HP OpenView SPI for Select Access 6.0

Integration Guide

For Microsoft Windows Operating Systems

February 2004

Legal Notices

Warranty

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

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices

Trademark Notices

OpenView® and Select Access® are trademarks of Hewlett-Packard Development Company, L.P.

Microsoft®, Windows NT®, Windows 2000®, Windows 2003®, and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

All other product names are the property of their respective trademark or service mark holders and are hereby acknowledged.

Support

Please visit the HP OpenView web site at:

http://openview.hp.com/

and also the HP OpenView Select Access web site at:

http://openview.hp.com/products/select/

There you will find contact information and details about the products, services, and support that HP OpenView offers, as well as product-specific information on HP OpenView Select Access.

You can go directly to the HP OpenView support web site at:

http://support.openview.hp.com/

The support site includes:

- Downloadable documentation
- Troubleshooting information
- Patches and updates
- Problem reporting
- Training information
- Support program information

Contents

The SASPI Integration Guide 7

Introduction 7

Audience 7

Chapters Summary 7

SASPI Concepts 9

Introducing the SMART Plug In for Select Access 9

How the SASPI Works 9

SASPI Components 11

Users and User Profiles 11

Message Group 11

Node Groups 11

Tools 12

Policy Groups 12

Policies 14

Service Views 15

Installing SASPI 17

Supported Software 17

Management Server Requirements 17

Managed Node Requirements 17

SASPI Installation 18

SASPI Removal 20

Removing Policies from all Managed Nodes 21

Removing the Policy Group from the Management Server 22

Removing the User Role 23

Removing the Tool Folders 24

Removing the Node Groups 25
Removing the Services 25
Removing the Software.. 25

Using & Customizing SASPI 27

Adding Nodes to Node Groups 27

Configuring SASPI Operators 27

Using SASPI Tools.. 28

Configuring SASPI Fault Monitoring.. 28

Configuring SASPI Availability Monitoring.. 30

Configuring SASPI Performance Monitoring 30

Customizing the SASPI Service View 31

1

The SASPI Integration Guide

Introduction

The SASPI Integration Guide describes how to install and configure the HP OpenView SPI for Select Access.

For information about Select Access, see the `\docs\PolicyBuilder\policy_builder_guide.pdf` on your Select Access CD or visit the Select Access website at: http://www.openview.hp.com/products/select/

Audience

This document is intended for administrators of OpenView Operations supporting a Select Access environment.

Chapters Summary

- Chapter 1 – The SASPI Integration Guide, describes the intent of the guide and its structure.
- Chapter 2 – SASPI Concepts, provides an overview of the SPI functionality, and a description of its components.
- Chapter 3 – Installing SASPI, lists the prerequisites, installation, and removal procedures for the SPI.
- Chapter 4 – Using and Customizing SASPI, covers the deployment and customization of the SPI.

2

SASPI Concepts

Introducing the SMART Plug In for Select Access

The Smart Plug In for Select Access (SASPI) adds monitoring capabilities to HP OpenView Operations for Windows (OVOW) to help you monitor and manage Select Access environments. The SASPI covers the monitoring of faults, service availability, and performance of Select Access components. Service Views provide root-cause analysis of all the reported alarms and integrated applications help to administer the Select Access services and troubleshoot problems.

From the OVOW console, you can apply the same familiar HP OpenView problem-managing processes to monitor a Select Access environment. This reduces the time to isolate and repair problems in Select Access service.

How the SASPI Works

The SASPI provides pre-configured policies that, when deployed, track events that occur in Select Access components. These events appear as messages in the OVOW Message Browser and Service View, and help you proactively address potential or existing problems and avoid serious disruptions to Select Access services.

The SASPI also monitors the availability and performance of Select Access components. Figure 1 illustrates the interaction between SASPI and Select Access components. (The purple boxes represent possible Select Access components in an environment, while the blue circles represent the OVO agents that would be installed on each computer.)

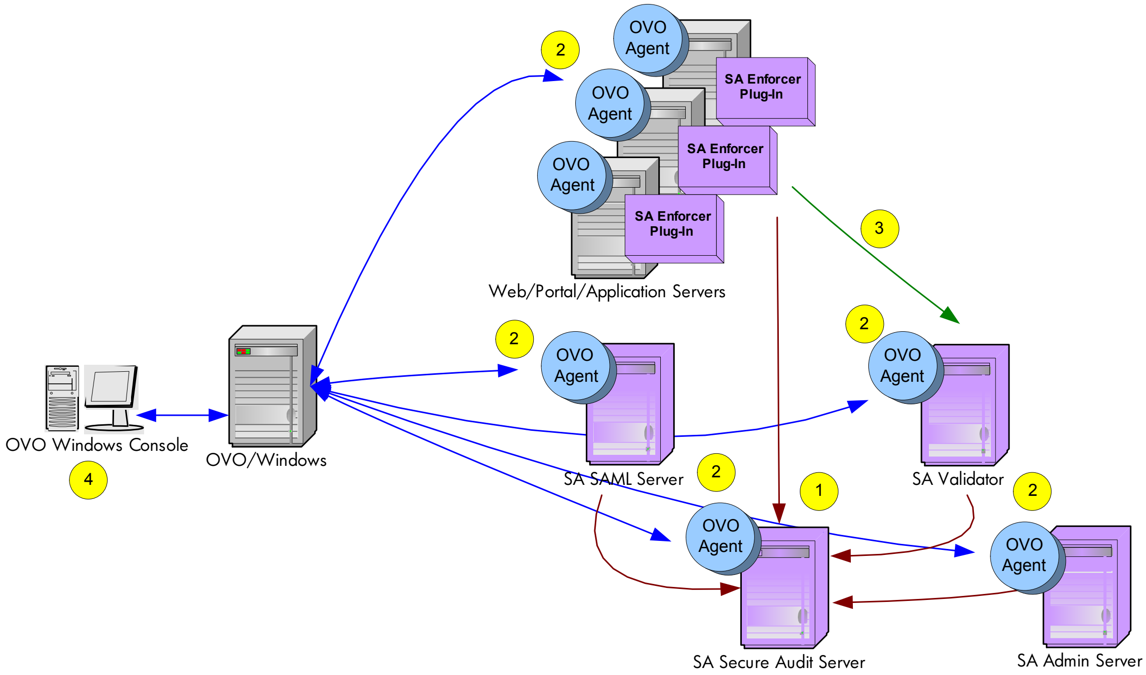


Figure 2-1: System Overview of OVOW and Select Access

1 All Select Access components will be configured to forward event data to a log file on the Secure Audit Server. This log file is monitored by the OVO agent looking for errors. These errors are then filtered and subsequently forwarded to the OVOW management server. Sending all messages to the Secure Audit Server allows the SASPI to report on problems that occurred on platforms not currently supported by the SASPI (e.g., HP-UX, Linux).

2 The SASPI monitors the availability of Select Access services on all supported nodes. The SASPI also includes operator applications to start, stop, and get status on the Select Access services.

3 The SASPI monitors the performance of the authentication and authorization process. By running a test query to the Validator from the systems with the Enforcer plug ins installed, the performance of the authentication and authorization process is isolated and compared against a threshold of an acceptable response time. This performance monitoring works well in combination with monitoring of the general Website performance since it is a component of the overall response time.

4 Messages from the SASPI are displayed in the OVOW console where they are mapped to a service view representing the Select Access service.

For the first release of SASPI, only the OVO Windows management platform and Microsoft Windows agent platforms will be supported. Further platform support will come in subsequent releases. For more information on installation requirements, see Supported Software.

SASPI Components

Users and User Profiles

The installation of the SASPI software adds a new user profile to OVOW. The OVOW administrator uses user profiles to simplify the process of assigning responsibilities to new OVOW users. The SASPI user profile is called **Select Access** and has visibility to all SASPI messages and tools.

Message Group

The SASPI installs a new message group that is specifically designed to handle messages generated by the policies and monitors started by the SASPI. This message group is called **Select Access**.

The Select Access message group is assigned by default to the Select Access user profile, which is uploaded to OVOW during the installation of the SASPI. This means that assigning the Select Access user profile to an OVOW user ensures that this user receives SASPI messages automatically, assuming the appropriate node groups are assigned.

Node Groups

While installing the SASPI, a number of new SASPI-specific node groups are added to OVOW. These node groups allow you to monitor the following components:

Select Access: A top-level node group that contains the other SASPI node groups.

SA Admin Server: Contains the nodes running the Select Access Administration Server component that you want to monitor with the SASPI.

SA Validator: Contains the nodes running the Select Access Validator component that you want to monitor with the SASPI.

SA Enforcer: Contains the nodes running any of the Select Access Enforcer plug in components that you want to monitor with the SASPI.

SA SAML: Contains the nodes running the Select Access SAML Server component that you want to monitor with the SASPI.

SA SAS: Contains the nodes running the Select Access Secure Audit Server component that you want to monitor with the SASPI.

The node groups themselves are empty on installation. During the configuration of the SASPI, you will have to assign nodes to the node group based on the Select Access component running on the node. Auto-deployment in OVOW (which is active by default) deploys the policies assigned to the node group automatically when a node is added to that node group. Note that the SASPI node groups are assigned to the Select Access user profile. This means that OVOW users to whom you assign the Select Access user profile will automatically receive messages from all those nodes included in the SASPI node groups.

Tools

The installation of the SASPI adds new tools to OVOW. The new tool group is called **SPI for Select Access** and contains four tool sub-groups. Each one of these sub-groups contains tools to start, stop, and check the status of a particular Select Access service. The following table describes the sub-groups and their tools:

Table 2-1: SASPI Tool Sub-Groups

SASPI Tool Sub-Group	Description
SASPI-Validator	Contains the applications Start Validator, Stop Validator, and Status Validator to control the Validator service
SASPI-AdminSrv	Contains the applications Start Admin Server, Stop Admin Server, and Status Admin Server to control the Administration Server service.
SASPI-AuditSrv	Contains the applications Start Audit Server, Stop Audit Server, and Status Audit Server to control the Secure Audit Server service.
SASPI-SAMLSrv	Contains the applications Start SAML Server, Stop SAML Server, and Status SAML Server to control the SAML Server service.

There are no applications for controlling the Enforcer plug ins because these plug ins are integrated into the Web or application servers. Tools to start and stop these components should be covered by a Web server or application server SPI.

Policy Groups

The installation of the SASPI creates four new policy groups in the OVOW database. The policy groups are assigned automatically to the corresponding high-level SASPI node groups to make policy assignment and distribution easier.

The top-level policy group is called **SPI for Select Access**. The following table lists the policy sub-groups and gives a short description of what they do.

Table 2-2: Policy Groups

Policy Group	Description
SASPI-Internal Errors	Contains policies that are used to monitor errors encountered by the SASPI itself (e.g., monitor script errors).

Policy Group	Description
SASPI-FaultMon	Contains policies to monitor the Select Access audit log.
SASPI-PerfMon	Contains policies used to monitor the performance of the Validator from the perspective of the Enforcer plug ins.
SASPI-AvailMon	Contains sub-policy groups and policies used to monitor the availability of the Select Access services. There are four sub-policy groups in this policy group: SASPI-Validator, SASPI-AdminSrv, SAPSI-SAMLSrv, and SASPI-AuditSrv. These sub-policy groups are named after the Select Access component that they monitor. Note: There is no availability monitoring for the Enforcer plug in because these plug-ins are integrated into a Web or application server. Availability of this component should be covered by a Web server or application server SPI.

Policy groups are assigned to node groups as an easy way to administer instrumentation on a managed node. When a managed node is added to a node group, it automatically gets assigned the policy groups that are designed for that class of node. The following table shows the mapping of node groups to policy groups in the SASPI.

Table 2-3: Node Group Mapping

SASPI Node Group	SASPI Assigned Policy Groups
SA Admin Server	*Policy Groups*- SASPI-Internal Errors, SASPI-AdminSrv
SA Validator	*Policy Groups*- SASPI-Validator, SASPI- Internal Errors
SA Enforcer	*Policy Groups*- SASPI-PerfMon, SASPI- Internal Errors
SA SAML Server	*Policy Groups*- SASPI-SAMLSrv, SASPI- Internal Errors
SA SAS	*Policy Groups*- SASPI-AuditSrv, SASPI-FaultMon, SASPI- Internal Errors

Policies

The policies provided with the SASPI are split into the following generic areas:

- Log file policies
- Availability policies
- Performance policies
- Self-management policies

These policies can be customized for your particular Select Access environment. For more information, see Configuring SASPI Fault Monitoring, Configuring SASPI Availability Monitoring, and Configuring SASPI Performance Monitoring.

The following tables describe the policies in SASPI.

Table 2-4: SASPI Log File Policy

Policy Name	Description	Polling Interval
SASPI-AuditLogs	Captures FATAL, ERROR, and WARNING messages from the audit file.	5m

Table 2-5: SASPI Availability Policies

Policy Name	Description	Polling Interval
SASPI_ProcMon_Validator	Monitors Select Access Validator service.	5m
SASPI_ProcMon_AdminSrv	Monitors Select Access Administration Server service.	5m
SASPI_ProcMon_SAMLSrv	Monitors Select Access SAML Server service.	5m
SASPI_ProcMon_AuditSrv	Monitors Select Access Secure Audit Server service.	5m

Table 2-6: SASPI Performance Policies

Policy Name	Description	Polling Interval
SASPI_PerfMon	Monitors the performance of Select Access Validator from the perspective of the Enforcer plug ins.	5m

Table 2-7: SASPI Self-Management Policies

Policy Name	Description	Polling Interval
SASPI-Internal Errors	Captures errors reported in the operation of the SASPI.	N/A

Service Views

During SASPI installation, a Select Access service view is added into the OVOW service tree. A service view is a representation of a service and the technology components that make up that service. It is a collection of managed elements grouped according to functional, logical, business, or other dependencies. The result is a tree-shaped view, where the top-level service (the root) is placed on top and branches representing sub-services extend from the top-level service. Each sub-service can again be divided into further sub-services.

The SASPI service view gives the operator an overview of the status of the Select Access components. Figure 2.2 is the default service view that is part of SASPI. The view focuses on Select Access components and their health. For information on modifying the service view, see Customizing the SASPI Service View

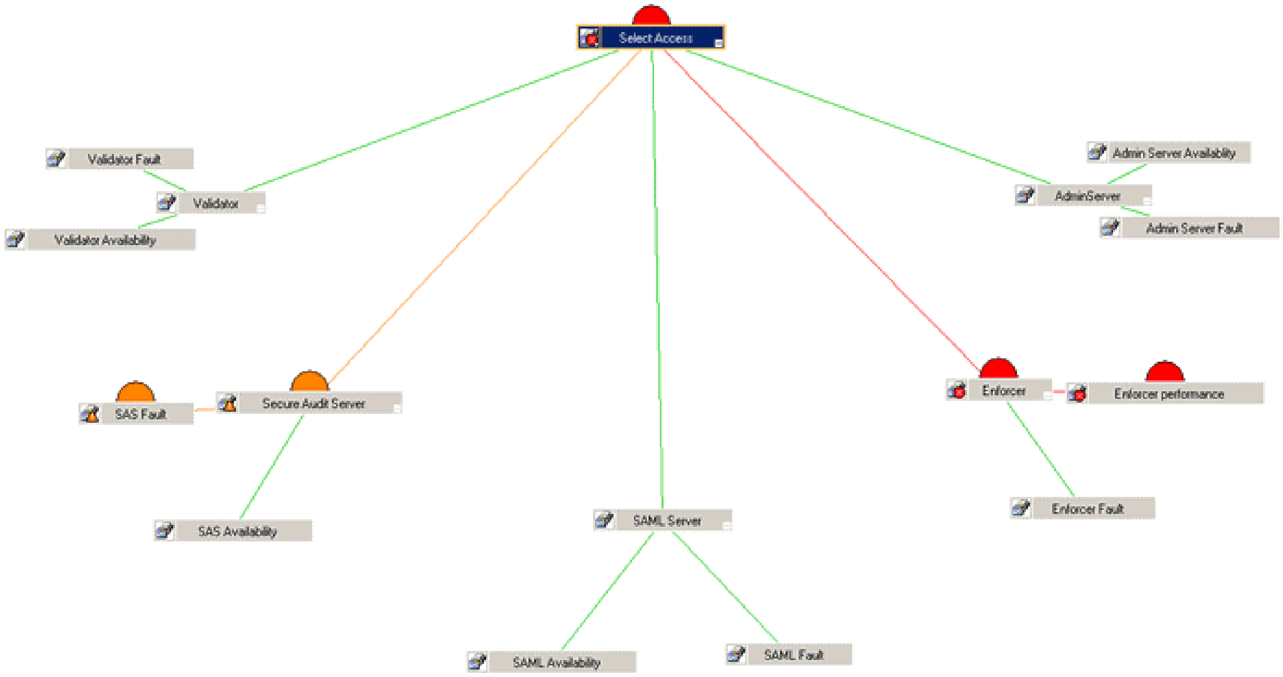


Figure 2-2: Default Service View

The top-level service is **Select Access** with each first sub-service representing the different classes of Select Access components (e.g., Validator, Enforcer, etc.). Each component sub-service has another level of sub-services where the SASPI messages received by OVOW are mapped.

3

Installing SASPI

Before using the Smart Plug In for Select Access, you must meet the software and hardware requirements for the management server and managed nodes, as listed below.

Supported Software

Management Server Requirements

Management Software Version	Management Platform
OVO for Windows 7.2x	Windows 2000 and Windows 2003

➤ Although not officially tested, the SASPI should work with OVO for Windows 7.1.

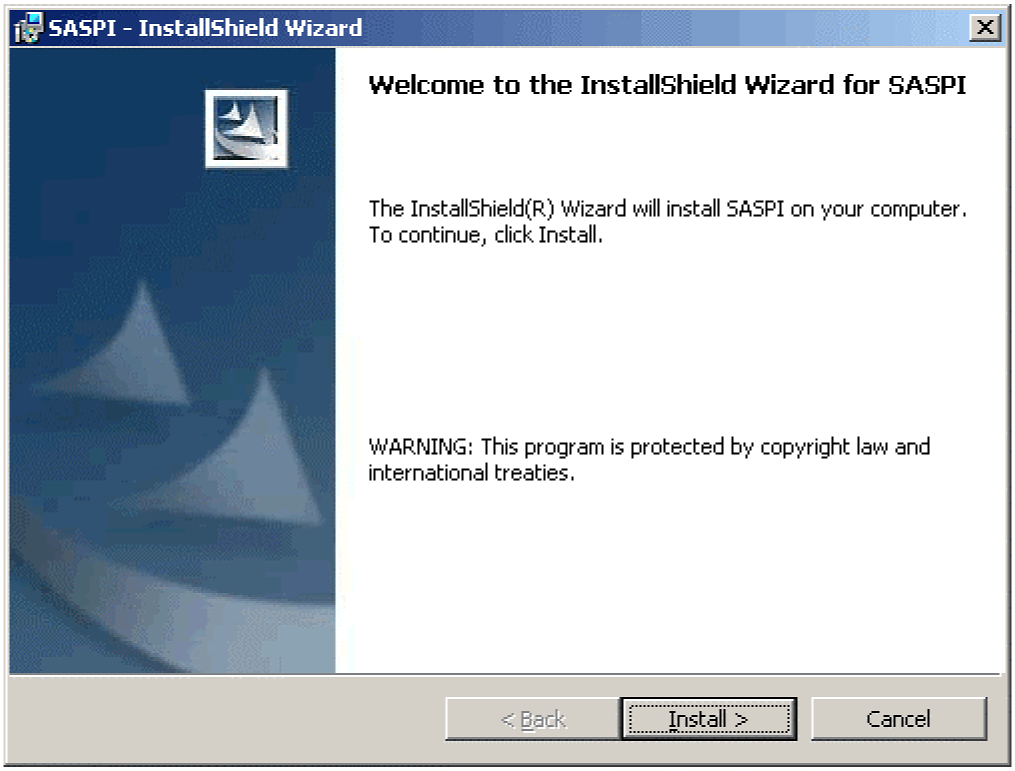
Managed Node Requirements

Select Access Component	Managed Platform
Select Access 6.0 Validator, Administration Server, SAML Server, and Secure Audit Server	Windows 2000 and Windows 2003
Select Access 6.0 IIS Enforcer plug in	Windows 2000 and Windows 2003

Although not officially tested, the SASPI should be able to monitor faults from Select Access components running on Linux, Solaris, and HP-UX platforms, if they are configured to send fault information to the Secure Audit Server running on a Windows platform with the log file policy installed.

SASPI Installation

1. Insert the OV Select Access installation media into the CD drive of the OVOW management server
2. On the media, look for **SASPI-1.00.msi**. This is the installation package for the SPI for Select Access.
3. Start this program and you will see the following Welcome screen. Click **Install** in the Welcome screen to start the installation.



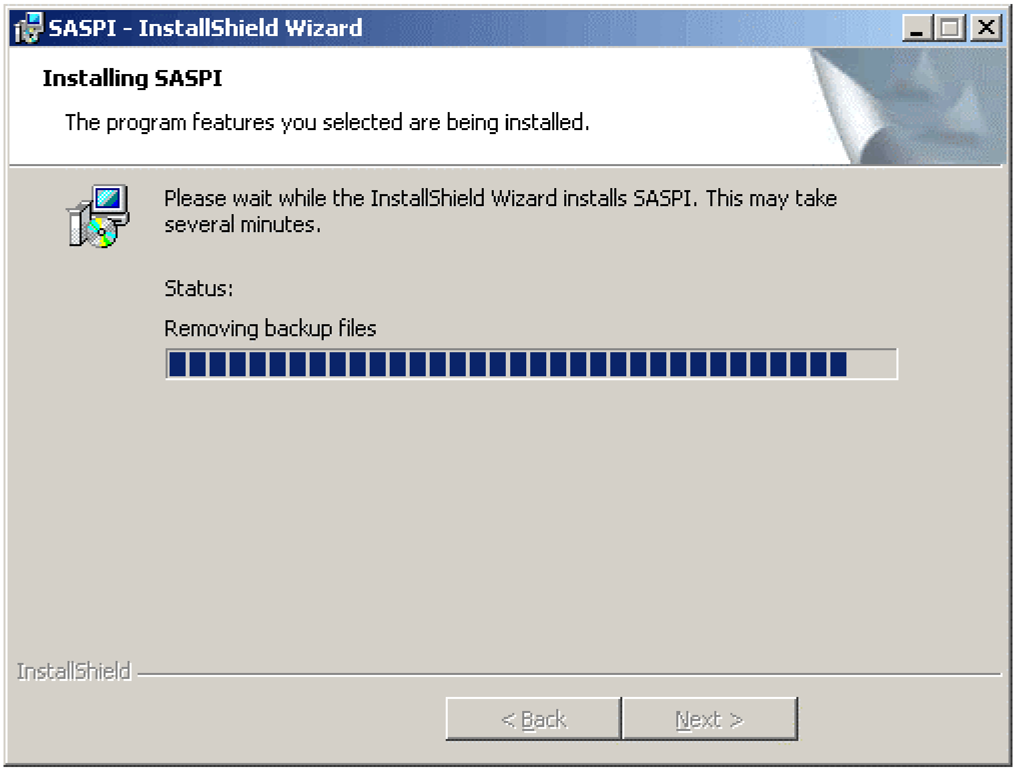
Welcome to the InstallShield Wizard for SASPI

The InstallShield(R) Wizard will install SASPI on your computer. To continue, click Install.

WARNING: This program is protected by copyright law and international treaties.

Figure 3-1: Welcome Screen

After clicking **Install**, you will see various status dialogs, like the example below, as the install program proceeds. This process should take less than a few minutes.



Installing SASPI

The program features you selected are being installed.

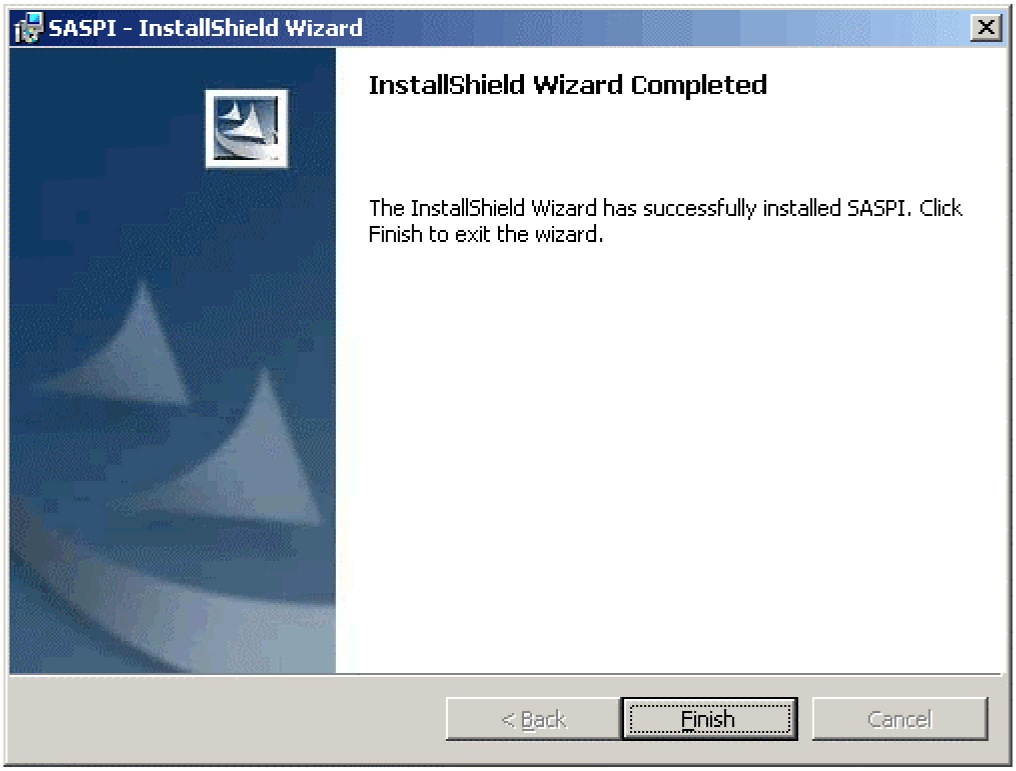
Please wait while the InstallShield Wizard installs SASPI. This may take several minutes.

Status:

Removing backup files

Figure 3-2: Installation Screen

The installation is finished when the completion screen displays “ Click **Finish** to conclude the installation.”



InstallShield Wizard Completed

The InstallShield Wizard has successfully installed SASPI. Click Finish to exit the wizard.

Figure 3-3: Installation Completed Screen

SASPI Removal

The removal of the SASPI occurs in **7** consecutive stages:

1. Removing the SASPI policies from all managed nodes
2. Removing the SASPI policy group from the management server
3. Removing the SASPI User Role
4. Removing the SASPI Tool Folders
5. Removing the SASPI Node Groups
6. Removing the SASPI Services
7. Removing the SASPI software

Removing Policies from all Managed Nodes

1. At the management console, expand the folder **Policy Management ->Policy Groups.**
2. Right-click **SPI for Select Access** and select **All tasks->Uninstall from....**
3. In the **Uninstall from...** window, select each check box next to the node(s) from which policies should be removed.
4. Click **OK**.

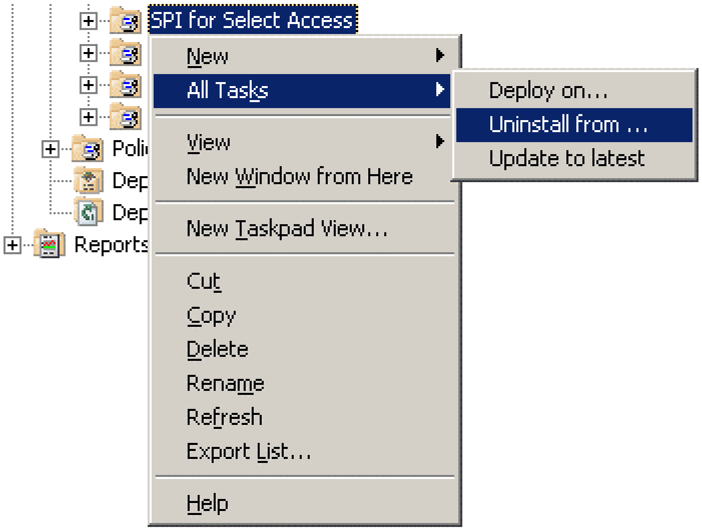


Figure 3-4: Removing Policies

Removing the Policy Group from the Management Server

1. In the console expand the folder **Policy Management ->Policy Groups.**
2. Right-click **SPI for Select Access** and select **Delete**.

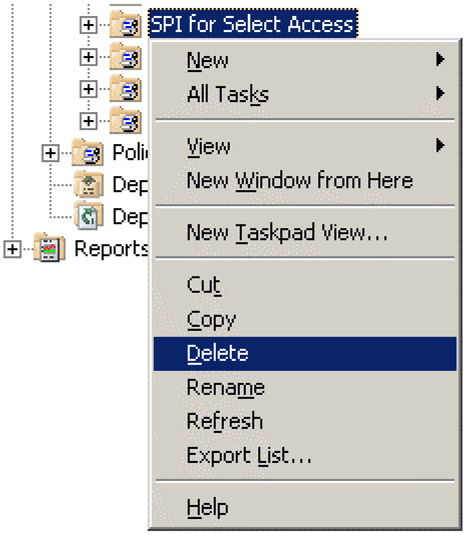
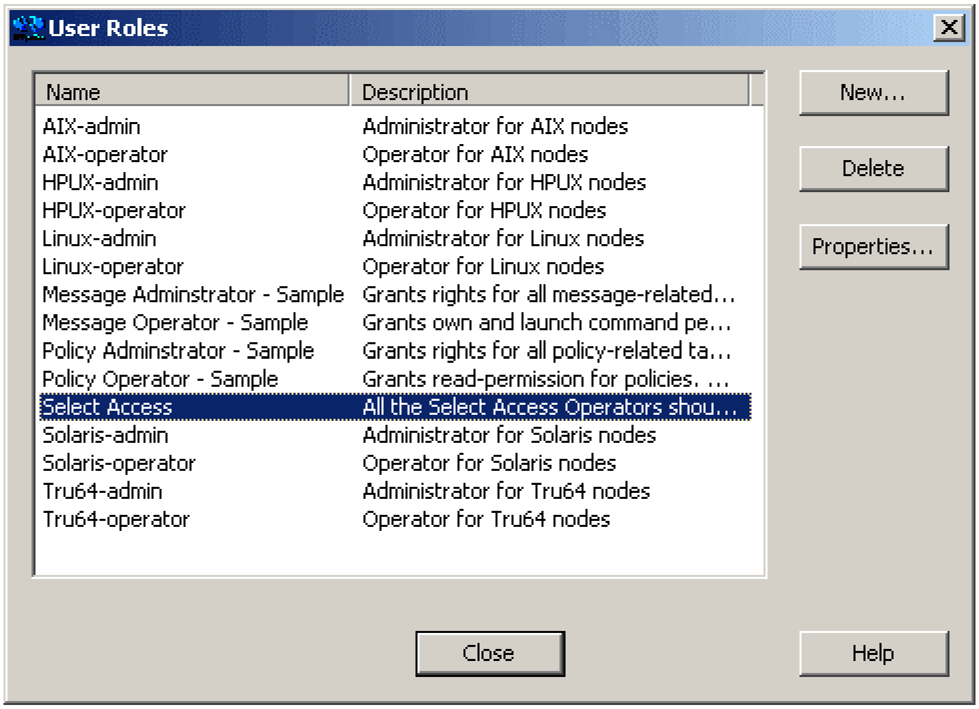


Figure 3-5: Removing Policy Group

Removing the User Role

1 From the management console menu, select **Action->Configure->User Roles**.

2 In the User Roles window that is displayed, select the role **Select Access,** then click **Delete** and **Close**.



Name	Description
AIX-admin	Administrator for AIX nodes
AIX-operator	Operator for AIX nodes
HPUX-admin	Administrator for HPUX nodes
HPUX-operator	Operator for HPUX nodes
Linux-admin	Administrator for Linux nodes
Linux-operator	Operator for Linux nodes
Message Adminstrator - Sample	Grants rights for all message-related...
Message Operator - Sample	Grants own and launch command pe...
Policy Adminstrator - Sample	Grants rights for all policy-related ta...
Policy Operator - Sample	Grants read-permission for policies. ...
Select Access	All the Select Access Operators shou...
Solaris-admin	Administrator for Solaris nodes
Solaris-operator	Operator for Solaris nodes
Tru64-admin	Administrator for Tru64 nodes
Tru64-operator	Operator for Tru64 nodes

Figure 3-6: Removing User Roles

Removing the Tool Folders

1. From the management console menu, select **Action->Configure->Tools**.
2. In the Tools window that is displayed, right-click the folder **SPI for Select Access** and then select **Delete**.

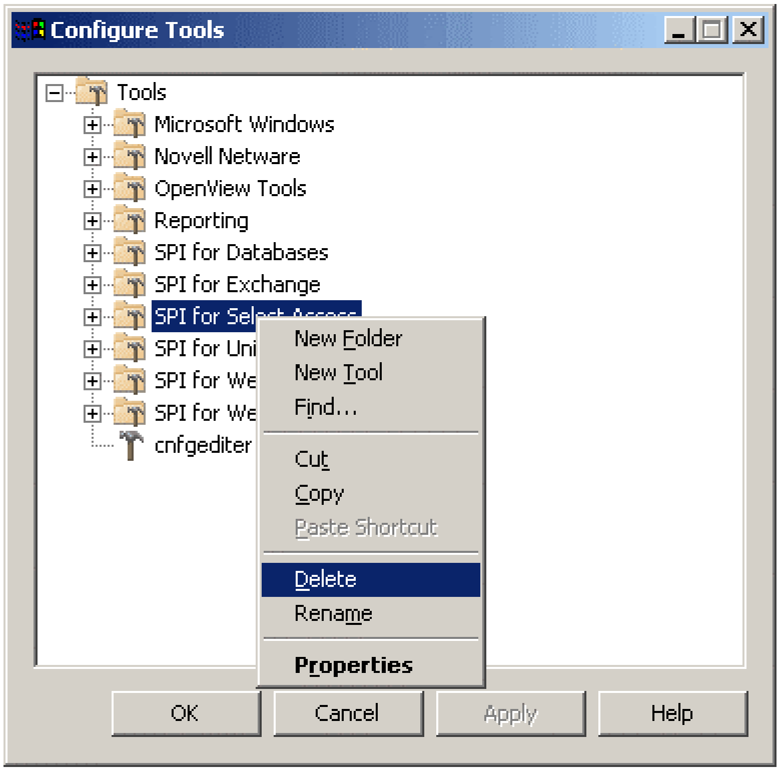


Figure 3-7: Removing Tools

Removing the Node Groups

1. From the management console menu, select **Action->Configure->Nodes**.
2. Select **Nodes-> Select Access** and expand the Select Access folder.
3. For each node group under Select Access, right-click on the node icons and select **Delete**.
4. After all nodes are removed from the Select Access node groups, select the Select Access node group, right-click and select **Delete**.
5. Select **Yes** when asked to confirm deletion.
6. Select **OK** to exit the Configure Managed Nodes window.

Removing the Services

1. From the management console menu, select **Action->Configure->Nodes**.
2. Select **Services->Applications-> Select Access** and then click **Delete**.
3. Select **Yes** when asked to confirm deletion.
4. Select **OK** to exit the Service Configuration window.

Removing the Software

1. On the management server, select **Add/Remove Programs** from the Control Panel.
2. Select **SPI for Select Access** and then click **Remove**.
3. A window displays the following message, “Are you sure you want to remove SPI for Select Access from your computer.” Select **Yes**.

The removal of the SPI for Select Access is complete once all these steps have been performed.

4

Using & Customizing SASPI

Adding Nodes to Node Groups

SASPI makes assigning policies to nodes easy by including component-specific node groups. Assigning a node to the corresponding SASPI node group automatically assigns the appropriate policies, as well as auto-deploys the policies. See Node Groups for a description of the SASPI node groups.

1 SASPI policies and tools rely on the Microsoft Windows instrumentation to be deployed to the managed node. If these are not deployed, SASPI monitors and tools will fail because programs cannot be found. To deploy Windows instrumentation:

   — Select **Policy management->Policy groups->Microsoft Windows->Auto-Discovery->Auto-Deploy** in the OVOW console.

   — Right-click on the policies WINOSSPI-MSWINApp_AutoDiscovery and select **All Tasks->Deploy on…**.

   — Select the nodes you want to deploy the software on and then press **OK**.

   — Repeat the same step for the policy WINOSSPI-MSWINSys_AutoDiscovery

2 From the console menu, select **Action->Configure->Nodes**.

3 In the right-hand pane, select the node you want to assign to a node group, right-click and select **Copy**. Then select the node group, right-click and select **Paste Shortcut**.

4 When all your assignments have been made, press **OK**.

Configuring SASPI Operators

An OVOW operator, to monitor the Select Access environment, will need to be assigned the Select Access message group and SASPI node groups. The easiest way to assign these responsibilities is to add the operator to the Select Access user profile.

1 From the console menu, select **Action->Configure->User Roles**.

2 Then highlight the **Select Access** user role, and click **Properties**.

3 Select the **Users** tab, and click **Add**.

4 Select a user from the HP-OVE-OPERATORS group, click **Add**, and then press **OK**.

5 Press **OK**.

Using SASPI Tools

The Smart Plug-in for Select Access includes tools to monitor the Select Access component services. Tools groups are created for the Validator, Administration Server, SAML Server, and Secure Audit Server components; each group contains the specific tools for the administration of that component. There are no tools for the Enforcer plug ins because these plug-ins are libraries loaded into a Web or application server. Control of this component should be managed by the Web server or the application server SPI.

You can perform the following activities with these tools on the Select Access components. You have to run the tool depending on the type of component installed on the managed node. The node groups created by SASPI will have the appropriate tools groups assigned to them, so that you can directly launch the correct tools by right-clicking on the node on which you want to launch the tool. For more information on tools, see the topic *Applying Tools to Managed Nodes and Services* in the OVOW on-line help.

- **Status of Select Access Service:** An operator can launch this tool against the node to find the status of the Select Access component service. The tool will run a program on the managed node to determine the status of the service and will display the result in the Tool Execution screen.
- **Stop Select Access Service:** Operators can launch this tool against a managed node to stop the Select Access component Service. The tool will run a NET STOP command on the selected node to stop the desired Select Access service; it will then display the result in the Tool Execution screen.
- **Start Select Access Service:** Operators can launch this tool against a managed node to start the Select Access component service. The tool will run a NET START command on the selected node to start the desired Select Access service; it will then display the result in the Tool Execution screen.

Configuring SASPI Fault Monitoring

The Select Access components have the ability to write out log messages to various destinations. The default functionality is to write messages to a system file (i.e., syslog or Event Log). In addition, the Select Access components can be configured to send log information to the Select Access Secure Audit Server.

To monitor Select Access error messages through OVOW, the Select Access components will need to be configured to log information into a text file on a central Secure Audit Server. This setup will centralize the log file monitoring to a single server. The SASPI_AuditLogs policy will translate messages that are forwarded to OVOW so that they appear to come from the affected server instead of the Secure Audit Server. This allows SASPI to support error messages from components that do not have OVOW agents on them or are platforms that are not supported by the SASPI (i.e., Linux, HP-UX, and Solaris).

To configure the Select Access components, use the Select Access Setup tool to create a log file destination. The SASPI_AuditLogs policy is pre-configured to monitor the text file `C:\Program Files\HP Openview\Select Access\logs\saspi.log`. Any destination log file could be used, but if you do not use the default, then you will have to modify the SASPI_AuditLogs policy to match the audit log destination. For information on modifying the log file source, see the topic *Select the Log File to Monitor* in the OVOW on-line help.

For more information on the Select Access Secure Audit Server or Setup tool, see the Select Access Installation Guide.

To configure the Select Access Secure Audit Server, start the Setup tool on the audit server node and proceed to the Secure Audit Server configuration section.

1 From the Audit Settings window, select **Add** to create a new destination.

2 Select **File** in the **Audit Trail** tab and click **Configure**.

3 In the Audit Trail – File Properties window, enter `C:\Program Files\HP OpenView\Select Access\logs\salog.log` in the Windows File Name field and press **OK**.

4 Select the **Audit Policy** tab, change the event level to WARNING, and press **OK**.

5 Press **Next** until the Secure Audit Server – Finish dialog is displayed, then press **Finish**.

For each Select Access component in the environment, start the Setup tool and proceed to the configuration for that component.

1 When the Audit Settings dialog is displayed for the component, click **Add**.

2 Select the Secure Audit Server destination, and click **Configure**.

3 Enter the name and port of the Secure Audit Server where you will distribute the SASPI fault monitoring policy and press **OK**.

4 In the **Audit Policy** tab, set the Component to * and the Event Level to WARNING and press **OK**.

5 Press **Next** until the Select Access component configured has finished and restarted.

The SASPI_AuditLogs policy includes basic conditions to capture all WARNING, ERROR, and FATAL messages. Eventually, an OVOW administrator may want to customize the policy to suppress some messages or to modify the default behavior of others. The best method for customizing policies is to use the current SASPI_AuditLogs conditions, select the condition that matches the severity as a base and copy it. Then modify the copy making sure that the new condition is ranked ahead of the basic condition. For more information on creating new log file conditions, see the topic *Set Log File Rule Conditions* in the OVOW on-line help.

Configuring SASPI Availability Monitoring

The SASPI availability monitoring reports on the status of the essential Select Access services and provides a facility to restart Select Access services as operator-initiated actions.

- If the monitored Select Access service is not running, the SASPI availability monitoring policies will generate an OVOW message in the active message browser to notify the operator.
- If the service restarts or is running again, the OVOW message in the active browser will be automatically acknowledged and a message will be sent to the OVOW acknowledged message browser stating the service is running.

The OVOW message includes an automatic action to get service status information for the unavailable service and an operator-initiated action to start the unavailable service.

The SASPI monitors the following services:

- HP Openview Select Access Validator
- HP Openview Select Access Administration Server
- HP Openview Select Access SAML Server
- HP Openview Audit Server

There is no availability monitoring for the Enforcer plug in because these plug-ins are libraries loaded into a Web or application server. Availability of this component should be covered by a Web server or application server SPI.

The default interval for monitoring a Select Access service is five minutes. If a different duration is required, you can edit the policy and redistribute. For more information on editing monitoring policies, see the topic *Set the Threshold Source Properties* in the OVOW on-line help.

Configuring SASPI Performance Monitoring

In a Select Access environment, as users request Web pages, the Enforcer plug in sends credential information to the Validator, where it is determined if the user has sufficient authorization to view the Web page. The performance of this authorization check is an important part of the overall end-to-end response time of the user request. The Select Access performance monitoring policy, when deployed to a node with an Enforcer plug in, performs a query from that node to the configured Validator to measure responsiveness. The results of these queries can be used to make sure that the Select Access environment does not impact the overall Web experience.

The SASPI performance monitoring policy SASPI_PerfMon uses the Select Access Query utility (typically found under `C:\Program Files\HP OpenView\Select Access\bin`). The Query utility is a command-line application that sends queries to a Validator to check a request against the policy matrix, evaluate the performance within the environment, and review simple and advanced authentication. For details, see *The Query Utility* in the Select Access Network Integration Guide.

SASPI_PerfMon does a single check against a user-configured URL. The results are checked against the default threshold of 0.9 seconds. If the query takes longer than the threshold, a message is generated to the OVOW message browser.

SASPI_PerfMon is dependent upon the Generic Enforcer Plug in being configured on the system upon which it runs. The Generic Enforcer Plug in is configured using the Select Access Setup tool. The Generic Enforcer Plugin creates an enforcer.xml file that is used by the Query utility and should be located in the same directory as the Query utility, which is in `<Select Access Install Directory>\bin (e.g., C:\Program Files\HP OpenView\Select Access\bin\enforcer.xml`.

To configure the target for the query, perform the following steps:

1. In the OVOW console, double-click on the **SASPI-PerfMon** policy to edit it.
2. In the Program Name field, go to the end of the line and replace “`http://www.hp.com`” with your target.

   You can also customize the threshold to match the performance expectations of your Select Access environment by clicking the **Threshold** levels tab. For more information on editing monitor policies, see the topic *Set General Threshold Rule Properties* in the OVOW on-line help
3. Highlight the **Checking for Validator Responsiveness** condition and click on **Modify**.
   - The threshold for this policy is defined in the SAPerfMon Object in the Threshold Limit field.
   - You will have to redeploy this policy to Enforcer nodes for the new target and threshold to be set.
   - If you plan to set different targets and thresholds for different nodes, make multiple copies of the SASPI_Perfmon policy by using the Save As option of the Policy Edit window. Refer to the OVOW User Guide for more information about editing and deploying policies on the managed nodes.

Customizing the SASPI Service View

The SASPI Service View installed by default is a virtual service view. The Select Access environment is represented by displaying the Select Access components rather than the systems that they run on. The components have sub-service containers representing availability, fault, and performance, depending on the type of component.

The sub-services represent the following:

- **Availability:** Any service failure of the Secure Audit Server, Administration Server, Validator, or SAML Server service will automatically show a problem for that component in the service tree on the availability sub-service.
- **Fault:** Detection of a warning, error, or fatal message will result in status change of the fault sub-service of the component that generated the message. Even though the policy is deployed on the Secure Audit Server, the policy will automatically find the Select Access component that generated the error in the log file.

- **Performance:** Performance monitoring detects response-time violations between an Enforcer and Validator. The performance sub-service is under the Enforcer branch of the Select Access service view since we are running the performance monitoring policy from the Enforcer node.

The Select Access Application tree is a virtual service tree and not a discovered service tree. All the sub-services under this tree have specific service IDs that correspond to message conditions created in the policies to directly affect the status of this service tree.