool. The *Select The Tool To Execute* dialog displays:



Select an item on the list: either Launch Sybari Client (to start the Antigen client) or one of the engines (to do an on-demand update). Click Launch to continue.

Launch Sybari Client

When you select Launch Sybari Client from the *Select The Tool To Execute* dialog, the *Edit Login* dialog displays:

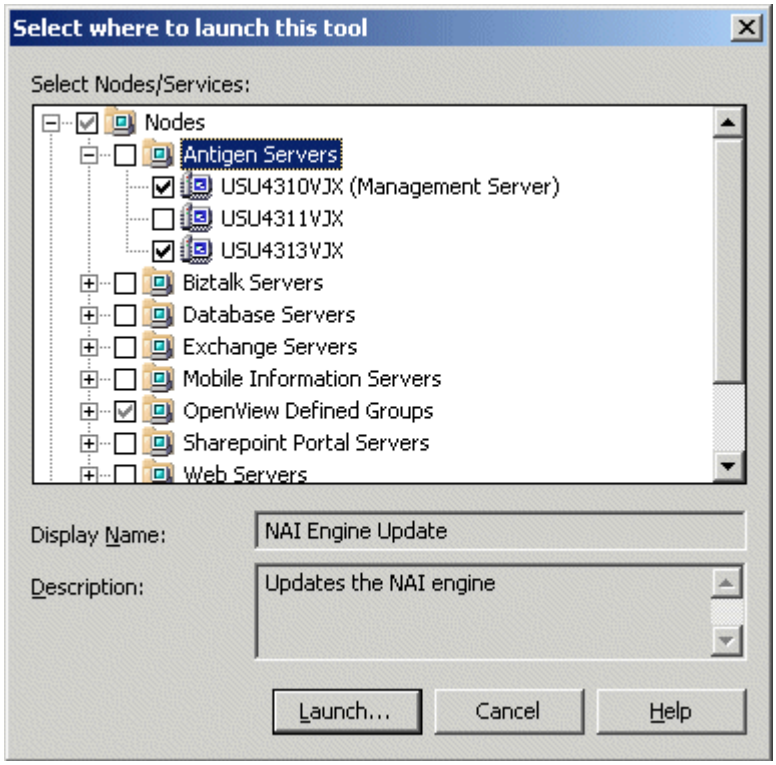


Clicking Launch on the *Edit Login* dialog starts the Sybari Client GUI.

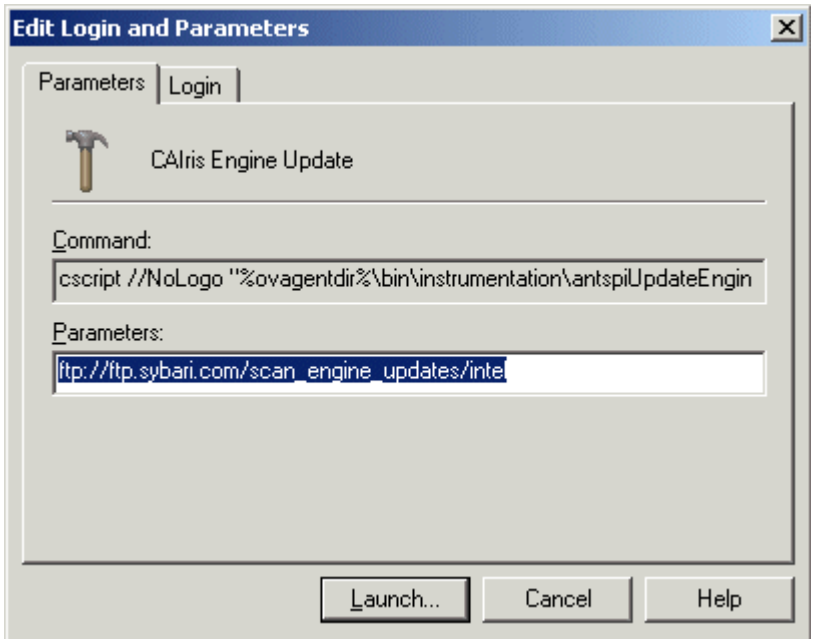
Please Note: Leaving the User Name and Password fields blank launches the Sybari client as the currently logged-on user.

Engine Updates

When you select an engine to be updated, from the *Select The Tool To Execute* dialog, the *Select Where To Launch This Tool* dialog displays:

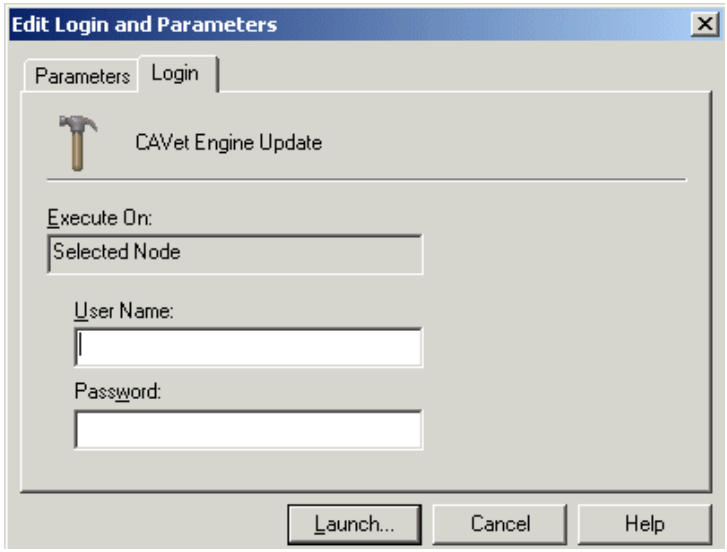


Use this dialog to select one or more servers to which the scanning engine update should be applied, and then click Launch. The *Edit Logon And Parameters* dialog appears:

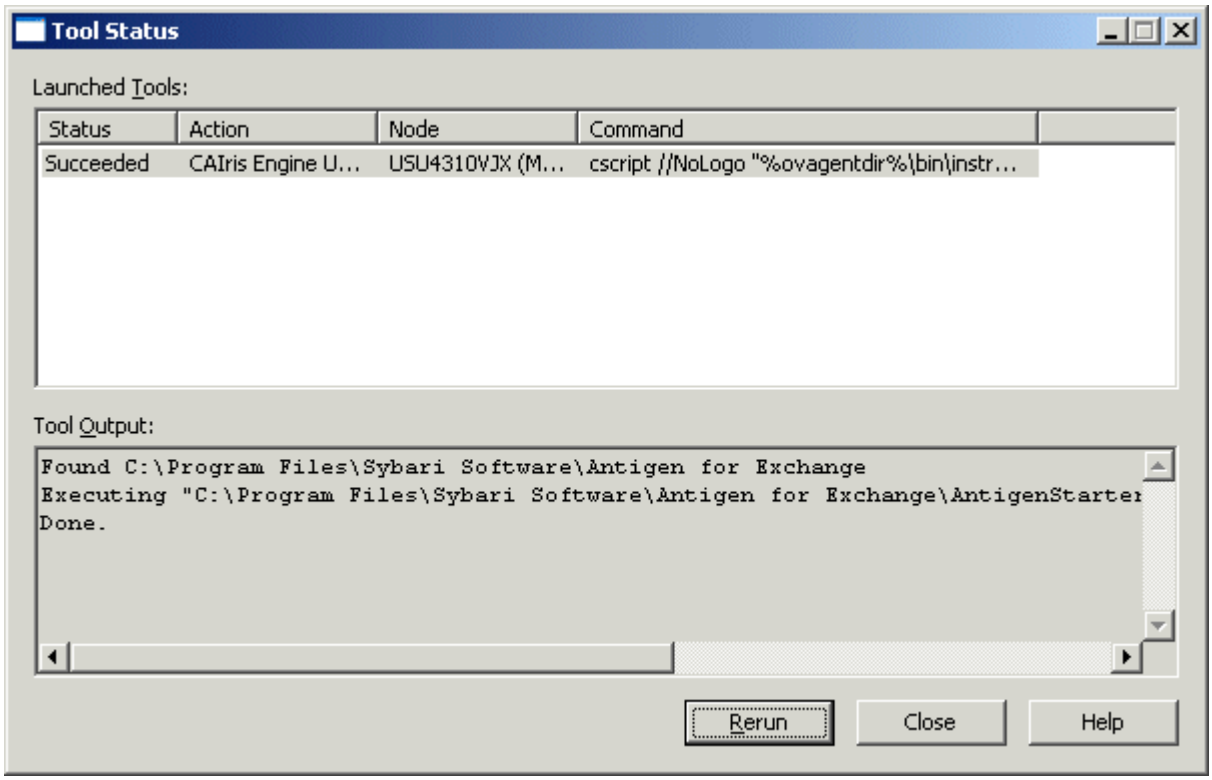


Please Note: The Parameters field displays with the default download path for the engine. You can change it to some other path, but unless you edit and modify the tool itself, the same default path will show up the next time the update is invoked.

If you are executing a remote engine update, use the Login tab to enter the login credentials of a user with permissions to execute the AntigenStarter utility on the managed node.



Click Launch to begin the update. The *Tool Status* dialog appears, showing you the results of the update attempt:



When the update finishes, click Rerun (in case there was a problem) or Close (to bring you back to the Console).

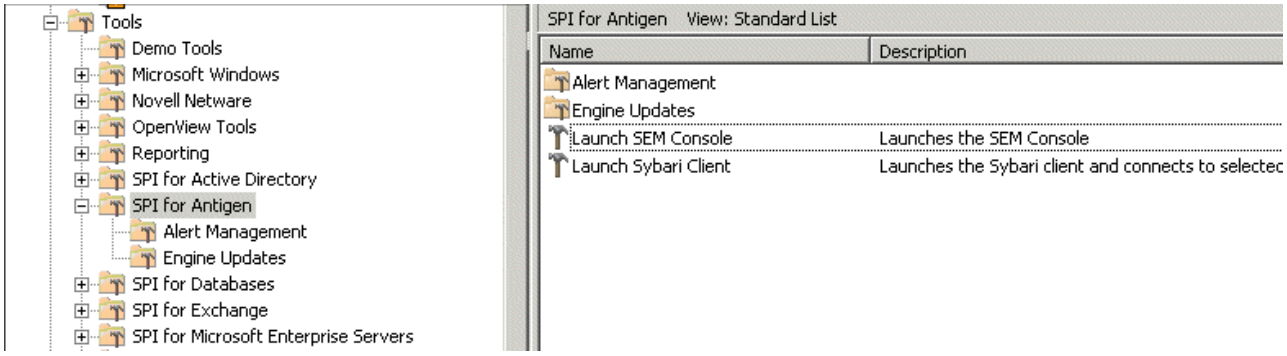
Please Note: The *Select The Tool To Execute* dialog lists all the scanning engines that Sybari supports. The only ones that you can successfully update, however, are those for which you have obtained a license. If you attempt to update an unlicensed engine, the Tool Status will indicate success, but the Console will show a message that you were not licensed to update that engine.

Please Note: To prevent informational engine update notification messages from being displayed in the OVOW Console, create a message filter that filters unmatched normal severity messages from the GetEngineFiles application. Please see *HP OpenView Operations* help for more information on creating message filters.

Tools

This item contains several tools, both in the main folder (SPI For Antigen) and in its two subgroups: Alert Management and Engine Updates.

When you select SPI For Antigen (under Tools), two tools appear in the right pane: Launch SEM Console and Launch Sybari Client. There are also folders for Alert Management and Engine Updates.



Launch SEM Console

Double-clicking this link launches the SEM Console, assuming that the web page is installed on the local host. You can modify the tool to point to the path of the server, if it isn't on the local host or if you are going to execute the tool from a remote console.

Launch Sybari Client

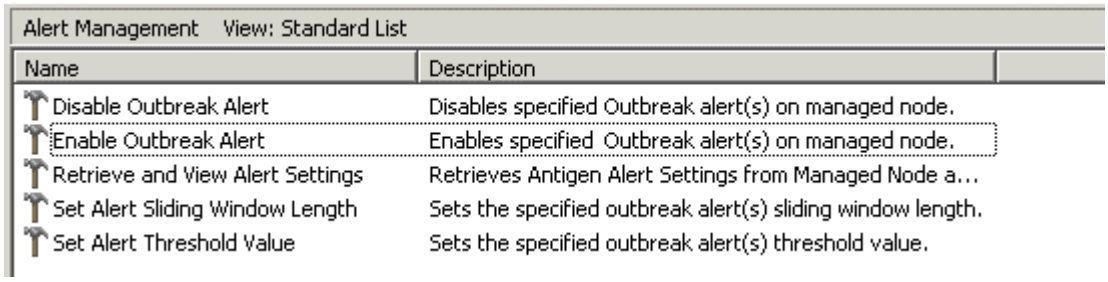
Displays the Sybari Client GUI. Double-click to display the *Edit Login And Parameters* dialog. Select a server and click Launch. The Sybari Client is launched and a connection is made to the selected server.

Alert Management

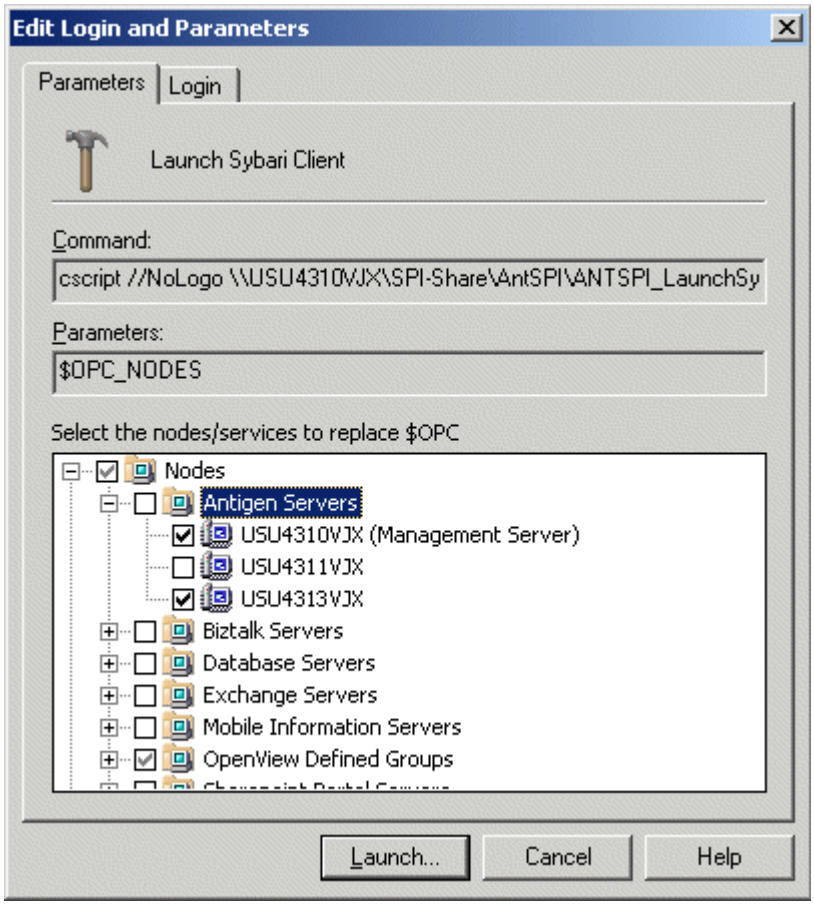
Use this facility to configure and manage outbreak alerts.

Managing Outbreak Alerts

When you double-click Alert Management, the names of the available tools display in the right pane:



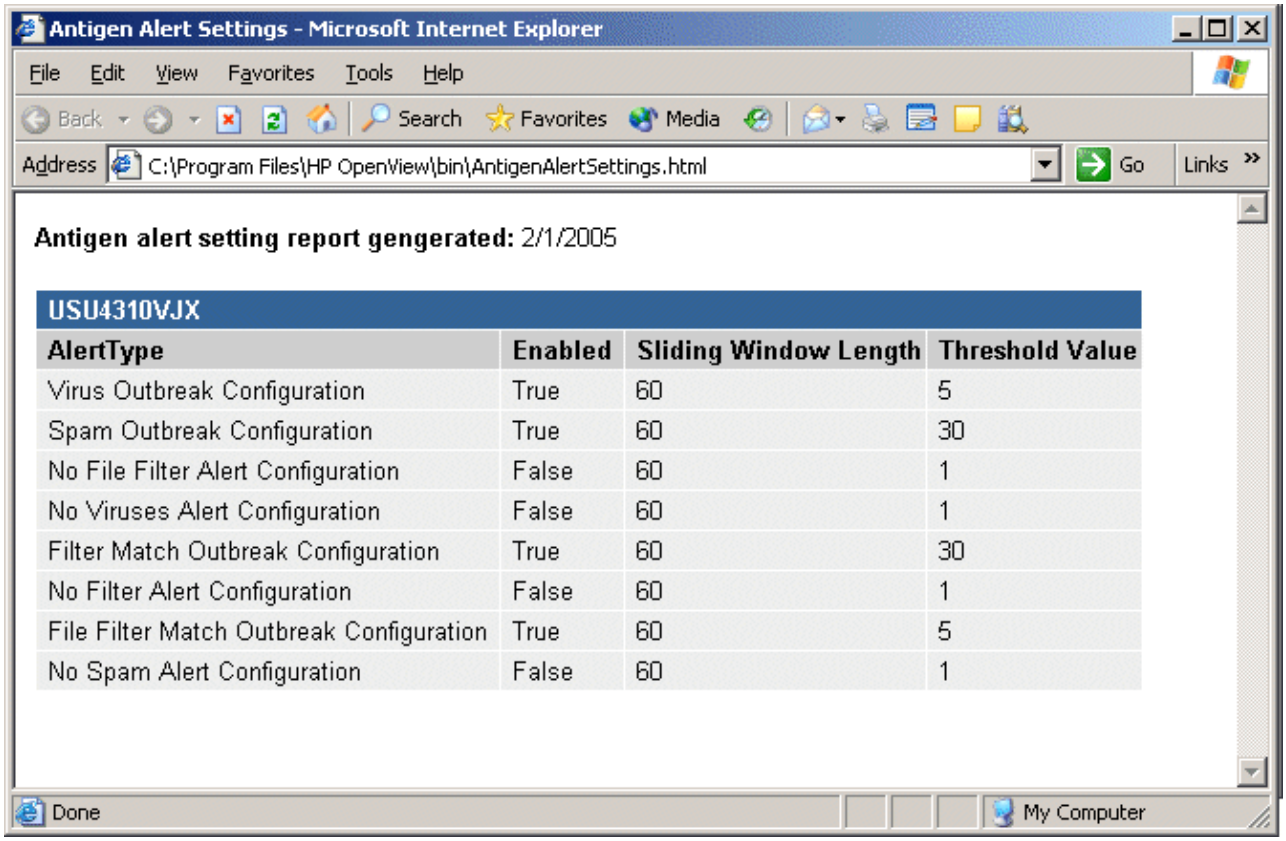
To work with any of the tools, double-click it and the *Edit Login And Parameters* dialog appears. Use it to select which servers the tool will apply to.



Select one or more servers to monitor, and then click Launch. If you have selected any tool other than Retrieve And View Alert Settings, the *Enter Alert Type(s)* dialog appears, allowing you to set or modify parameters. Retrieve And View Alert Settings shows you a report.

Retrieve And View Alert Settings

The Retrieve And View Alert Settings tool displays a report that shows you the current settings for one or more servers (the server name is USU4310VJX in the example). This is what the report looks like:



The report tool shows you, for each Alert Type, whether it's enabled or disabled, as well as its Sliding Window Length and its Threshold Value. This is what the various types and values mean:

Virus Outbreak Alerts
Notifies administrators of possible virus outbreaks.

Spam Outbreak Alerts
Notifies administrators of possible spam outbreaks/attacks.

Content Filter Match Alerts
Notifies administrators of unusually high or low content filtering activity (based on message counts).

File Filter Match Alerts
Notifies administrators of unusually high or low file filtering activity (based on file attachment counts).

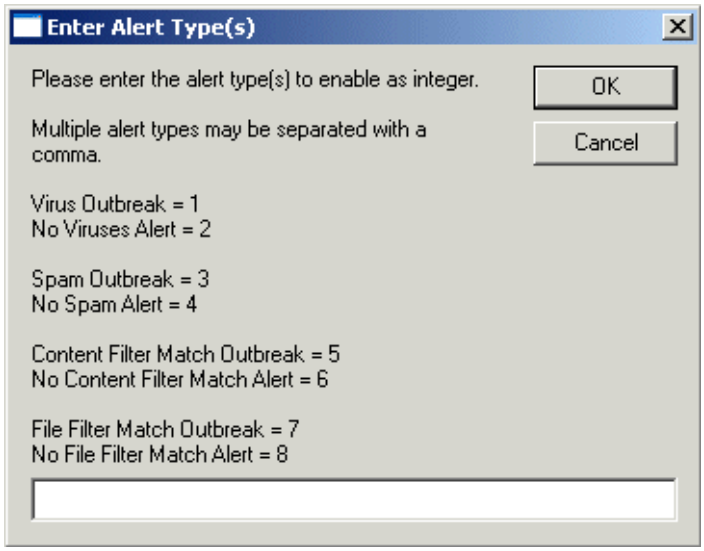
Enabled/Disabled
Indicates whether the Alert Type is enabled.

Sliding Window Length
Indicates the time frame (in minutes) during which the Threshold Value will be applied, in order to determine if there was a reportable outbreak.

Threshold Value
Indicates the minimum number of incidents that must be detected within the sliding window time frame, in order to trigger an alert to the Console.

Enter Alert Types Dialog

The *Enter Alert Type(s)* dialog allows you to set or modify the parameters for Alerts. Double-click any of the tools, other than Retrieve And View Alert Settings, to display it. They all work identically.



Select the events to trigger an alert and enter them as a comma-delimited list. For example, to enable Virus Outbreak, Spam Outbreak, and File Filter Match Outbreak, enter:

1,3,7

By using the "No *type* Alert" values (2, 4, 6, and 8), you can be alerted if you *don't* get a substantial number of these within the specified time span.

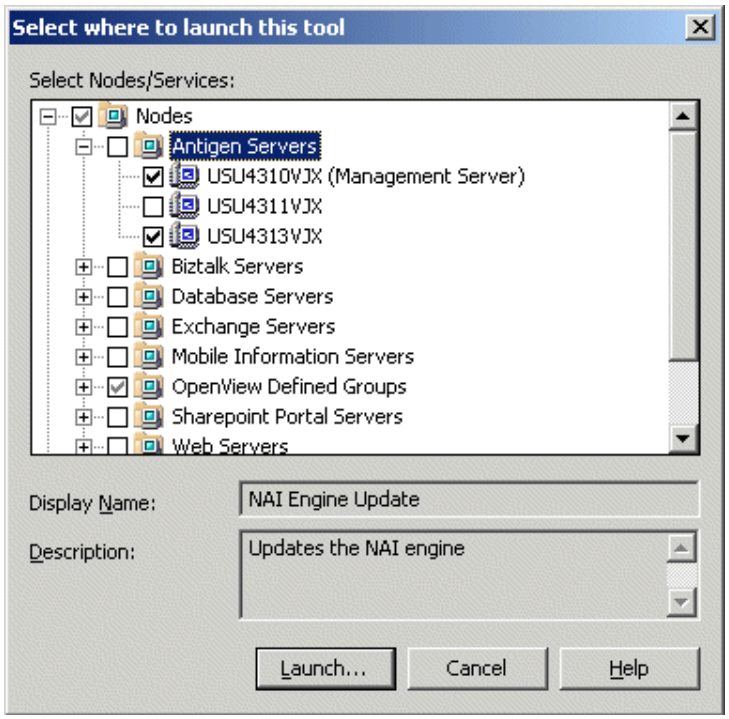
Please Note: The *Enter Alert Type(s)* dialog for Set Alert Threshold Value is slightly different in that there are no "No *type* Alert" choices.

Engine Updates

Use Engine Updates to update one or more scanning engines. Select the Engine Updates tool group for a list of all engine update tools.

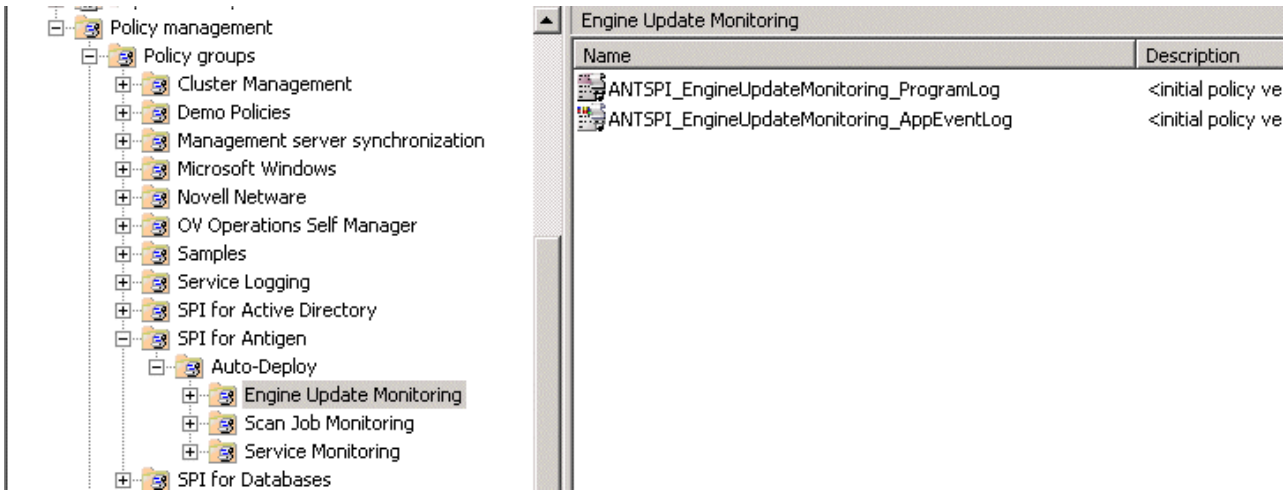
Please Note: All possible engines display. However, you may only update those for which you have a license.

Select an engine to be updated and double-click it. The *Select Where To Launch This Tool* dialog appears. Use it to select one or more servers to which the update should be applied.



Policy Management

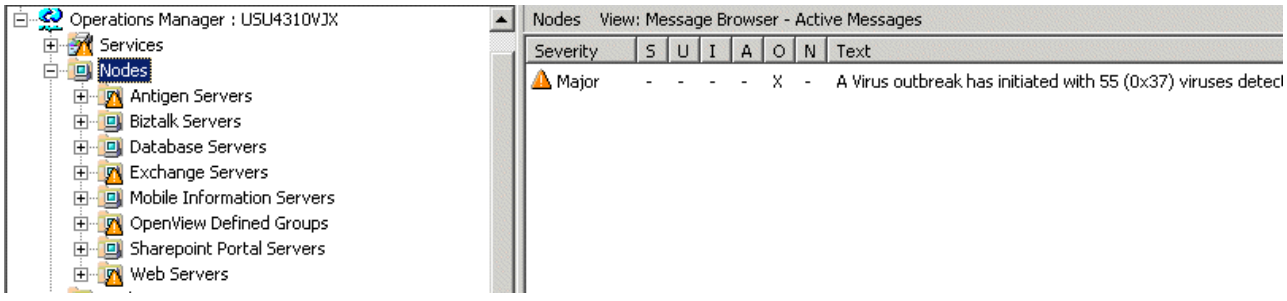
There are several groups of policies listed in the left pane. Selecting any one of them shows the individual policies in the right pane. You should not need to make any changes to any of them, since they are all configured to work with Antigen. Each of the rules is described in the “Policy Rules” appendix.



Viewing Alerts On The Console

The policies within the SPI For Antigen policy group are deployed to managed nodes, where they monitor various logs. If a log entry is found that matches a policy rule, an alert is sent to the OpenView Console.

The right pane displays the alert. You can double-click the explanation to display the *OpenView Message Properties* dialog, which contains more information. This is how the console looks when an alert is triggered:



Appendix A – Policy Rules

These are the various kinds of policy rules that are defined in HP OpenView For Antigen. These events are caught using the Event ID or Message text as listed in the Criteria section for each event

Exchange Scan Job Monitoring Events

Event Rule Name	ScanJobTerminatedA / ScanJobTerminatedB
Provider	Application Event Log
Criteria	Source = AntigenManual Event ID = 5012 or 5014
Alert Severity	Major
Description	The Manual Scan Job terminated before completion. Possibly caused by broken store database links to attachments or other store level corruption.
Event Rule Name	ScanManualEngineMapE
Provider	Application Event Log
Criteria	Log Text = “Realtime Scan Aborted”
Alert Severity	Warning
Description	Antigen Engine Mapper generated an error when trying to pass a scan task to the file scanner. The file scanner is damaged or inaccessible
Event Rule Name	ScanManualStarted
Provider	Application Event Log
Criteria	Source = AntigenManual Event ID = 2002
Alert Severity	Normal
Description	A manual scan job started execution.
Event Rule Name	ScanManualStopped
Provider	Application Event Log
Criteria	Source = AntigenManual Event ID = 2005
Alert Severity	Normal
Description	A manual scan job finished execution.

Event Rule Name	ScanRealtimeAbortE
Provider	Antigen ProgramLog
Criteria	Log Text = “Realtime Scan Aborted”
Alert Severity	Warning
Description	Realtime scan job aborted. Possibly due to a scanning timeout. Typically, recovery is automatic.
Event Rule Name	ScanRealtimeDisabled
Provider	Application Event Log
Criteria	Source = AntigenRealtime Event ID = 2001
Alert Severity	Normal
Description	Realtime scan job moved into a disabled state as a response to being disabled manually in the Antigen Client, or due to an AntigenStore service shutdown.
Event Rule Name	ScanRealtimeEnabled
Provider	Application Event Log
Criteria	Source = AntigenRealtime Event ID = 2000
Alert Severity	Normal
Description	A realtime scan job went into an enabled state on the system.
Event Rule Name	ScanRealtimeEngineMapE
Provider	Application Event Log
Criteria	Source = AntigenRealtime Event ID = 5030
Alert Severity	Critical Error
Description	Antigen Engine Mapper generated an error when trying to pass a scan task to the file scanner in the realtime scan job. The file scanner is damaged or inaccessible
Event Rule Name	ScanRealtimeTimeoutE
Provider	Antigen ProgramLog
Criteria	Log Text = “Realtime scan exceeded the allowed scan time limit”
Alert Severity	Warning
Description	Realtime scan job exceeded the specified time limit for a single scan task. The realtime scan job should be reinitialized automatically and continue to scan.

Event Rule Name	ScanUnapprovedVersionE
Provider	Application Event Log
Criteria	Source = AntigenStore Event ID = 4005
Alert Severity	Critical
Description	In ESE mode, Antigen has detected that the Exchange ESE interface is not a recognized version. Antigen has not integrated the ESE mode scanning interface, and no realtime scanning will occur.

Exchange Service Monitoring

Event Rule Name	ServicesAntigenStoreStartE
Provider	Application Event Log
Criteria	Source = AntigenStore Event ID = 1005
Alert Severity	Normal
Description	The AntigenStore service was successfully started.
Event Rule Name	ServicesAntigenStoreStartFailE
Provider	System Event Log
Criteria	Source = Service Control Manager Event ID = 7000 or 7001 Description = “The AntigenStore service”
Alert Severity	Critical
Description	The AntigenStore service failed to initialize and was not started. This could be due to a dependency service failure, or a corruption problem with service components.
Event Rule Name	ServicesAntigenStoreStopE
Provider	Application Event Log
Criteria	Source = AntigenStore Event ID = 1006
Alert Severity	Normal
Description	The AntigenStore service was stopped.
Event Rule Name	ServicesAntigenStoreTerminatedE
Provider	System Event Log
Criteria	Source = Service Control Manager Event ID = 7034 Description = “The AntigenStore service terminated”
Alert Severity	Critical
Description	The Service Control Manager determined that the Antigen Store service terminated unexpectedly.
Event Rule Name	ServicesSMTPStartE (Disabled by Default)
Provider	Application Event Log
Criteria	Source = MSExchangeTransport Event ID = 332
Alert Severity	Normal
Description	The Exchange SMTP transport came online. Basically this event is equivalent to the SMTP service starting. The SMTP service is monitored with a separate Event Rule.

Event Rule Name	ServicesSMTPStopE (Disabled by Default)
Provider	Application Event Log
Criteria	Source = MSExchangeTransport Event ID = 333
Alert Severity	Normal
Description	The Exchange SMTP transport went offline. Basically this event is equivalent to the SMTP service stopping. The SMTP service is monitored with a separate Event Rule.
Event Rule Name	ServicesStoreStartE
Provider	Application Event Log
Criteria	Source = AntigenMonitor Event ID = 1007
Alert Severity	Normal
Description	Antigen Monitor detected the Information Store service was started and has gone online.
Event Rule Name	ServicesStoreFailE
Provider	Application Event Log
Criteria	Source = AntigenMonitor Event ID = 1009
Alert Severity	Critical
Description	The AntigenMonitor detected that the Exchange Information Store service terminated unexpectedly.
Event Rule Name	ServicesStoreStopE
Provider	Application Event Log
Criteria	Source = AntigenMonitor Event ID = 1008
Alert Severity	Normal
Description	Antigen Monitor detected the Information Store service was successfully stopped and has gone offline.

Engine Update Monitoring

Event Rule Name	UpdateFailConnection
Provider	Application Event Log
Criteria	Source = GetEngineFiles Event ID = 6059
Alert Severity	Major
Description	Engine update failed because a network connection to the update source server failed or connection was denied by the update source server.
Event Rule Name	UpdateFailCRC
Provider	Application Event Log
Criteria	Source = GetEngineFiles Event ID = 6010
Alert Severity	Major
Description	The CRC check performed on the newly downloaded engine file (engine.syb) failed. The engine file is corrupt or invalid.
Event Rule Name	UpdateFailDisable
Provider	Application Event Log
Criteria	Source = GetEngineFiles Event ID = 6012
Alert Severity	Critical
Description	Engine update failed because Antigen was unable to unload the scan engines from the running scan jobs. This error actually indicates something more serious then just an engine update problem. It indicates that a scan job is in a malfunctioning or error state.
Event Rule Name	UpdateFailEnable
Provider	Application Event Log
Criteria	Source = GetEngineFiles Event ID = 6015
Alert Severity	Critical
Description	Engine Update failed because Antigen was unable to reload the scan engines into scan jobs. This error actually indicates something more serious then just an engine update problem. It indicates that a scan job is in a malfunctioning or error state.

Event Rule Name	UpdateFailFTPPath
Provider	Application Event Log
Criteria	Source = GetEngineFiles Event ID = 6008
Alert Severity	Major
Description	The engine update failed because the specified FTP path to the engine update server was invalid.
Event Rule Name	UpdateFailGeneric
Provider	Application Event Log
Criteria	Source = GetEngineFiles Event ID = 6014
Alert Severity	Major
Description	A generic engine update failure occurred. This event will typically be accompanied by other, more specific, update failure events that will help identify the cause of the failure.
Event Rule Name	UpdateFailHTTPPath
Provider	Application Event Log
Criteria	Source = GetEngineFiles Event ID = 6063
Alert Severity	Major
Description	The engine update failed because the specified HTTP path to the engine update server was invalid.
Event Rule Name	UpdateFailLocked
Provider	Antigen ProgramLog
Criteria	Log Text = “ERROR: File is in use or has read-only attribute”
Alert Severity	Minor
Description	The scan engine update failed because a file in the current engine folders is locked or its read-only attribute is set.
Event Rule Name	UpdateFailLocked_8.1
Provider	Antigen ProgramLog
Criteria	Log Text = “ERROR: Could not delete directory”
Alert Severity	Minor
Description	The scan engine update failed because a file in the current engine folders is locked or its read-only attribute is set.
Event Rule Name	UpdateFailTimeout
Provider	Antigen ProgramLog
Criteria	Log Text = “GetEngineFiles Timed Out”
Alert Severity	Minor
Description	Engine Update process timed out while attempting to download the engine update package. The download task was aborted.

Event Rule Name	UpdateFailUNCPath
Provider	Application Event Log
Criteria	Source = GetEngineFiles Event ID = 6009
Alert Severity	Major
Description	The engine update failed because the specified UNC path to the engine update server was invalid.
Event Rule Name	UpdateFileUpdateIni
Provider	Application Event Log
Criteria	Source = GetEngineFiles Event ID = 2030 or 2032
Alert Severity	Major
Description	Engine Update process was unable to retrieve the "Update.ini" file from the specified engine update source server. This issue is often related to Internet proxy configuration issues or firewall restrictions.
Event Rule Name	UpdateRollbackFail
Provider	Application Event Log
Criteria	Source = GetEngineFiles Event ID = 2017 or 6016
Alert Severity	Minor
Description	The scan engine that just updated automatically rolled back to the previous engine definition version. A rollback occurs if the newly updated engine generates an error on attempting its first scan task.
Event Rule Name	UpdateSuccessful
Provider	Application Event Log
Criteria	Source = GetEngineFiles Event ID = 2014 or 2016
Alert Severity	Normal
Description	Successful scan engine update completed.
Event Rule Name	EngineUpdateFailures_8_1
Provider	Application Event Log
Criteria	Source = GetEngineFiles Event ID = 100
Alert Severity	Minor
Description	Download of engine update files failed
Event Rule Name	CreateSYBFail
Provider	ProgramLog
Criteria	Log Text = "ERROR: Could not create the syb package"
Alert Severity	Minor
Description	Antigen was unable to create an engine update .syb package from the incremental files.

Event Rule Name	IncrDlFailedPrimary
Provider	ProgramLog
Criteria	Log Text = “ERROR: Downloading <*> incremental files with primary path failed. Attempting download with secondary path.”
Alert Severity	Minor
Description	Antigen failed to download Incremental update files from the primary update path.

Event Rule Name	IncrDlFailedPrimary
Provider	ProgramLog
Criteria	Log Text = “ERROR: Downloading <*> incremental files with primary path failed. Attempting download with secondary path.”
Alert Severity	Minor
Description	Antigen failed to download Incremental update files from the primary update path.

Event Rule Name	DlINIFailedPrimary
Provider	ProgramLog
Criteria	Log Text = “ERROR: Downloading the <*> update.ini with primary path failed. Attempting download with secondart path.”
Alert Severity	Minor
Description	Antigen failed to download update.ini from the primary download path.

Event Rule Name	DlINIFailedSecondary
Provider	ProgramLog
Criteria	Log Text = “ERROR: Downloading the <*> update.ini with secondary path failed. Attempting download with secondart path.”
Alert Severity	Minor
Description	Antigen failed to download update.ini from the secondary download path.

Scan Job Monitoring

Event Rule Name	GetScanEnabledError
Provider	Antigen ProgramLog
Criteria	Log Text = “ERROR: Problems retrieving appropriate index from GetScanEnabled”
Alert Severity	Major
Description	Antigen was unable to retrieve the index associated with a storage group for a scan job.
Event Rule Name	ScanConfigDataAccess
Provider	Antigen ProgramLog
Criteria	Log Text = “ERROR: The call to StgOpenStorage”
Alert Severity	Critical
Description	Antigen was unable to retrieve scan job configuration information during Antigen initialization. An Antigen data file (ADB file) may have become corrupt or inaccessible.
Event Rule Name	ScanInternalError
Provider	Antigen Programlog
Criteria	Log Text = “ERROR: Internal error”
Alert Severity	Critical
Description	An internal error occurred in the Antigen software. This can be caused by a number of issues including: system, executable file, data file or registry problems. Typically it would indicate a loss of critical functionality.
Event Rule Name	ScanInternetAbort
Provider	Antigen ProgramLog
Criteria	Log Text = “Internet scan abort”
Alert Severity	Warning
Description	The Internet Scan Job aborted execution. This could occur due to a scanning timeout. Recovery should be automatic.
Event Rule Name	ScanInternetDisabled
Provider	Application Event Log
Criteria	Source = AntigenInternet Event ID = 2008
Alert Severity	Normal
Description	The Internet Scan Job has gone into a disabled state. This occurs when the Internet Scan Job is disabled in the Antigen Client manually or when the AntigenIMC service is shutdown.

Event Rule Name	ScanInternetEnabled
Provider	Application Event Log
Criteria	Source = AntigenInternet Event ID = 2007
Alert Severity	Normal
Description	The Internet Scan Job has gone into an enabled state. This occurs when the Internet Scan Job is enabled manually in the Antigen Client or when the AntigenIMC service and SMTP services are started.
Event Rule Name	ScanInternetEngineMap
Provider	Application Event Log
Criteria	Source = AntigenInternet Event ID = 5030
Alert Severity	Major
Description	An attempt to pass a scan task, on the Internet Scan Job, to a specific scan engine fails. It indicates that the scan engine is damaged or inaccessible.
Event Rule Name	ScanInternetInternalError
Provider	Application Event Log
Criteria	Source = ScanInternetSink Event ID = 4007
Alert Severity	Critical
Description	An internal error on the SMTP sink occurred.
Event Rule Name	ScanInternetSink
Provider	Application Event Log
Criteria	Source = AntigenSMTPSink Event ID = 4008
Alert Severity	Major
Description	An SMTP Sink error was registered by Antigen. This will occur when Antigen is unable to access message objects in the SMTP Queue. This may indicate a temporary resource problem on the system.
Event Rule Name	ScanInternetTimeout
Provider	Antigen ProgramLog
Criteria	Log Text = “A scanning thread has been terminated and restarted”
Alert Severity	Warning
Description	Internet Scan Job exceeded the specified time limit for a single scan task. The Internet Scan Job should be automatically reinitialized and continue to scan.

Event Rule Name	ScanManualPaused
Provider	Application Event Log
Criteria	Event ID = 2003
Alert Severity	Normal
Description	A manual scan job was paused.
Event Rule Name	ScanManualRestart
Provider	Application Event Log
Criteria	Event ID = 2006
Alert Severity	Normal
Description	A manual scan job was restarted.
Event Rule Name	ScanManualResumed
Provider	Application Event Log
Criteria	Event ID = 2004
Alert Severity	Normal
Description	A manual scan job was resumed after a pause
Event Rule Name	ScanManualStarted
Provider	Application Event Log
Criteria	Event ID = 2002
Alert Severity	Normal
Description	A manual scan job has started
Event Rule Name	ScanManualStopped
Provider	Application Event Log
Criteria	Event ID = 2005
Alert Severity	Normal
Description	A manual scan job was stopped
Event Rule Name	ScanRealtimeDisabled
Provider	Application Event Log
Criteria	Event ID = 2001
Alert Severity	Normal
Description	The Realtime Scan Job has gone into a disabled state.
Event Rule Name	ScanRealtimeEnabled
Provider	Application Event Log
Criteria	Event ID = 2000
Alert Severity	Normal
Description	The Realtime Scan Job has gone into an enabled state.

Service Monitoring

Event Rule Name	ServicesAntigenIMCStart
Provider	Application Event Log
Criteria	Source = AntigenIMC Event ID = 1002
Alert Severity	Normal
Description	The AntigenIMC service was started successfully.
Event Rule Name	ServicesAntigenIMCSFail
Provider	System Event Log
Criteria	Source = Service Control Manager Event ID = 7000 or 7001 Description = “The AntigenIMC service”
Alert Severity	Critical
Description	The AntigenIMC service failed to start. Possible causes could be file, data, or registry corruption, or failure of a dependency service.
Event Rule Name	ServicesAntigenIMCStop
Provider	Application Event Log
Criteria	Source = AntigenIMC Event ID = 1003
Alert Severity	Normal
Description	The AntigenIMC service was stopped.
Event Rule Name	ServicesAntigenIMCTerminate
Provider	System Event Log
Criteria	Source = Service Control Manager Event ID = 7034 Description = “The AntigenIMC service terminated unexpectedly”
Alert Severity	Critical
Description	The AntigenIMC service terminated unexpectedly. Possible causes could be an application exception in the AntigenIMC process or the AntigenIMC process was killed.
Event Rule Name	ServicesSMTPStarted
Provider	System Event Log
Criteria	Source = Service Control Manager Event ID = 7036
Alert Severity	Normal
Description	The SMTP service was started successfully.

Event Rule Name	ServicesSMTPStartFail
Provider	System Event Log
Criteria	Source = Service Control Manager Event ID = 7000 or 7001 Description = “The Simple Mail Transfer Protocol (SMTP) service”
Alert Severity	Critical
Description	The SMTP service failed to start. Possible causes could be file, data, or registry corruption or failure of a dependency service.
Event Rule Name	ServicesSMTPStart
Provider	Application Event Log
Criteria	Event ID = 7035
Alert Severity	Normal
Description	The SMTP service was sent a start control.
Event Rule Name	ServicesSMTPStop
Provider	Application Event Log
Criteria	Event ID = 7035
Alert Severity	Normal
Description	The SMTP service was sent a stop control.
Event Rule Name	ServicesSMTPStopped
Provider	System Event Log
Criteria	Source = Services Control Manager Event ID = 7036
Alert Severity	Normal
Description	The SMTP service was stopped.
Event Rule Name	ServicesSMTPTerminate
Provider	Antigen Programlog
Criteria	Log Text = “ERROR: Antigen Monitor detected abnormal INETINFO shutdown”
Alert Severity	Critical
Description	Antigen Monitor detected the INETINFO process unexpectedly stopped execution. The SMTP Service will stop functioning.

Index