

# HP OpenView Select Access

For the Windows®, HP-UX, Linux, and Solaris Operating Systems

Software Version: 6.1

---

## Installation Guide

May 2005



## 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

© Copyright 2000-2005 Hewlett-Packard Development Company, L.P.

No part of this document may be copied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard Company. The information contained in this material is subject to change without notice.

### Trademark Notices

HP OpenView Select Access includes software developed by third parties. The software HP OpenView Select Access uses includes:

- The OpenSSL Project for use in the OpenSSL Toolkit.
- Cryptographic software written by Eric Young.
- Cryptographic software developed by The Cryptix Foundation Limited.
- JavaService software from Alexandria Software Consulting.
- Software developed by Claymore Systems, Inc.
- Software developed by the Apache Software Foundation.
- JavaBeans Activation Framework version 1.0.1 © Sun Microsystems, Inc.
- JavaMail, version 1.2 © Sun Microsystems, Inc.
- SoapRMI, Copyright © 2001 Extreme! Lab, Indiana University.
- cURL, Copyright © 2000 Daniel Stenberg.
- Protomatter Syslog, Copyright © 1998-2000 Nate Sammons.
- JClass LiveTable, Copyright © 2002 Sitraka Inc.

For expanded copyright notices, see HP OpenView Select Access <install\_path>/3rd\_party\_license directory.

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://www.managementsoftware.hp.com/>**

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

You can also go directly to the support web site at:

**<http://support.openview.hp.com/>**

HP OpenView online software 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 valuable support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter 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 log in. Many also require a support contract.

To find more information about access levels, go to:

**[http://support.openview.hp.com/access\\_level.jsp](http://support.openview.hp.com/access_level.jsp)**

To register for an HP Passport ID, go to:

**<https://passport2.hp.com/hpp/newuser.do>**



# Contents

<b>1</b>	<b>Preparing to Install Select Access Components</b>	<b>7</b>
	Audience	7
	The Select Access Documentation Set	7
	Gauging Your Installation Environment	8
	Minimum System Requirements	9
	Platform Availability	9
	Supported LDAP Directory servers	11
	Supported Third-Party Servers	12
	Chapter Summary	12
<b>2</b>	<b>Planning Your Rollout of Select Access</b>	<b>15</b>
	Chapter Overview	15
	Issues That Affect Deployment	15
	Analyzing Corporate Security	17
	Analyzing Your Redundancy Policy	18
	Analyzing Your Directory Topology	20
	Analyzing Your Affiliates or Partners	20
	Analyzing Your Potential for Growth	21
	Analyzing your Content Servers and Third-Party Technologies	21
	Deployment Scenarios	22
	Centrally Located Deployment by a Mid-Sized Manufacturer	23
	Fully Distributed Deployment by a Multi-National Enterprise	25
<b>3</b>	<b>Installing Select Access</b>	<b>29</b>
	Chapter Overview	29
	Before You Begin: Available Install Options	29
	Installing Select Access for the First Time	30
	Upgrading from a Previous Version of Select Access	30
	Upgrade Issues	32
	Reapplying Index.html Customizations	32
	Supporting IBM and Apache 2 Servers	32
	The Retirement of the SAML server	32
	Installing the WSE Enforcer Plugin	33
	Manually Deleting Old Files on Unix	34
	Running the Select Access 6.1 Installer	34
	Preinstallation Issues	34
	Running the Installer—a Mode Overview	37
<b>4</b>	<b>Configuring Select Access</b>	<b>55</b>
	Chapter Overview	55

Where Data is Recorded . . . . .	55
About the selectaccess.conf File . . . . .	56
Understanding Setup Methods and Parameter Types. . . . .	56
Using the Setup Tool . . . . .	57
How to Set up Select Access. . . . .	58
Things to Check Before You Finish. . . . .	61
<b>5 Configuring the Administration Server . . . . .</b>	<b>63</b>
Chapter Overview . . . . .	63
What the Administration Server Does . . . . .	63
Configuring the Administration Server . . . . .	64
The Administration Server's Main Setup Types. . . . .	64
Using the Setup Tool to Configure the Administration server. . . . .	64
Defining the Administrator Credentials . . . . .	68
Defining your Policy Store . . . . .	69
Specifying the Policy Data Location . . . . .	70
Preconfiguring an Identity Location . . . . .	71
Choosing your Setup Type . . . . .	73
Defining the Administration Server Connection Information . . . . .	74
Configuring the Policy Builder Administration Modes . . . . .	75
Configuring the Web-based Administration Services. . . . .	76
Setting up SSL Connection Handling . . . . .	77
Configuring the Directory Server's Certificate . . . . .	78
Configuring Policy Store Data Signing . . . . .	79
Verifying the Signer's Certificate. . . . .	81
Creating a Replicated Directory Servers List . . . . .	82
Configuring Global Audit Settings . . . . .	83
Configuring Database Reporting . . . . .	84
Completing the Administration Server Setup Process. . . . .	85
Failing Over to Another Administration server . . . . .	86
Adding Delegated Administration CA Certificates . . . . .	86
Different Certificate Types. . . . .	87
<b>6 Configuring the Secure Audit Server . . . . .</b>	<b>93</b>
Chapter Overview . . . . .	93
Understanding the Secure Audit Server . . . . .	93
Differences in Message Types . . . . .	94
Setting up Server-based Auditing. . . . .	94
Configuring the Secure Audit Server . . . . .	95
Using the Setup Tool . . . . .	95
Configuring the Secure Audit Server Connection Information . . . . .	97
Configuring Server-Specific Audit Settings . . . . .	98
Configuring Audit Stream Signing . . . . .	99
Completing the Secure Audit server Setup Process . . . . .	100
Configuring an Audit Trail . . . . .	101
Configuring a Secure Audit Server . . . . .	103
Configuring a Database . . . . .	104

Creating Database Tables .....	106
Configuring a Log File .....	107
Configuring an Email Alert .....	108
Configuring System Logging .....	110
Configuring a Standard Error Stream .....	110
Configuring an Audit Policy .....	110
How you create audit policies.....	110
<b>7 Configuring the Policy Validator .....</b>	<b>115</b>
Chapter Overview .....	115
How Does the Policy Validator Work?.....	115
Configuring the Policy Validator.....	117
The Policy Validator's Main Setup Types .....	117
Using the Setup Tool to Configure the Policy Validator.....	117
Connecting to the Administration Server .....	120
Choosing Your Setup Type .....	121
Setting Connection Parameters for the Policy Validator .....	122
Configuring Validator-Specific Audit Settings .....	124
Defining Data Encryption Settings .....	125
Specifying a Password Dictionary .....	126
Tuning your Policy Validator .....	126
Completing the Policy Validator Setup Process .....	128
<b>8 Configuring the Enforcer Plugins .....</b>	<b>129</b>
Chapter Overview .....	129
How the Enforcer Plugin Works .....	129
Configuring the Enforcer Plugin.....	129
The Enforcer Plugins' Main Setup Types .....	130
A Note About Enforcer-Specific Setup Wizards .....	130
Using the Setup Tool to Configure the Enforcer Plugin.....	131
Connecting to the Administration Server .....	135
Choosing Your Setup Type .....	136
Defining an Enforcer Plugin ID .....	138
Setting up Single Domain Single Sign-on .....	139
Setting up Multiple Domain Single Sign-on .....	140
Setting up SOAP Message Signing .....	141
Setting up SOAP Message Encrypting .....	142
Setting up a List of Ignored Filenames .....	143
Setting up a list of pass-through domains.....	145
Configuring Enforcer-Specific Audit Settings.....	146
Configuring Policy Validator Settings .....	148
Mapping Policy Validators to NAT Addresses.....	149
Tuning your Enforcer plugin .....	150
Completing the Enforcer Plugin Setup Process .....	154
Starting Your Enforcer Plugin.....	156
The Netscape/iPlanet/Sun ONE Web Server Dialog Box .....	156
The Apache Web Server Dialog Box.....	157
The IIS Web Server Dialog Box .....	158

The Axis Host Application Dialog Box . . . . .	159
Manually Configuring inetd to Start the TCP Enforcer Plugin . . . . .	159
Uninstalling the Enforcer plugins . . . . .	160
<b>9 Configuring Custom Settings . . . . .</b>	<b>161</b>
Chapter Overview . . . . .	161
Understanding Custom Settings . . . . .	161
When is it Necessary to Configure Custom Settings? . . . . .	161
Configuring the Custom Settings Flags . . . . .	162
About Select Access Predefined Flags . . . . .	162
Using the Setup Tool to Configure the Custom Settings Flags . . . . .	163
Connecting to the Administration Server . . . . .	164
Enabling Custom Settings Flags . . . . .	165
Completing the Custom Settings Setup Process . . . . .	166
<b>10 Maintaining Select Access: Failovers, Repairs, and Updates . . . . .</b>	<b>169</b>
Chapter Overview . . . . .	169
Failing Over to Another Administration Server . . . . .	169
Tips for Ensuring a Smooth Recovery . . . . .	169
Maintaining Select Access . . . . .	171
Repairing Select Access . . . . .	171
Modifying Select Access . . . . .	184
Uninstalling Select Access . . . . .	194
<b>11 Starting and Stopping Components . . . . .</b>	<b>201</b>
Starting the Setup Tool . . . . .	202
Starting the Setup Tool from the Installer . . . . .	202
Starting the Setup Tool Any Time . . . . .	202
Starting the Policy Builder . . . . .	203
Starting and Stopping the Administration Server . . . . .	203
When to Restart the Administration server . . . . .	203
Starting and Stopping the Policy Validator . . . . .	205
When to Restart the Policy Validator . . . . .	205
Starting and Stopping the Secure Audit Server . . . . .	208
When to Restart the Secure Audit server . . . . .	208
<b>11 Chapter:Title . . . . .</b>	<b>210</b>
<b>A Policy Validator Stability: Setting File Descriptor Limits . . . . .</b>	<b>211</b>
Appendix Overview . . . . .	212
Increasing Unix Connection Limits for the Policy Validator . . . . .	212
Configuring the Limit on Linux and Solaris . . . . .	212
Configuring the Limit on HP-UX . . . . .	212
<b>B Character Set Listing . . . . .</b>	<b>215</b>
<b>C Troubleshooting . . . . .</b>	<b>223</b>
Appendix Overview . . . . .	223
Installer Errors . . . . .	223



Out of Memory Error when Installing on HP-UX . . . . .	223
Policy Builder Errors . . . . .	224
Network Discovery Not Detecting Redirects . . . . .	224
Policy Builder and Critical Path Index Node Values . . . . .	224
Running Policy Builder in Delegated Administration Mode . . . . .	225
Running Two Sessions on the Same Machine . . . . .	225
X11 Display Error with Delegated Mode on Solaris . . . . .	225
Policy Validator Errors . . . . .	226
Policy Validator Registers with Wrong Address on Linux . . . . .	226
Policy Validator Generates Error When Installing . . . . .	226
Policy Validator Failing at Startup . . . . .	227
Policy Validator and Hostnames . . . . .	227
iPlanet 4.0 and Sun ONE 6.0: Cookies Not Refreshed on IE . . . . .	227
Policy Validator Looping . . . . .	228
Policy Validator Short Circuits . . . . .	228
Policy Validator Missing SSL session Information . . . . .	228
Web server/Application Server Errors . . . . .	228
HTTP Basic Authentication Problematic . . . . .	229
Restricted IBM HTTP Server Resources . . . . .	229
Virtual Web Server Support Problems with IIS . . . . .	229
Caching Problems with IIS . . . . .	230
Integrated Windows authentication issues on IIS . . . . .	230
Denied Access Errors . . . . .	231
Denied Access to Service . . . . .	231
Denied Access on Default Page . . . . .	231
Browser Gets Deny yet Policy Validator Returns Allow . . . . .	231
Directory Server Errors . . . . .	232
Active Directory 2003 and Profile Password Setup Problems . . . . .	232
iPlanet and iPlanet Unicode Problems . . . . .	232
Critical Path and Siemens Over SSL Problems . . . . .	233
Certificate Errors . . . . .	233
Browsing for OCSP certificates on Critical Path . . . . .	233
Generic Problems . . . . .	234
Microsoft Certificates and Failed Signing . . . . .	234
Problems Specific to IIS . . . . .	235
Problems Specific to Apache . . . . .	235
Browser Errors . . . . .	235
SSO Failing on Internet Explorer . . . . .	236
Logging Errors . . . . .	236
Database and email outputs creates XML error . . . . .	236
Personalization Problems . . . . .	236
Empty Dynamic Group Attribute Values . . . . .	236
Password Management Problems . . . . .	237
Glossary . . . . .	239
Index . . . . .	247



# 1 Preparing to Install Select Access Components

Identity management touches upon almost every aspect of the HP Adaptive Enterprise vision, affecting access to information across hardware, software, network resources, application servers, enterprise applications, and web portals within an organization and across organizations via business-to-business transactions.

For managing an adaptive enterprise—one that can respond quickly to change—HP OpenView Select Access provides systematic and secure user access to third-party network services and the enterprise resources they deploy. Select Access provides integrated infrastructure management that drastically reduces corporate IT costs.

By using a highly scaleable and extensible architecture, Select Access integrates with most dynamic IT environments that include:

- Wireless, web, non-web and legacy applications support.
- Native LDAP v3 directory serves as the repository for user, resource and policy data; works with existing user data and directory schema.
- Leading web J2EE-compliant application and portal servers.
- Popular authentication schemes to allow flexibility in strength of user identification.

## Audience

This document is intended for system administrators mandated to install and configure HP OpenView Select Access 6.1 to suit their business and industry environment. This guide assumes a working knowledge of:

- **LDAP directory servers:** This ensures that information in Policy Builder is set up correctly.
- **Web server and plugin technology:** This helps you to understand how different components of Select Access communicate with each other and with your existing infrastructure.

## The Select Access Documentation Set

This manual refers to the following Select Access documents. These documents are installed with Select Access and are available in the `<install_path>/docs` folder.

- *HP OpenView Select Access 6.1 Installation Guide*, © Copyright 2000-2005 Hewlett-Packard Development Company, L.P. (`installation_guide.pdf`).
- *HP OpenView Select Access 6.1 Policy Builder Guide*, Copyright 2000-2005 Hewlett-Packard Development Company, L.P. (`policy_builder_guide.pdf`)

- *HP OpenView Select Access 6.1 Network Integration Guide*, © Copyright 2002-2005 Hewlett-Packard Development Company, L.P. ([integration\\_guide.pdf](#))
- *HP OpenView Select Access 6.1 Concepts Guide*, © Copyright 2005 Hewlett-Packard Development Company, L.P. ([concepts\\_guide.pdf](#))

*Integration Papers* for Select Access and vendor—specific technologies are available on the product CD in the `docs/solutions` folder.

Online help is available with both the Setup Tool and the Policy Builder components.

As part of the Select Access SDK, two other documents are also available with this product:

- *HP OpenView Select Access 6.1 Developer's Tutorial Guide*, © Copyright 2004-2005 Hewlett-Packard Development Company, L.P. ([dev\\_tut\\_guide.pdf](#))
- *HP OpenView Select Access 6.1 Developer's Reference Guide*, © Copyright 2004-2005 Hewlett-Packard Development Company, L.P. ([dev\\_ref\\_guide.pdf](#))

For details on how to obtain this SDK, visit HP's Partner Care site ([http://support.openview.hp.com/partner\\_care.jsp](http://support.openview.hp.com/partner_care.jsp)).

## Gauging Your Installation Environment

Before you begin installing Select Access, consider your current network architecture and see what limitations can affect your deployment of Select Access components on various network host machines. Potential limitations are described in the following topics:

- [Minimum System Requirements](#) on page 9
- [Platform Availability](#) on page 9

Additionally, depending on which third-party technologies you want to integrate Select Access with, consider reviewing which servers are supported by this version of the product. Supported technologies are summarized in the following sections:

- [Supported LDAP Directory servers](#) on page 11
- [Supported Third-Party Servers](#) on page 12

## Minimum System Requirements

To install any of the Select Access components, your system must meet the minimum hardware and software requirements outlined in [Table 1](#).

**Table 1 Minimum System Requirements**

Hardware & Software	Minimum on Windows	Minimum on Unix
Processor	For single-component installs: Pentium 4 For combined Administration server & Setup Tool installs: 2.6 GHz	For single-component installs on Linux: Pentium 4 For single-component installs on Solaris: Sun Ultra5 For single-component installs on HP-UX: HP-UX 9000
Memory	For single-component installs: 512 MB RAM For combined Administration server & Setup Tool installs: 1 GB	For single-component installs: 512 MB RAM For combined Administration server & Setup Tool installs: 1 GB
Disk space (combination of temporary space and real space required for a full install)	250 MB	For Linux: 150 MB For Solaris: 300 MB For HP-UX: 220 MB
Video card	256 colors	256 colors
Operating systems <i>Note:</i> Not all components are supported on all operating systems. See <a href="#">Platform Availability</a> on page 9 for details.	Windows 2000 Professional Service Pack 2 Windows 2000 Server Service Pack 2 Windows 2003 Windows XP	Red Hat Enterprise Linux 3 Solaris 9 HP-UX 11.B.11.23 64 bit with all required patches

## Platform Availability

The Select Access components are available for the following platforms: Windows (Windows XP, Windows 2000, and Windows 2003) and Unix (Linux, Solaris, and HP-UX).



HP-UX hosts must apply the all required patches before running and installing Select Access.

You can install or upgrade Select Access components on different platforms; all components communicate with each other irrespective of the platform you installed them on. However, if you are upgrading components, you must adhere to strict upgrade path guidelines, for details, see [Upgrading from a Previous Version of Select Access](#) on page 30.

[Table 2](#) provides a comprehensive list of components and their corresponding supported platforms.

**Table 2 Platform Availability**

Components	Platforms					
	Windows XP	Windows 2000	Windows 2003	Red Hat Linux AS 3.0	Solaris 9	HP-UX 11.23 PA-RISC
<b>Documentation set:</b> A set of documents that are designed to help you use Select Access.	•	•	•	•	•	•
<b>Front-end (GUI) components</b>						
<b>Setup Tool:</b> A standalone configuration tool that is installed on any computer that hosts any Select Access component.	•	•	•	•	•	•
<b>Policy Builder:</b> The interface used to manage access policies and delegate and/or sub-delegate administration duties.	•	•	•		•	•
<b>Back-end components</b>						
<b>Administration server:</b> A component that conducts administrative functions such as component configuration, certificate management, and policy data administration.		•	•		•	•
<b>Policy Validator:</b> Select Access’s decision-making component that determines whether identity access is allowed or denied.		•	•	•	•	•
<b>Secure Audit server:</b> Select Access’s log tool that collects and manages incoming log messages from components on a network.		•	•		•	•
<b>Enforcer plugins:</b> Select Access’s decision-enforcement component. Select Access includes Enforcer plugins for the following Web servers:						
• Sun/Netscape/iPlanet Enforcer plugin for Sun 6.0 Web servers, Netscape 6.1 Web server and iPlanet 4.0 Web servers		•	•	a	•	•
• Apache 2 Enforcer plugin		•	•	•	•	•
• IIS Enforcer plugin		•	•			
• WSE Enforcer plugin (Available only if the .NET framework and associated utilities have been installed.)		•	•			
• Axis Enforcer plugin		•	•	•	•	•
• Servlet Enforcer plugin		•	•	•	•	•

**Table 2 Platform Availability (cont'd)**

Components	Platforms					
	Windows XP	Windows 2000	Windows 2003	Red Hat Linux AS 3.0	Solaris 9	HP-UX 11.23 PA-RISC
<ul style="list-style-type: none"> <li>TCP Enforcer plugin</li> </ul>				•	•	•
<b>Utility programs</b>						
<p><b>Query program:</b> A command-line application that sends queries to a Policy Validator.</p>		•	•	•	•	•

a. The Netscape 6.1 Web server is not supported on Red Hat Linux 3.0. Therefore, Select Access' Sun/Netscape/iPlanet Enforcer plugin is also not supported with this combination.

## Supported LDAP Directory servers

Select Access uses LDAP v3-compliant directory servers for searching and storing identity information. By integrating with standards-compliant LDAP servers and metadirectories for access to legacy identity data stores, information can be easily synchronized across a globally dispersed network, including those with multiple delegated administrators.



If your directory servers require a schema update, you must do this before you install and run Select Access. Depending on your directory server, the schema update process can be automatic or require manual intervention. For details, see [Chapter 2, Directory Server Integrations](#), in the *HP OpenView Select Access 6.1 Network Integration Guide*.

To make the adoption of Select Access as immediate and as far-reaching as possible, HP has included support for several LDAP v3-compliant directory servers:

- Sun ONE 5.1 and Netscape 6.01
- NDS eDirectory 8.7.3
- Siemens DirX 6.0 01/2004
- Critical Path Directory 4.2
- Microsoft Active Directory for Windows 2000 with SP4 and for Windows 2003
- Microsoft ADAM for Windows 2003
- Oracle Internet Directory 9.2
- CA eTrust 8
- OpenLDAP 2.2.23



To see a list of which characters are supported by specific directory servers only, see [Appendix A, Invalid Characters](#) in the *HP OpenView Select Access 6.1 Policy Builder Guide*.

## Supported Third-Party Servers

You can protect a number of third-party servers with Select Access. The three most common types are the following:

- **Web servers:**
  - IIS 5.0/6.0 (core product support)
  - Apache 2.x (core product support)
  - Sun 6.0 Web servers, Netscape 6.1 Web server and iPlanet 4.0 Web servers (core product support)
  - Tomcat 4.0.3 (manual integration required)
- **Authentication servers:**
  - SecurID 4.1 on Solaris 2.8
  - ACE Agent 4.4 on Windows NT
  - ACE Agent 4.1 on Solaris 2.8 and HP-UX
  - ACE Agent 1.1 on Windows 2000
  - Active Card RADIUS 4.0 on Windows NT
- **Application/portal/e-provisioning servers :**
  - BEA WebLogic 8.1 (manual integration required)
  - IBM WebSphere 5.0 (manual integration required)
  - iPlanet Application Server (manual integration required)
  - Domino 5.0.8 Application Server (manual integration required)
  - Oracle 10g Application Server for Windows 2003 only (manual integration required)
  - Outlook Web Access Server for Windows 2000 (manual integration required)
  - Citrix Metaframe Presentation Server 3.0 Web Interface (manual integration required)
  - Siebel 7.0.4 (manual integration required)
  - Plumtree Corporate Portal 4.5 (manual integration required)

For information on how to integrate Select Access with third-party technologies, see the corresponding *Integration Paper* in the `docs/solutions` folder of the product CD.

## Chapter Summary

This guide includes the chapters listed in [Table 3](#).



See the *HP OpenView Select Access 6.1 Release Notes* (`relnotes.pdf`) on the Select Access installation CD for known installation issues at the time of this release.



**Table 3 Guide Overview**

<b>Chapter</b>	<b>Description</b>
Chapter 2, Planning Your Rollout of Select Access	Before you begin installing Select Access, allocate some resources to planning your deployment. By taking time up front to understand your network and needs, you are more likely to deploy an access management system that is as easy to scale as it is to manage. This chapter gives you the necessary knowledge and advice that reduces any complexity inherent in a component-based product like Select Access.
Chapter 3, Installing Select Access	Because HP employs an InstallAnywhere installer, Select Access is as simple to install as it is to configure. This chapter provides an overview of how to install the Select Access components on your network.
Chapter 4, Configuring Select Access	Select Access is considered a management-free system. That means that a wizard, known as the Setup Tool, guides you through configuration options for components you have installed. It then manages this setup through the directory server, which enables you to effortlessly add additional components for real-time scalability. New components are registered in the directory, and component configurations are automatically downloaded from the directory. This chapter provides an overview of how to configure Select Access with the wizard-based Setup Tool.
Chapter 5, Configuring the Administration Server	The Administration server is the first component you need to set up. The Administration server handles SSL details and configuration information. Without an Administration server configured and running, you are not allowed to configure your remaining Select Access components—except the Secure Audit server. This chapter describes how to deploy this component on your network.
Chapter 6, Configuring the Secure Audit Server	The Secure Audit server is a tamper-resistant method for monitoring stability, data integrity, and corporate security—all via a centralized server. This chapter describes how to deploy the Secure Audit server, so that it records all access and authorization actions, as well as all policy administrative changes.
Chapter 7, Configuring the Policy Validator	The Policy Validator is Select Access’s evaluation engine. It decides when and how to authorize identity access to a given resource. This chapter describes how to deploy this component on your network.

**Table 3 Guide Overview (cont'd)**

<b>Chapter</b>	<b>Description</b>
Chapter 8, Configuring the Enforcer Plugins	The Enforcer plugin acts as an intermediary between the identity and the service on which it protects content. Because it relays messages to and from the Policy Validator on behalf of the service it protects, it is crucial that you set up this plugin correctly. This chapter describes this process.
Chapter 9, Configuring Custom Settings	While the Select Access Setup Tool provides a setup wizard for each Select Access component, it also includes an extra Custom Settings setup wizard designed to handle those rare instances when necessary parameters are not available in a component's own setup wizard. This chapter documents how to configure these settings.
Chapter 10, Maintaining Select Access: Failovers, Repairs, and Updates	From time to time, changes on your network may require that you modify your current deployment of Select Access. From failures to new third-party technologies, you may find that you need to re-distribute components you have installed. This chapter explains how to perform these tasks.
Chapter 11, Starting and Stopping Components	Once you have installed and configured your Select Access components, you can start and stop them as required. Different components support different start and stop methods. This chapter documents those methods.
Appendix A, Policy Validator Stability: Setting File Descriptor Limits	This appendix describes how to increase Unix connection limits for the Policy Validator.
Appendix B, Character Set Listing	This appendix lists the character sets supported by Select Access. Table 1 lists the specific sets you can define when configuring the Enforcer plugin's tuning parameters—either with the Setup Tool or the Policy Builder.
Appendix C, Troubleshooting	This appendix provides solutions to possible problems you may be experiencing.

---

## 2 Planning Your Rollout of Select Access

Before you begin installing Select Access, allocate some resources to planning your deployment. By taking time up front to understand your network and needs, you are more likely to deploy an access management system that is as easy to scale as it is to manage. This chapter gives you the necessary knowledge and advice that reduces any complexity inherent in a component-based product like Select Access.

### Chapter Overview

Topics in this chapter include subjects that describe how to plan your Select Access rollout:

- [Issues That Affect Deployment](#) on page 15
- [Deployment Scenarios](#) on page 22

### Issues That Affect Deployment

All successful deployments of Select Access require some assessment of your current environment. Environment issues, like those described in [Table 1](#), can have a substantial impact on your deployment of Select Access components. It is important that you analyze your environment to discover any unexpected integration concerns.

**Table 1 Environment Deployment Issues**

<b>Issue</b>	<b>Deployment Impact</b>
<i>Existing security measures</i> that work together to safeguard your organization’s resources and back-office systems from threats of unauthorized access or tampering, denial-of-service, and non-repudiation.	Determine how access management must complement these measures and integrate with them logically. If you require regular auditing or alerts to warn administrators, you need to plan and configure these accordingly. For details, see <a href="#">Analyzing Corporate Security</a> on page 17.
<i>Planned data and component redundancy</i> where replicas work together to prevent system faults and distribute loads evenly across server components on your network.	Decide where and how redundancy works specifically with Select Access components and your directory data. For details, see <a href="#">Analyzing Your Redundancy Policy</a> on page 18
<i>Distributed directory data topology</i> where an extremely large number of entries are logically distributed among different servers.	Establish how: <ul style="list-style-type: none"> <li>• The distribution of data across more than one server impacts your configuration of the Policy Builder.</li> <li>• Select Access supports a directory system that takes advantage of referrals.</li> </ul> For details, see <a href="#">Analyzing Your Directory Topology</a> on page 20.
<i>Multiple affiliations and partnerships</i> where you plan to integrate sites among your organizations in the near or not-too-distant future.	Requires the addition of a Select Access Federation server to your deployment. For details, see <a href="#">Analyzing Your Affiliates or Partners</a> on page 20.
<i>The potential for growth</i> and how you plan to adapt as the number of identities and resources requiring policy increases.	Entails looking at your current network resources and determining how readily they scale. For details, see <a href="#">Analyzing Your Potential for Growth</a> on page 21.
<i>Existing content servers</i> and any third-party application servers and portal content vendors you have.	Requires that you determine where dedicated and virtual Web servers exist, and how you set up Select Access to work with the latter. It also entails integrating Select Access with these products so that it can protect these vendor resources seamlessly. For details, see <a href="#">Analyzing your Content Servers and Third-Party Technologies</a> on page 21.

## Analyzing Corporate Security

The way you deploy Select Access depends on how you use access management to support your existing security system. Select Access can add a new level of security when shielding your network resources and other enterprise-level back-office systems.

### What security systems do you currently use?

You may already have a security system that is well adapted to your needs. Select Access needs to integrate with any of the following security techniques:

- **Authentication schemes:** Select Access currently supports the following authentication schemes: password, registration, certificate, Integrated Windows, NTLM, Kerberos, SecurID, and RADIUS. For each scheme that Select Access supports, you must provide configuration details that allows Select Access to use these methods. For details, see [Chapter 6, Setting Up Authentication Services](#), of the *HP OpenView Select Access 6.1 Policy Builder Guide*. If you have an unsupported authentication scheme, you need to create a plugin for it. For details, see the *HP OpenView Select Access 6.1 Developer's Tutorial Guide* and the *HP OpenView Select Access 6.1 Developer's Reference Guide*.
- **Password policies:** Select Access allows you to configure a password policy. If you have an existing corporate policy on passwords, you want to set up the Select Access policy so that it closely replicates important criteria of your corporate policy. For details, see [Configuring Password Policies](#) on page 185 of the *HP OpenView Select Access 6.1 Policy Builder Guide*.
- **SSL encryption and PKI systems:** Select Access uses certificate-based SSL encryption to protect the integrity of information as it is communicated among Select Access components, or between the directory servers Select Access relies on for its identity data. There are two ways you can deploy Select Access with SSL:
  - **Using your own SSL Certificates.** This option is the more difficult of the two options, due to the inherent complexity of different SSL configuration options among Select Access components. If you intend to use your own SSL certificates, ensure that you perform a **Custom** setup.
  - **Letting Select Access handle SSL its own way.** This is the recommended method of enabling SSL because it removes the complexity of configuring all Select Access components separately. If you do not need to configure SSL, ensure you perform a **Typical** setup.

For details on setting up SSL, see the component configuration chapters of the *HP OpenView Select Access 6.1 Installation Guide*.



SSL encryption only protects data while it is in transit. If you have concerns about protecting data at its source, you can use digital signatures to sign policy data in the directory server acting as your Policy Store. For details on signing policy data, see [Chapter 15, Managing your Policy Data](#), in the *HP OpenView Select Access 6.1 Policy Builder Guide*.

### Do you require regular auditing/reporting of network activities?

If so, you want to install a Secure Audit server to extend your current corporate auditing standards to include all Select Access components. The Secure Audit server allows you to track runtime messages of all Select Access components—especially when they are installed on a distributed network. It audits and collects log files generated by Select Access clients so you can check:

- The efficiency of all components
- Problems they might experience at runtime
- Conceivable or actual security threats or breaches



The Secure Audit server is not typically required in a small Select Access deployment. Because components are typically installed over a small, localized number of machines, collecting logs is a simple task that does not warrant a separate server.



If you use a JDBC-compliant database, you need to configure it correctly before the Secure Audit Server can log to it.

First, you need to enable database reporting in the Administration server setup wizard (this option is only available when you perform a **Custom** installation). For details, see [To configure database reporting](#) on page 85, in the *HP OpenView Select Access 6.1 Installation Guide*.

Second, you need to run the corresponding SQL script installed with Select Access. For details, see [Configuring a Database](#) on page 104 in the *HP OpenView Select Access 6.1 Installation Guide*.

To make the auditing of Select Access components more targeted, you can also create reports from the Secure Audit server's database or file output, as well as configure email alerts for more severe events that require immediate notification. For details on creating alerts and generating reports, see [The Alert Notification Decision Point](#) on page 165 and [Creating and Viewing a Report with the Report Viewer](#) on page 249 in the *HP OpenView Select Access 6.1 Policy Builder Guide* respectively.

## Analyzing Your Redundancy Policy

Redundant systems can have different goals, ranging from increasing performance to increasing fault tolerance. Different Select Access components support some, if not all, of these goals via a system of replication. There are two different meanings of replication, depending on the component:

- *Replication of directory data:* A mechanism that automatically copies data from a master directory server to a slave server.
- *Replication of software components:* A mechanism that requires you to manually install duplicate Select Access components on different areas of your network.

### How do you increase the performance of Select Access components?

Queries can be processed more quickly when Enforcer plugins do not have to wait for a specific Policy Validator to become available. You can increase the performance of components by configuring replicated Policy Validators for load-balancing. Load-balancing is a system whereby load is evenly distributed among a redundant pool of Policy Validators. For high volume networks, load-balancing is an important aspect for increasing Policy Validator availability as well as increasing performance of your Select Access-protected network.

To deploy Select Access such that it supports load balancing:

- [Create a Validator pool](#): Do this by installing multiple Policy Validators on different areas of your back-office network to create a list of Validators that can share network load.



If you have a group of Policy Validators, the RSA algorithm-based key needed to validate Select Access, cookies must be shared with other Policy Validators. As a result, it must be published to the Policy Store. This ensures that identities do not have to reauthenticate because the required key to validate cookies was not published.

To share the key, ensure that you check the **Share key with other Validators** box in the Policy Validator **Secure Identity Credentials** setup screen. Note that this screen only appears when you do a **Custom** setup.



Always install all Policy Validators on the same network as your other back-office systems. The firewall you use to protect these systems needs to also protect Policy Validators from attack.

For details on how to configure redundant Policy Validators, see [Chapter 7, Configuring the Policy Validator](#), in the *HP OpenView Select Access 6.1 Installation Guide*.

- [Configure your Enforcer plugins](#) so they know to distribute queries among a group of redundant Policy Validators, rather than use one specific Policy Validator. For details on how to configure Enforcer plugins to support round-robinning of Policy Validators in a Policy Validator pool, see [Chapter 8, Configuring the Enforcer Plugins](#), in the *HP OpenView Select Access 6.1 Installation Guide*.

## How do you increase the fault tolerance of Select Access components?

You can improve the fault tolerance of Select Access-protected networks by replicating elements for failover. This ensures that data and components are always available to Select Access clients in the event of a software, hardware, or network fault.

To deploy Select Access such that it supports failover:

- [Replicate directory data to multiple directory servers](#). This ensures data is always available to Select Access clients in the event of a software, hardware, or network fault. For details on how to integrate this functionality with your Select Access deployment, see [Chapter 2, Directory Server Integrations](#), in the *HP OpenView Select Access 6.1 Installation Guide*.
- [Configure your Enforcer plugins](#). Create a list of Policy Validators, so Enforcer plugins know:
  - How long to wait for a Policy Validator or how many times to retry it before it is deemed unavailable to process a query
  - Where to direct queries if a Policy Validator is considered to be unavailable

For details on how to configure Enforcer plugins to support failover, see [Chapter 8, Configuring the Enforcer Plugins](#), in the *HP OpenView Select Access 6.1 Installation Guide*.

- [Physically configure multiple Policy Validators](#), so they know to which directory servers to failover to. Install Policy Validators on different areas of your back-office network. If you have replicated all or parts of your directory data, you need to further configure Policy Validators to support failover of directory servers.



Always install all Policy Validators on the same network as your other back-office systems. The firewall you use to protect these systems needs to also protect Policy Validators from attack.

For details, see [Chapter 7, Configuring the Policy Validator](#), in the *HP OpenView Select Access 6.1 Installation Guide*.

## Analyzing Your Directory Topology

Most directory servers allow you to design a distributed directory in which identity data is spread across multiple physical directory servers. The benefit of distributing identity data among distributed servers is that you improve the performance of the directory system as well as other client applications that make use of that data.

### How does a distributed directory affect Select Access?

If you have a distributed directory topology, you likely have set up a network of referrals among these different servers. Referrals allow you to hide the functional details of your distribution by allowing servers to redirect queries to the appropriate data location. This process of referrals makes your directory topology seem as if it were centralized on one machine.

A distributed topology affects your deployment in that it requires you to check the type of referrals you use. Select Access supports referrals. If you use referrals, ensure that the referral syntax is compatible with Select Access's referral support. For details on deploying Select Access with a directory system that uses referrals, see [Chapter 2, Directory Server Integrations](#), in the *HP OpenView Select Access 6.1 Installation Guide*.

## Analyzing Your Affiliates or Partners

Select Access supports trusted servers and federated partnerships, which avoids the need for reauthentication when an identity tries to access resources that are hosted by an affiliate organization. This creates an interoperable mechanism for passing credentials and other related information among servers belonging to partnering organizations—even if they have their own authentication and authorization systems.

### How do I take advantage of federation with my Select Access deployment?

There are two main issues to keep in mind:

- You and your federation partners must:
  - Exchange unique identifiers, connection parameters, and assertion processing details.
  - Agree on what attribute namespaces you require.
  - Determine which servers are responsible for sending and/or receiving authenticated identities to partner sites.

Without knowing these details in advance, you are not able to configure your federation server.



- The Select Access Federation server is a standalone component that you can install with Select Access or separately from it. Consequently, it can run on either the same host machine as the Validator and/or the Web server or on a different host altogether. The Federation server communicates directly with the Validator, so that it can send and retrieve the information it needs. It communicates with the other federated servers on the network with which it has a relationship.

## Analyzing Your Potential for Growth

Select Access is scalable: as the number of identities and resources requiring policy increase, the demands on your existing Select Access components increase accordingly. Select Access's componentry allows your access management deployment to scale according to changes in volume.

### How do I roll out new components in stages?

Depending on your current size, there can be varying combinations of new components you need to:

- **Monitor your loads closely.** If you start reaching upwards of 75% of your capacity, consider installing additional Policy Validators to maintain suitable performance levels. Adding more Policy Validators helps reduce the load. There is no limit to the number of additional Policy Validators you can use within a given system. Each query an Enforcer plugin makes can go to any Policy Validator and get the same answer.
- **Find a suitable balance** between the number of identities and the number of security administrators. As your organization grows, you may find the need to delegate administration to remote security administrators. For example, you could have one delegated security administrator for every department of a company that looks after policy creation.
- **Install a new Enforcer plugin** for each new resource server you add, and add those resources to the Policy Matrix's Resource Tree. Ensure you make this part of your deployment procedure for new servers. For details, see [Chapter 8, Configuring the Enforcer Plugins](#), in the *HP OpenView Select Access 6.1 Installation Guide*.
- **Distribute directory data** so you can scale your directory among multiple directory servers. A distributed directory can:
  - Adapt more quickly, when identity numbers change over time
  - Fail over, if a master directory server fails
  - Balance load, if demands on a given replicated directory server exceed the CPU capacity of the machine hosting it.

For each new branch of directory data you add, you also need to configure the corresponding branch of the Identities Tree in the Policy Matrix. For details, see [Chapter 3, Building your Identities and Resources Trees](#), in the *HP OpenView Select Access 6.1 Policy Builder Guide*.

## Analyzing your Content Servers and Third-Party Technologies

Web servers and other third-party content servers help your organization to thrive on the Web. Your content system may include any combination of:

- Dedicated Web servers

- Virtual Web servers
- Application servers
- Portal content and portal servers

## How do application or portal vendors affect my deployment?

Select Access supports certain application servers and portal vendors. If Select Access supports a vendor, you can integrate Select Access with this third-party technology to ensure that its resources are Select Access-protected. To determine which third-party products you can integrate with, check `<install_path>/docs/solutions` for the list of technology-specific integration documents available to you.

## Deployment Scenarios

How you deploy your version of a Select Access access management solution depends on the size and nature of your organization. [Table 2](#) provides two general examples of how Select Access can be configured. You can extend these examples into your specific environment and use them as a starting point for developing your own access management deployment plan.

**Table 2 Example Select Access Deployment Scenarios**

Disbursement	Details
<p>A <i>single machine</i> that has most Select Access components installed on it, with the exception of the Enforcer plugins and a directory server.</p> <p>This example:</p> <ul style="list-style-type: none"> <li>• Is the simplest of all Select Access deployment scenarios</li> <li>• Is typically used by mid-size organizations</li> <li>• Takes advantage of only some of Select Access’s features</li> </ul>	<p><a href="#">Centrally Located Deployment by a Mid-Sized Manufacturer on page 23</a></p>
<p><i>Several geographically dispersed</i> machines that have a single Select Access component installed on them, and the topology of the directory system is replicated and globally dispersed.</p> <p>This example:</p> <ul style="list-style-type: none"> <li>• Is the most advanced of all Select Access deployment scenarios</li> <li>• Is typically used by large multi-national enterprises</li> <li>• Takes full advantage of Select Access’s features and componentry</li> </ul>	<p><a href="#">Fully Distributed Deployment by a Multi-National Enterprise on page 25</a></p>

## Centrally Located Deployment by a Mid-Sized Manufacturer

Ball Brothers Manufacturing (BBM), a ball bearing manufacturer, is a mid-size company that consists of 600 employees, with a single office in Flint, Michigan. BBM recently purchased a single instance of iPlanet v 5.0 directory server, and wanted to extend it by purchasing Select Access to manage access of network resources, much of which is of a highly sensitive nature.

Other significant details include:

- All of BBM's identity data is centrally managed by a single directory administrator, who also takes on the role of security administrator. If possible, the security administrator would like to work from her home office, due to lengthy commute times.
- BBM has little knowledge of PKI, and has no plans to invest in this kind of infrastructure.
- BBM recently launched an Internet site that is intended to facilitate work processes for their suppliers and simplify ordering for customers.
- BBM has a limited IT budget so existing hosts must be used wisely.
- BBM does not allow anonymous access and requires that new and unknown identities register to the directory server. Known identities must authenticate via password.

### Their Select Access Solution

Based on their business and IT environment, BBM's best deployment is one that is small and centrally located. Therefore, deployment of BBM's components are installed among a few host computers—hosts that also host other applications. This solution requires minimal network topology and firewall configuration planning, and does not require all of Select Access's components.

In this scenario, BBM likely has:

- A single firewall that divides its network into public and private zones
- A single host that includes:
  - A directory server that holds all identity and policy data
  - The Administration Server
  - The Policy Validator
- Another computer that hosts only an Enforcer-protected Web server

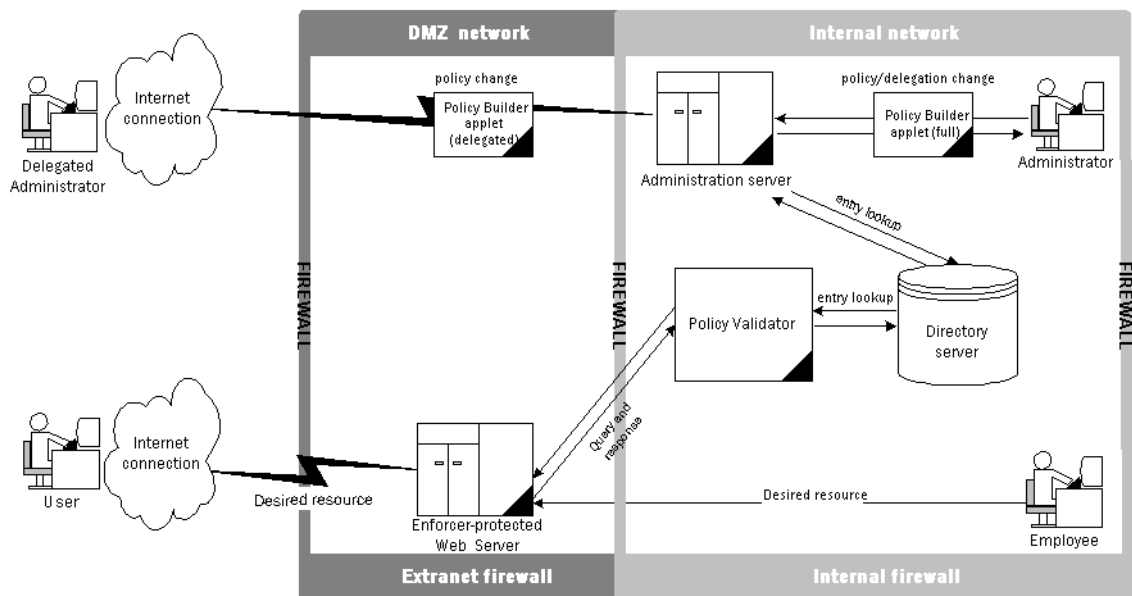
## Location of Select Access Components

Because BBM is a mid-size organization, it is not likely to require all of the robust features and components included with Select Access. Like most organizations of this nature, BBM has divided its network into two zones. Table 3 summarizes on which network zone it plans to install Select Access components.

**Table 3 Deploying Select Access on a localized network**

Network Zone	Components Hosted
DMZ network	<ul style="list-style-type: none"> <li>A single Enforcer-protected Web server accessed over the extranet</li> </ul>
Internal network	<ul style="list-style-type: none"> <li>A single Policy Validator</li> <li>The Administration server/ Policy Builder</li> <li>The directory server that holds all identity, policy, and configuration information Select Access uses</li> </ul>

Figure 1 illustrates the topology of this deployment.



**Figure 1 Localized Select Access Deployment**

## Component Configuration

After installing each component in the appropriate physical location, BBM accepts all of Select Access's setup defaults by performing a **Typical** setup for all components. A Typical setup is generally performed when you do not need to customize configuration or enable special features. Therefore, the only configuration values BBM provides are those for host and server names and locations.

## Additional Features Used

After all components are up and running, BBM still needs to configure Select Access to take advantage of the following features:

- Password and registration authentication support, which also includes taking the corresponding form templates that were installed with Select Access and customizing them
- Identity profiles so suppliers and/or customers can update their own profile info
- Password policies to match BBM's existing corporate policy
- The delegated administration applet so the full administrator can determine and set delegated administration policies that allow delegated identities to administer other identities and/or policies remotely

## Fully Distributed Deployment by a Multi-National Enterprise

Magellan Financial International (MFI), a financial services provider, is a large multi-national enterprise that consists of thousands of employees worldwide, with regional offices in North America, Europe, and Southeast Asia. MFI has legacy back-office systems on different platforms that include Windows 2000, Linux, and Solaris. To help them manage their employees, as well as their vast network of agents, brokers, and clients, MFI purchased several licences for the Siemens DirX directory server a year ago. Since then, it has successfully:

- Logically distributed directory entries among all regions
- Used replication and referrals to ensure 100% availability and improve throughput of data

Other significant details include:

- Due to the amount of identity data that must be managed across multiple locations, MFI has recently created a new role of security administrator. There is one senior security administrator to manage the process on a global scale and several security administrators to whom access management is delegated.
- MFI has recently purchased UniCERT PKI to further shield their systems from attack, and to facilitate the authentication of their identities.
- MFI has recently launched an extranet that is intended to improve relationships with their network of agents and brokers and give them the knowledge they need to give sound financial advice in their region. The extranet also allows clients to view or modify their portfolio as needed.
- MFI has a large IT budget. One of the CEO's mandates is to continue to use any technology available to:
  - Reduce overhead costs
  - Build online relationships with agents, brokers, and clients
- MFI does allow anonymous access. However, a more robust online experience requires that new and unknown identities authenticate to the system via registration, password-based authentication, or, for more sensitive resources, certificate-based authentication. The executive team is also using SecurID to access legal, acquisition, and financial resources that are only available on a "need-to-know" basis.

- MFI has also started negotiations to affiliate with a leading insurance provider so it can offer additional services to its clients. It plans to close the deal within a few months, but is still unsure how to avoid having identities reauthenticate as they move between the two corporate sites.
- MFI's VP of IT also requires that all major security schemes be audited to watch for possible security issues, and to be notified when any security application has problems at run time.

## Their Select Access Solution

Based on their business and IT environment, MFI's deployment is best served by a large scale, full-featured configuration. Therefore, deployment of components would be distributed among multiple machines. This solution requires a lot of network topology integration and firewall configuration planning, which needs to take full advantage of Select Access's componentry.

In this scenario, MFI likely has:

- Firewalls that control traffic between network zones and components. You need a firewall for your extranet and Internet traffic, and a firewall for your intranet and back-office traffic. For details, see [Location of Select Access components](#) on page 27.



If MFI had a NAT firewall, they would also have to map network addresses for Enforcer plugin and Policy Validators so they could communicate over this firewall successfully. They can configure this mapping when setting up their Enforcer plugins. For more information, see the *HP OpenView Select Access 6.1 Installation Guide*.

- Multiple directory servers:
  - One for each regional office, which holds the identity data for that region. These directory servers also use a system of smart referrals to redirect third-party application clients to the corresponding database server location.
  - One for the Select Access Administration server and Policy Store, which holds the configuration information and policy data.
  - Several replicas of the original servers to protect against possible server or network faults.
- Several Enforcer-protected Web servers hosted on their own machines and on different platforms.
- An administration server to serve up both the Policy Builder applet and the Delegated Administration applet. This allows administrators who have had administration entitlements delegated to them to remotely configure access policies to their segment of identities.
- A validator pool, consisting of three Policy Validators. A computer in each regional office hosts these Policy Validators.
- A federated Web server, which allows MFI to exchange identity credentials with partnering sites to offer their identities a seamless Web experience.
- A Secure Audit server to coordinate the logging activity among Select Access components, and simplify the generation of reports by collecting data from geographically dispersed components. The Secure Audit server is configured to output to a JDBC-compliant database that has been set up to work with Select Access.

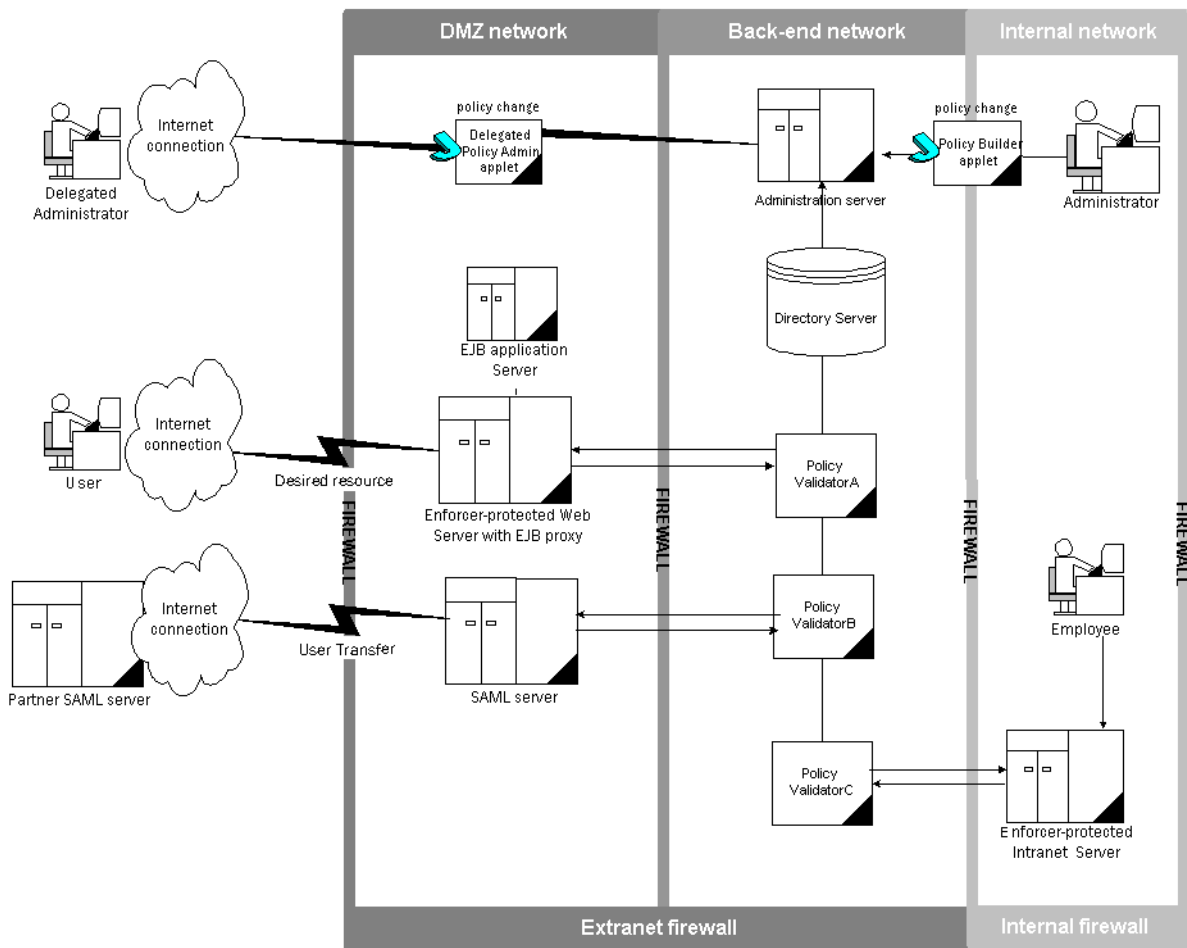
## Location of Select Access components

Because MFI is a multi-national organization, deployment options are quite advanced. Like most organizations of this nature, MFI has divided their network into three zones. [Table 4](#) shows that there are three network zones that fully distributed organizations employ.

**Table 4 Deploying Select Access on a distributed network**

<b>Network Zone</b>	<b>Components Hosted</b>
DMZ network	<ul style="list-style-type: none"><li>• Any Enforcer-protected Web servers accessed over the Internet</li><li>• A Federated server</li></ul>
Back-end network	<ul style="list-style-type: none"><li>• Policy Validators</li><li>• The directory server that holds all identity, policy, and configuration information used by Select Access</li><li>• The Administration Server (and Policy Builder applet)</li></ul>
Internal network	<ul style="list-style-type: none"><li>• Any Enforcer-protected servers that host internal systems or applications</li></ul>

[Figure 2](#) illustrates the topology of this deployment.



**Figure 2 Fully Distributed Select Access Deployment**

## Component Configuration

Because of the complexities of this deployment, MFI needs to customize its configuration of Select Access components. This allows them to tweak their installation to allow for their unique needs. MFI would not perform a **Typical** setup on any of their components. Instead, all components need to be customized.

## Additional Features Used

After all components are up and running, MFI still needs to configure Select Access to take advantage of the following features:

- Password, certificate, and registration authentication support, which also includes taking the corresponding forms templates that were installed with Select Access and customizing them
- Identity profiles so clients can update own profile info
- Password policies to match MFI's existing corporate policy
- Full use of the Report Viewer to create reports from the JDBC-compliant log to which the Secure Audit server outputs



# 3 Installing Select Access

Because HP employs an InstallAnywhere installer, Select Access is as simple to install as it is to configure. This chapter provides an overview of how to install the Select Access components on your network.

## Chapter Overview

This chapter includes important topics on how to successfully install Select Access components (upgraded or new) on Windows and on Unix host computers. Topics in this chapter include:

- [Before You Begin: Available Install Options](#) on page 29
- [Upgrade Issues](#) on page 32
- [Running the Select Access 6.1 Installer](#) on page 34



Before installing Select Access, read [Chapter 2, Planning Your Rollout of Select Access](#). This chapter describes deployment options you can consider, depending on the size of your organization.

## Before You Begin: Available Install Options

Depending on which version of Select Access you are upgrading from, there are different procedures you need to follow, which vary in complexity. The scenarios that affect your installation include those described in [Table 1](#).

**Table 1 Different Deployment Scenarios**

Scenario	Details
<a href="#">A new install of Select Access.</a> Because you have never installed Select Access before, this installation is relatively straightforward. Few caveats apply.	<a href="#">Installing Select Access for the First Time</a> on page 30
<a href="#">An update/upgrade.</a> This means that you have a previous version of Select Access installed.	<a href="#">Upgrading from a Previous Version of Select Access</a> on page 30

## Installing Select Access for the First Time

With the addition of the installation wizard and Setup Tool, first-time installations of Select Access are relatively straightforward. What increases the complexity is how distributed your deployment is, how your directory architecture works, and how many components you need to install. Therefore, the procedure for first-time installations is limited to the steps outlined in [Table 2](#).

**Table 2 First-time Installations**

Step	Details
1 To help you understand installation and configuration options, analyze your network architecture.	<a href="#">Chapter 2, Planning Your Rollout of Select Access</a>
2 Depending on your directory server, you may need to modify its schema to ensure Select Access can upload it.	<a href="#">Chapter 2, Directory Server Integrations</a> , in the <i>HP OpenView Select Access 6.1 Network Integration Guide</i>
3 Install Select Access 6.1.	<a href="#">Running the Select Access 6.1 Installer on page 34</a>
4 Configure the components you installed.	<a href="#">Using the Setup Tool on page 57</a>

## Upgrading from a Previous Version of Select Access

Upgrading to this version of Select Access requires that you follow the steps outlined in [Table 3](#).

**Table 3 Upgrading from Previous Versions**

Step	Details
1 Check to see whether or not your directory server's schema requires any updates. You must update the directory server's schema before you upgrade to Select Access 6.1.	<a href="#">Schemas Requiring Manual Changes and Specific Integration Concerns</a> on page 19 in the <i>HP OpenView Select Access 6.1 Network Integration Guide</i>
2 If the platform you are running Select Access on also requires a platform upgrade, perform the platform upgrade first. Platforms that require upgrade include: <ul style="list-style-type: none"><li>— HP-UX 11 to HP-UX 11.23 PA-RISC</li><li>— RedHat Linux to Linux AS 3.0</li><li>— Solaris 8 to Solaris 9</li></ul>	Platform-specific documentation.
3 Make sure there are no pending workflow requests. Either reject or approve all the requests before installing the new version.	<a href="#">Administering Change Requests</a> on page 225 in the <i>HP OpenView Select Access 6.1 Policy Builder Guide</i>

**Table 3 Upgrading from Previous Versions (cont'd)**

<b>Step</b>	<b>Details</b>
<p>4 Upgrade to Select Access 6.1 by running the installer for this version. The following order is HP's recommend upgrade path for Select Access components:</p> <ul style="list-style-type: none"> <li>a Upgrade you Administration server first.</li> <li>b Upgrade all Policy Validators on your network.</li> <li>c Upgrade all Enforcer plugins on your network.</li> </ul> <p><b>Caution:</b> If administrators perform a cache refresh from the Policy Builder during the Policy Validator upgrade process, only the caches of upgraded Policy Validators are refreshed.</p> <p><b>Note:</b> As you deploy upgraded components gradually across your network, corporate resources will still be Select Access-protected.</p> <p><b>Note:</b> The Apache 2 Enforcer plugin supports standard Apache as well as Apache 2 servers. It also supports the IBM Apache server on Windows.</p> <p>For details, see <a href="#">Supporting IBM and Apache 2 Servers</a> on page 32.</p>	<p><a href="#">To run the installer in default mode on top of a previous install on page 44</a></p>
<p>5 If you have a SAML server installed, the installer will remove this component. As of this release, the SAML server is obsolete. As a result, you must remove all SAML-related data before Select Access 6.1 can be successfully installed and configured.</p> <p>You can instead replace this component with the HP OpenView Select Federation server.</p>	<p><a href="#">The Retirement of the SAML server on page 32</a></p>
<p>6 Reconfigure the components you upgraded and/or installed.</p> <p><b>Warning:</b> You must run the setup program after the upgrade. Because the Keytools crypto libraries have been replaced by the Bouncy Castle Crypto API, the Administration Server fails to start unless you reconfigure it.</p>	<p><a href="#">Using the Setup Tool on page 57</a></p>
<p>7 Reapply customizations you may have made to <code>index.html</code> files for Forms-based and Web-based administration.</p> <p><b>Note:</b> If you have not customized the 6.0 versions of these forms, ensure you delete them to avoid confusion in the future.</p>	<p><a href="#">Reapplying Index.html Customizations on page 32</a></p>

For any other additional upgrade issues, see the [Upgrade Issues](#) section that follows.

# Upgrade Issues

Be aware of the following issues when upgrading to this version from a version of Select Access prior to 6.1:

- [Supporting IBM and Apache 2 Servers](#) on page 32
- [The Retirement of the SAML server](#) on page 32
- [Installing the WSE Enforcer Plugin](#) on page 33
- [Manually Deleting Old Files on Unix](#) on page 34

## Reapplying Index.html Customizations

If you have customized the `index.html` files to support the Web-based and Form-based administration features in Select Access 6.0 or Select Access 6.0 with Patch 1, all previously existing files are backed up by renaming them in their respective directory. The following `index.html` files are affected:

- Delegated Administration
- Password Reset
- Self-Management
- Self-Registration

For example, the installer renames the old version of `<SA_install_path>/shared/jetty/policy_builder/WebAdmin/delegated_admin/index.html` to `<SA_install_path>/shared/jetty/policy_builder/WebAdmin/delegated_admin/index.html.backup`.

This allows you to refer to your old files should you want to reapply the customizations you have already made to the new index files. Note that in the case of Password Reset, Self-Management and Self-Registration, these files are now JSP pages.

HP recommends that you delete these backup files once you have reapplied former customizations to 6.1 files.

## Supporting IBM and Apache 2 Servers

The IBM HTTPD Enforcer plugin is no longer a separately installed plugin. Going forward, the Apache 2 Enforcer plugin protects IBM, standard Apache, and Apache 2 servers. This minimizes the number of code bases that need to be maintained.

### To upgrade to the Apache 2 Enforcer plugin

- 1 Uninstall either the IBM HTTPD Enforcer plugin or the Apache Enforcer plugin.
- 2 Reinstall the Apache 2 Enforcer plugin and configure it according to the requirements of the server you are protecting.

## The Retirement of the SAML server

SAML support has been retired from Select Access. A new standalone product now supports single sign-on and cross-domain identity management initiatives with partner sites. For more information, visit <http://openview.hp.com/products/slctfed/>.

## To understand how the retirement of the SAML server affects your deployment

- 1 The Select Access administrator is responsible for completing the following task in the Policy Builder before running the Select Access 6.1 installer:
  - Delete all SAML resources/services from the network tree.
  - Delete all SAML entries from the **Component Configuration** window.
  - Disable Select Auth when configured with a SAML authentication service
  - Delete all configured SAML authentication services.
  - Delete all SAML profile attributes.
- 2 The installer is responsible for the following tasks on installation of Select Access 6.1:
  - Stopping the SAML service.
  - Deregistering the server.
  - Removing all SAML-related files from the disk.
- 3 The Setup Tool will no longer allow you to configure the SAML server.
- 4 The Administration server will remove the following Policy Store entries:
  - `nxPolicyComponent=saml,ou=authenticationmethods,ou=securitypolicy`
  - `cn=saml_servers,cn=components,cn=configuration,ou=securitypolicy`
- 5 Transient user profiles created by the SAML server will remain in the Users Tree.

## Installing the WSE Enforcer Plugin

In order for the WSE Enforcer plugin to function, two assemblies, `InteropENFORCERLib.dll` and `WSEEnforcer.dll`, must be added to the .NET Framework Global Assembly Cache (GAC). When you select this plugin for installation, the Select Access installer searches for a file `gacutil.exe`, which it uses to automatically install the necessary assemblies during the installation process.

However, if the installer is unable to locate the file, then the required assemblies will not be installed automatically. In this case, you must manually add the assemblies to the GAC.

### To manually add the assemblies to the GAC

- 1 Click **Start**→**Programs**→**Administrative Tools**→**Microsoft .NET Framework Configuration**. The **.NET Framework Configuration** window opens.
- 2 In the left pane, click the **Assembly Cache** entry.
- 3 Add the WSE Enforcer plugin assemblies to the GAC. To add the assemblies:
  - a Click **Action**→**Add an Assembly to the Assembly Cache**. The **Add an Assembly** dialog box appears.
  - b Select the `Interop.ENFORCERLib.dll` and click **Open**.
  - a Click **Action**→**Add an Assembly to the Assembly Cache**. The **Add an Assembly** dialog box appears.
  - b Select the `WSEEnforcer.dll` and click **Open**.
- 4 Close the **.Net Framework Configuration** window.

## Manually Deleting Old Files on Unix

If you are upgrading Select Access from a previous release, certain files do not get removed when you uninstall the product. To do a clean upgrade, Linux and Solaris end users need to delete the following files from their system:

```
/usr/lib/libopenssl.so  
/usr/lib/libopenssl.so.0
```

HP-UX end users need to delete the following files:

```
/usr/lib/libopenssl.sl  
/usr/lib/libopenssl.sl.0
```

## Running the Select Access 6.1 Installer

Select Access takes full advantage of software modularity so that you can install various components on any combination of host computers—provided that the component supports that platform. As a result, the installer and Setup Tool are designed in such a way so as to facilitate the modularity across any distributed network.

- ▶ If you want to install an additional component on this host computer at a later time, you can rerun the installer and select the new component *in addition to* the other components you have already installed. You then only need to configure the new component, as the configuration information for existing components remains unchanged and intact.
- ▶ If you are installing Select Access on a Windows host computer, you must only install Select Access on an NTFS partition.

## Preinstallation Issues

Before you begin installing this version of Select Access—irrespective of your current situation—there are important sets of installation addenda for you to consider. Please take note of the following items and gauge their impact accordingly as you install the product.

- [The Importance of the Correct Administration Entitlements](#) on page 37
- [Multiple Versions of Select Access Sharing One Directory Server](#) on page 35
- [About the Entropy Gathering Daemon and Select Access](#) on page 35
- [Tuning HP-UX Performance Parameters](#) on page 35
- [About gzip on HP-UX](#) on page 36
- [Out of memory error when installing on HP-UX](#) on page 36
- [The Importance of the Correct Administration Entitlements](#) on page 37

## The Impact of Running Control Panel Applications

If you are uninstalling and/or installing or configuring Select Access components on a Windows host computer, ensure that you do not have the Services window—or any other Control Panel application—open. This open Control Panel application triggers conflicts that cause the installer and Setup Tool to behave abnormally.

## Multiple Versions of Select Access Sharing One Directory Server

HP does not support multiple Select Access software versions running from a single directory server. Select Access modifies your LDAP policy store when you upgrade your software, to upgrade to a new schema and support new features.

## About the Entropy Gathering Daemon and Select Access

If you have an Entropy Gathering Daemon (EGD) installed on your system, Select Access uses it to generate random data for SSL. Select Access looks for an EGD socket in the following locations:

- /var/run/egd-pool
- /dev/egd-pool
- /etc/egd-pool
- /etc/entropy

If the EGD socket cannot be found, Select Access uses its own internal mechanism to generate random data.

## Tuning HP-UX Performance Parameters

In order to improve the performance of Select Access on HP-UX, HP recommends tuning the kernel configuration. Some of the default parameters are not large enough for Select Access's needs.

Table 4 lists HP's minimum recommend parameter values. Ensure your system meets or exceeds these minimum recommended values.

**Table 4 Minimum Recommended HP-UX Parameter Values**

Parameter	Value
<b>Out of box parameters:</b> To ensure the successful installation of Select Access, you should change the following values.	
maxusers	512
nproc	2048
max_thread_proc	3000
nkthread	6000
nfile	4513
maxfiles	2048
maxfiles_lim	2048
ncallout	6000
maxdsiz	2063835136
<b>Other recommended values</b> To improve the performance of Select Access, you should change the following values.	
fs_async	0

**Table 4 Minimum Recommended HP-UX Parameter Values (cont'd)**

Parameter	Value
maxssiz	134217728
maxtsiz_64bit	1073741824
maxuprc	100
nflocks	200
ninode	2728
sema	1
semmap	1026
semmni	1024
semmns	1024
semmnu	90
semume	30
shmem	1
shmmax	1073741824
shmmni	1024
shmseg	500

## About gzip on HP-UX

When you run the setup program as root, `gzip`, a utility to unzip the Select Access installer, may not appear in your default `PATH`. By default, `gzip` is located in `/usr/contrib/bin`. If you cannot locate it, add the `gzip` path to the `PATH` as follows:

- 1 At the command line prompt, type `PATH=$PATH:/usr/contrib/bin`.  
These commands apply if you are using the `BASH` shell. If you are using another shell, find the appropriate commands for it.
- 2 Type `export PATH`
- 3 Type `which gzip`. The following path appears: `/usr/contrib/bin/gzip`
- 4 Run the installer.

## Out of memory error when installing on HP-UX

When installing Select Access on HP-UX, an out of memory error may sometimes be generated. If this occurs, you will need to adjust the `maxdsiz` parameter in the kernel configuration in the HP-UX System Administration Manager (SAM) to increase the size of the kernel.

To adjust the `maxdsiz` parameter

- 1 Start the System Administration Manager.
- 2 Double-click **Kernel Configuration**.



- 3 Double click **Configurable Parameters**.
- 4 Double click the `maxdsiz` parameter.
- 5 Change the value of `maxdsiz`. HP recommends a value of 2 063 835 136 to ensure that the installer does not run out of memory.
- 6 Exit the SAM, create a new kernel, and then reboot.

## The Importance of the Correct Administration Entitlements

On Windows, HP recommends that only administrators with local administration entitlements install the product. Otherwise, the installer cannot create the required registry entries.

On Unix, only run installers as root. This allows the installer to set up all the required symbolic links. The installer removes these links when you uninstall all or part of Select Access.

## Ensuring that the Administration server can Locate `printenv`

Before installing the Administration server on a Unix platform, you must ensure that the path to `printenv` is added to the root's default execute path. If you need to add this path to the execute path, do so as follows:

- 1 Determine the path to `printenv`.
  - On Solaris, it is usually located in `/usr/ucb`
  - On HP-UX or Linux, it is usually located in `usr/bin`
- 2 Add this path using the command appropriate for your shell. For example, on Solaris using the BASH shell, the command would be:

```
echo $PATH
/usr/sbin:/usr/bin

PATH=$PATH:/usr/ucb

export PATH
echo $PATH
/usr/sbin:/usr/bin:/usr/ucb
```

Once added, you can run the installer or Setup Tool.

## Running the Installer—a Mode Overview

HP allows you to run the Select Access 6.1 installer in two modes: Default mode (or GUI mode) or Console mode (on Unix only). If you are installing Select Access on a Unix host, Console mode is particularly useful to Unix end users who do not have X-Windows or VNC running on their system.



By running the installer in Console mode, you cannot use the Setup Tool to configure the components you install on the Unix host. For details, see [To configure a component installed by Console mode](#) on page 53.



If you leave the IIS Web service running during an installation, the installer automatically shuts it down as well as its dependencies (for example, FTP). However, while the Setup Tool automatically restarts the server, it does not necessarily restart all of IIS' dependencies. Following an installation, check to see that all IIS-related services are running again. If not, restart them manually.



If you are uninstalling, installing, upgrading, or configuring Select Access components on a Windows host computer, ensure that you do not have the Services window—or any other Control Panel application open. This open Control Panel application triggers conflicts that cause the installer and Setup Tool to behave abnormally.

## To run the installer in default mode on a clean host machine

- 1 Start the Select Access setup program by running the corresponding setup file from the root of the Select Access product CD:

- On Windows, enter the following command: `setup_win32.exe`

or

- On Unix, enter the following command: `./setup_<platform>`

Where `<platform>` is the Unix platform you are running on (that is, either `linux`, `solaris`, or `hpux`).



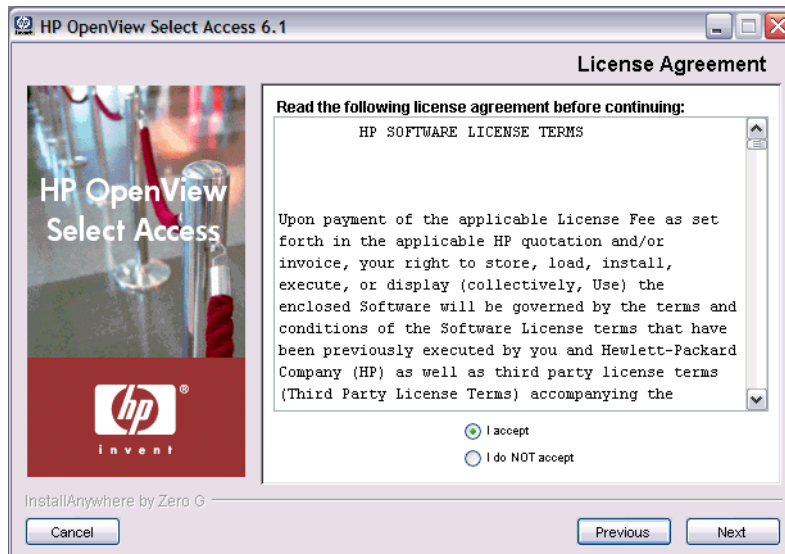
If you are uninstalling and/or installing or configuring Select Access components on a Windows host computer, ensure that you do not have the Services window—or any other Control Panel application open. This open Control Panel application triggers conflicts that cause the installer and Setup Tool to behave abnormally.

The installer extracts the installation files, then prepares the Select Access Install Wizard. When it has finished loading, the **Welcome to HP OpenView Select Access Installation** screen appears, as shown in [Figure 1](#).



**Figure 1** Welcome to HP OpenView Select Access Installation Screen

- 2 Click **Next**. The **License Agreement** screen appears.

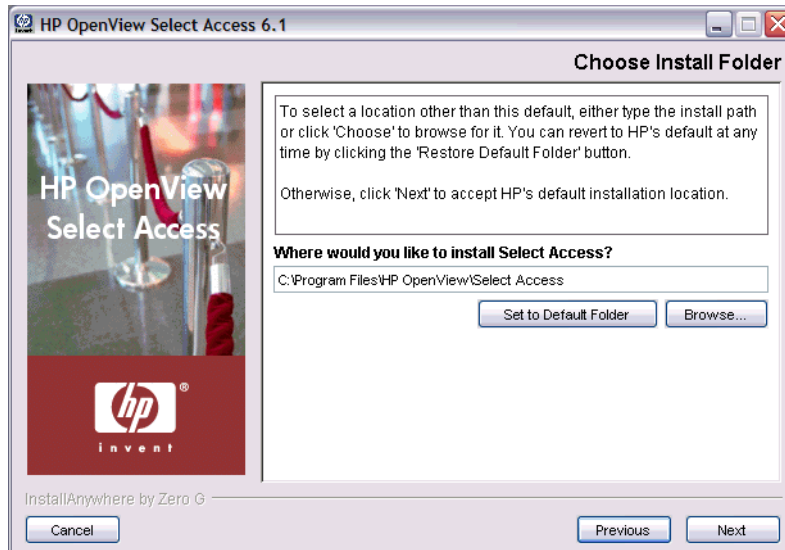


**Figure 2 License Agreement Screen**

- 3 Read the license agreement. When you understand and agree to the terms, click the **I accept** option and click **Next**.

➤ You cannot proceed to the next screen until you accept the terms of the license agreement.

The **Choose Install Folder** screen appears, as shown in [Figure 3](#).

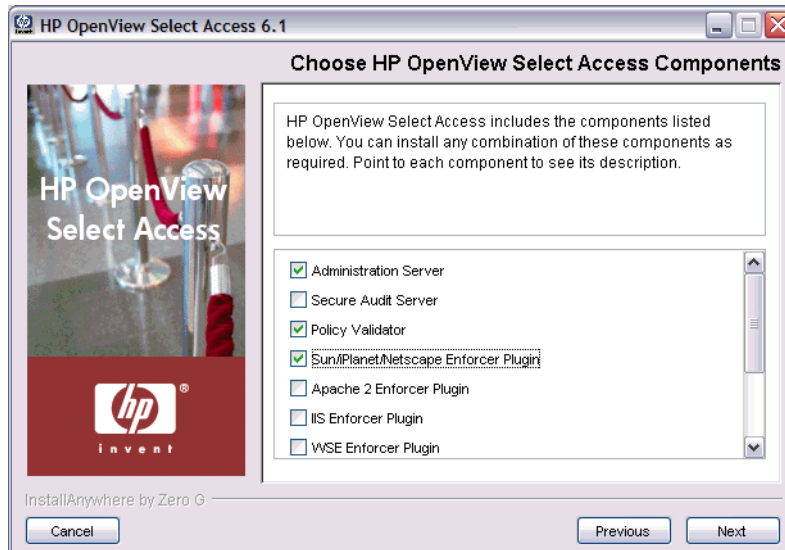


**Figure 3 Choose Install Folder Screen**

- 4 Select from one of the following configuration options:
  - If the default location is acceptable, proceed to [step 5](#).
  - If you want to select a different installation folder, click the **Choose** button, select a folder, then click **OK**. The new folder appears in the **Where would you like to install Select Access?** field.

- If you choose the wrong folder, click the **Restore Default Folder** button to restore the Select Access defaults.

5 Click **Next**. The **Choose HP OpenView Select Access Components** screen appears.



**Figure 4 Choose HP OpenView Select Access Components Screen**

6 Select which components you want to install by checking the corresponding box for that component.

You can install any combination of the following components on a single computer. Component availability depends on the installation platform. For more information, see *Platform Availability* on page 9.

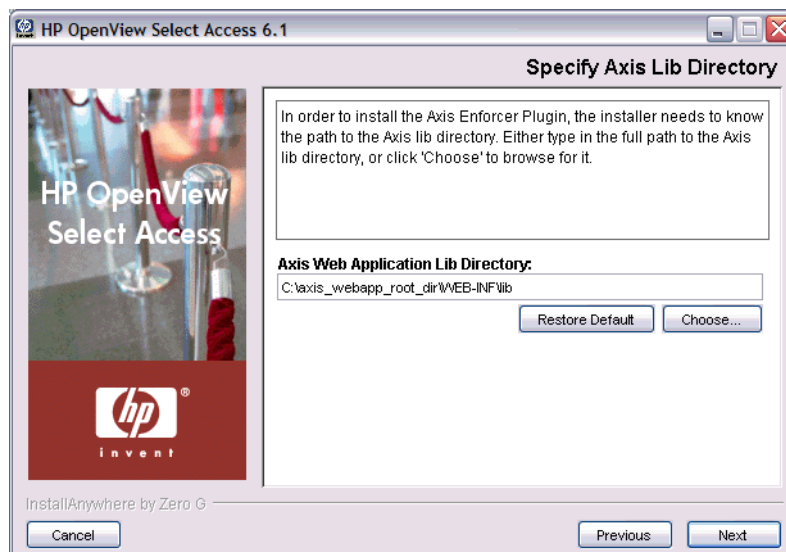
**Table 5 Select Access Components**

Plugin	Description
<b>Administration server</b>	Select Access’s Web server-based component that conducts administrative functions that include: component configuration, SSL certificate generation and management, and policy data administration. <i>Note:</i> Only install a single instance of the Administration server on your network. If your host computer fails, only then consider installing a new one. For details, see <i>Failing Over to Another Administration server</i> on page 86.
<b>Secure Audit server</b>	Select Access’s log tool that collects and manages incoming log messages from components on a network.
<b>Policy Validator</b>	Select Access’s decision-making component. The Policy Validator evaluates Enforcer plugin queries to determine if a user is allowed or denied access.
<b>Sun/Netscape/iPlanet Enforcer plugin</b>	Select Access’s decision-enforcement component for the Sun ONE (formerly iPlanet) Web server.
<b>Apache 2 Enforcer plugin</b>	Select Access’s decision-enforcement component for the Apache Web server. This component is also used by the IBM HTTPD Web server.

**Table 5 Select Access Components**

Plugin	Description
<b>IIS Enforcer plugin</b>	Select Access's decision-enforcement component for the IIS Web server. <b>Note:</b> When installing the IIS enforcer plugin, Select Access stops all affected services on IIS (for example the Web Server and the FTP server). However, if after configuring the IIS Enforcer plugin you allow Select Access to automatically restart IIS, only the Web server is restarted. Ensure you manually restart all services when you are done installing and configuring your IIS Enforcer plugin.
<b>WSE Enforcer plugin</b>	Select Access's decision-enforcement component for .NET Web services. <b>Note:</b> The WSE Enforcer plugin is only available for installation if you have previously installed the Microsoft .NET Framework, the Web Services Enhancements 1.0 add-on, and the General Assembly Cache tool ( <code>gac_util.exe</code> ). For information on installing these components, refer to your .NET documentation.
<b>Axis Enforcer plugin</b>	Select Access's decision-enforcement component for Java Web services.
<b>Servlet Enforcer plugin</b>	Select Access's decision-enforcement component for any servlet engine.
<b>TCP Enforcer plugin</b>	Select Access's decision-enforcement component for Unix services configured in <code>Inetd</code> .

- 7 Click **Next**.
  - If you are installing the Axis Enforcer plugin, see step 8.
  - Otherwise, see step 10.
- 8 If you are installing the **Axis Enforcer plugin**, the **Specify Axis Lib Directory** screen appears, as shown in [Figure 5](#).



## Figure 5 Specify Axis Lib Directory Screen

- The installer installs the Axis Enforcer plugin directly into the `Axis lib` directory. In order to do so, however, the installer must be able to correctly locate this directory. This screen allows you to specify the full path to the required directory.

In the **Specify Axis Lib Directory** screen, either type the path to the root Axis directory or click the **Choose** button to browse for it. The new directory appears in the **Axis Web Application Lib Directory** field.

- ▶ The path you configure must already exist. The installer does not allow you to specify a non-existent location.
- ▶ If you mistakenly changed the default location, click the **Restore Default** button to restore the Select Access default.

- Click **Next**. The **Pre-Installation Summary** screen appears, as shown in [Figure 5](#).



**Figure 6 Pre-Installation Summary Screen**

The **Pre-Installation Summary** screen creates a digest of the following installation information you provided to this point:

- The name and version of the product (that is, HP OpenView Select Access 6.1)
- The install path of Select Access.

On Windows, the default install path is:

```
C:\Program Files\HP OpenView\Select Access
```

On Unix, the default install path is:

```
/opt/OV/SelectAccess
```

- The folder that holds the program shortcuts for the Select Access administration tools.
- The Select Access components you selected to install on this computer.
- The installation location of the Java Virtual Machine that the Select Access Install Wizard has automatically installed. The Java Virtual Machine is required to run both the maintenance program as well as Select Access components—with the exception of the Policy Validator and the Enforcer plugins.

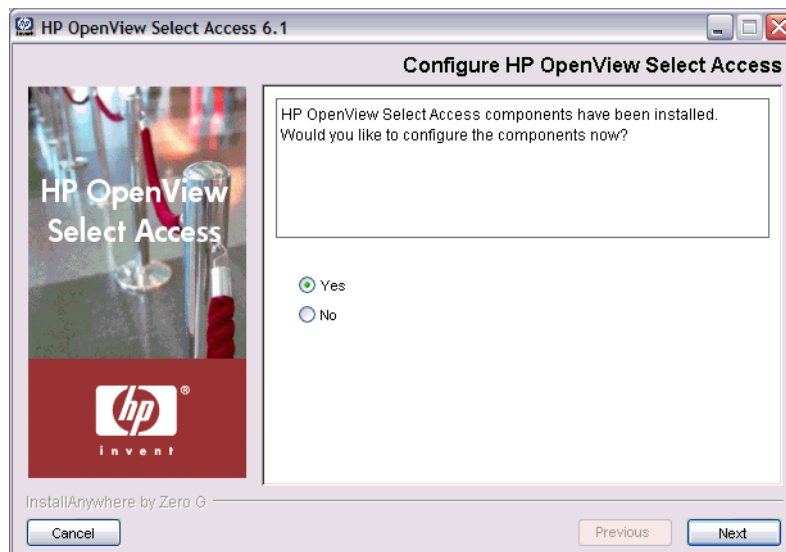
- The amount of disk space required for the components you selected to install. If the disk space required exceeds what is available on this computer, free up space or adjust what you are currently intending to install.
- 11 Review this information. If your installation details are acceptable, click **Install** to begin the installation.
- ▶ If you want to make changes, click **Previous** to change the install settings as required.

The **Installing HP OpenView Select Access 6.1** screen appears and outlines the installation progress of the components you selected to install.



**Figure 7 Installing HP OpenView Select Access 6.1 Screen**

- 12 On completion, the Select Access Install Wizard prompts you to decide whether you want to configure the components the wizard has just installed:
- Choose **Yes** to configure those components now.
  - Choose **No** to configure those components later.



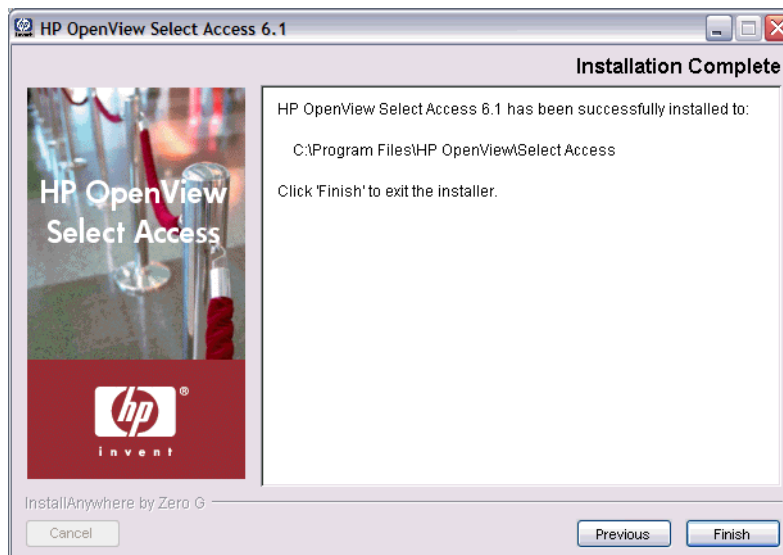
## Figure 8 Configure HP OpenView Select Access Screen

### 13 Click **Next**.

- If you selected **Yes** in the previous step, a **Please Wait** screen appears while the Installer loads the Setup Tool. When the Setup Tool has loaded, the **Welcome to HP OpenView Select Access Setup** screen appears. Use the Setup Tool to configure the components you just installed as needed. For details, see [Chapter 4, Configuring Select Access](#).
- If you selected **No** in the previous step, you have finished the install procedure.

▶ You must configure your components before you can start them. The Administration server must be configured before all other Select Access components.

### 14 When you are finished installing and/or configuring Select Access components, the **Installation Complete** screen appears.



## Figure 9 Installation Complete Screen

### 15 Click the **View Release Notes** box if you want to read the *HP OpenView Select Access 6.1 Release Notes* before continuing.

### 16 Click **Finish** to complete the installation of the product. The installer then:

- Creates/modifies a global configuration file called `selectaccess.conf` in your installation directory root.
- Cleans up all temporary installation files.

## To run the installer in default mode on top of a previous install

### 1 Start the Select Access setup program by running the corresponding setup file from the root of the Select Access product CD:

- On Windows, enter the following command: `setup_win32.exe`
- or
- On Unix, enter the following command: `./setup_<platform>`

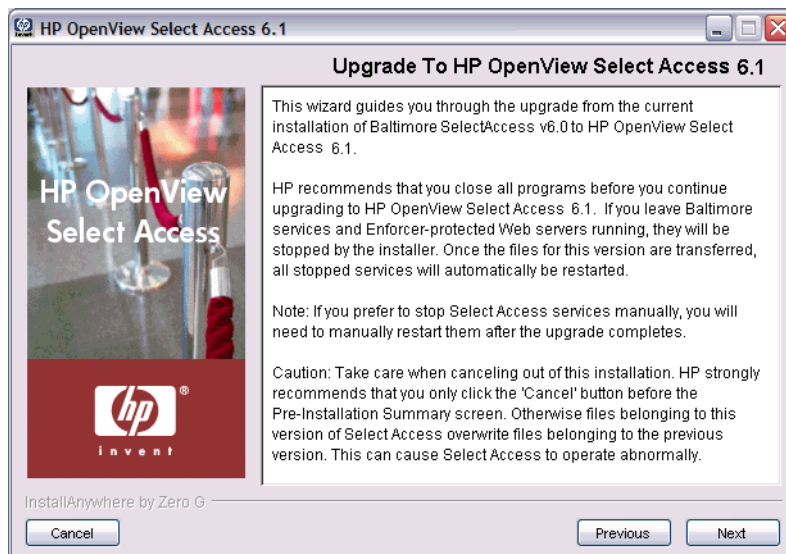


Where <platform> is the Unix platform you are running on (that is, either linux, solaris, or hpux).



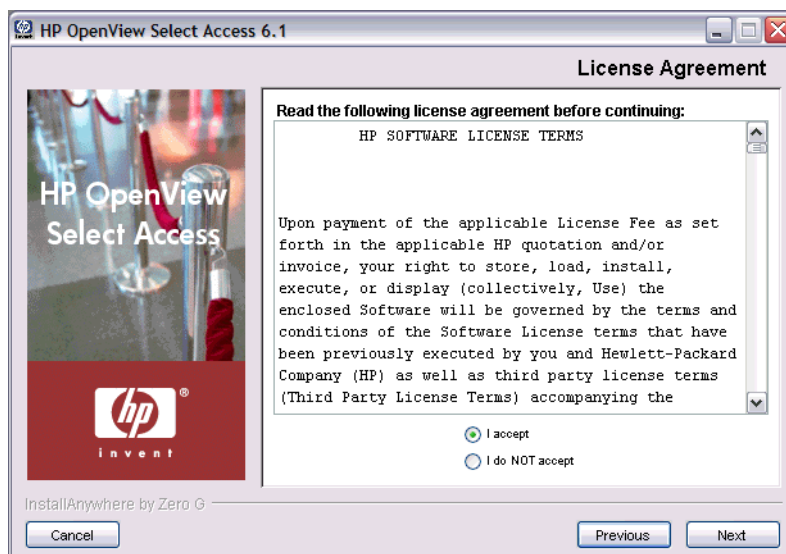
If you are uninstalling and/or installing or configuring Select Access components on a Windows host computer, ensure that you do not have the Services window—or any other Control Panel application open. This open Control Panel application triggers conflicts that cause the installer and Setup Tool to behave abnormally.

The installer extracts the installation files, then prepares the Select Access Install Wizard. When it has finished loading, the **Upgrade to HP OpenView Select Access 6.1** screen appears.



**Figure 10 Upgrade to HP OpenView Select Access 6.1 Screen**

2 Click **Next**. The **License Agreement** screen appears.

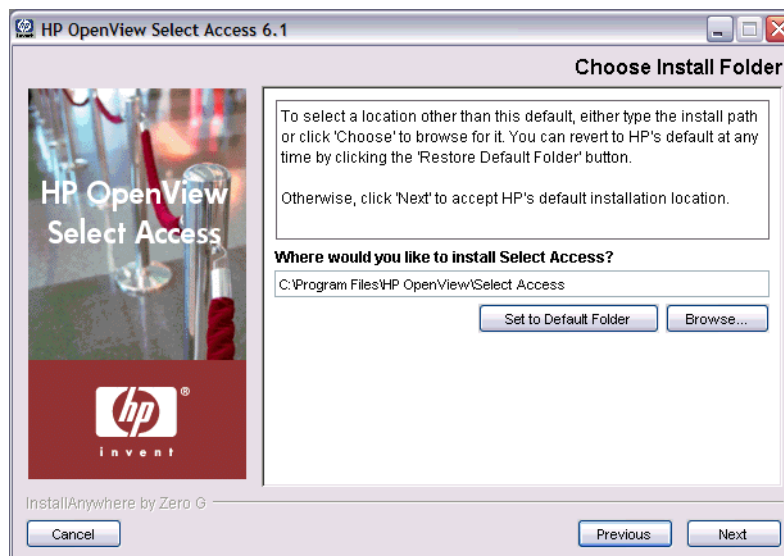


**Figure 11 License Agreement Screen**

- 3 Read the license agreement. When you understand and agree to the terms, click the **I accept** option and click **Next**.

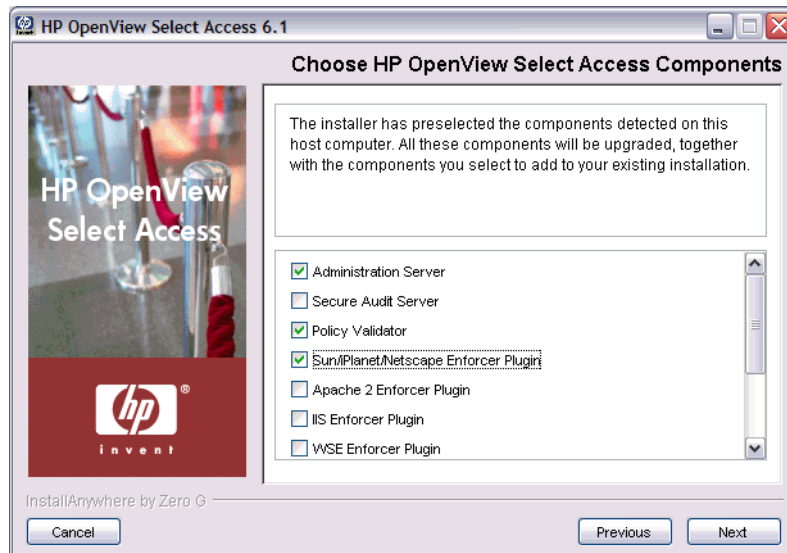
➤ You cannot proceed to the next screen until you accept the terms of the license agreement.

- If you are upgrading from Baltimore Select Access versions 5.0 or 5.1: the **Choose Install Folder** screen appears, as shown in Figure 12.
- If you are upgrading from HP OpenView Select Access 5.2 or 6.0: your new version is installed to the same directory as your existing installation. Skip to [step 5](#).



**Figure 12 Choose Install Folder Screen**

- 4 Select from one of the following configuration options:
  - If the default location is acceptable, skip to [step 5](#).
  - If you want to select a different installation folder, click the **Choose** button, select a folder, then click **OK**. The new folder appears in the **Where would you like to install Select Access?** field.
    - If you are upgrading from Baltimore Select Access versions 5.0 or 5.1, you cannot use the existing folder of that installation. When the upgrade completes, the previous version remains in the old location but is not functional. You can delete this installation if you choose; all configurations are backed up in the new installation location.
    - If you are upgrading from HP OpenView Select Access 5.2, the previous installation directory is renamed to C:\Program Files\HP OpenView\Select Access-5.2. You can delete this installation if you choose; all configurations are backed up in the new installation location.
  - If you choose the wrong folder, click the **Restore Default Folder** button to restore the Select Access defaults.
- 5 Click **Next**. The **Choose HP OpenView Select Access Components** screen appears.



**Figure 13 Choose HP OpenView Select Access Components Screen**

- 6 Select which components you want to additionally install by checking the corresponding box for that component.



Those components that were installed with the previous version must be reinstalled when you update, and are therefore automatically selected. You may choose to select any additional components.

You can install any combination of the following components on a single computer. Component availability depends on the installation platform. For more information, see *Platform Availability* on page 9.

**Table 6 Select Access Components**

Plugin	Description
<b>Administration server</b>	Select Access's Web server-based component that conducts administrative functions that include: component configuration, SSL certificate generation and management, and policy data administration.  <b>Note:</b> Only install a single instance of the Administration server on your network. If your host computer fails, only then consider installing a new one. For details, see <i>Failing Over to Another Administration server</i> on page 86.
<b>Secure Audit server</b>	Select Access's log tool that collects and manages incoming log messages from components on a network.
<b>Policy Validator</b>	Select Access's decision-making component. The Policy Validator evaluates Enforcer plugin queries to determine if a user is allowed or denied access.
<b>Sun/Netscape/iPlanet Enforcer plugin</b>	Select Access's decision-enforcement component for the Sun ONE (formerly iPlanet) Web server.
<b>Apache 2 Enforcer plugin</b>	Select Access's decision-enforcement component for the Apache Web server. This component is also used by the IBM HTTPD Web server.

**Table 6 Select Access Components**

Plugin	Description
<b>IIS Enforcer plugin</b>	Select Access's decision-enforcement component for the IIS Web server. <b>Note:</b> When installing the IIS enforcer plugin, Select Access stops all affected services on IIS (for example the Web Server and the FTP server). However, if after configuring the IIS Enforcer plugin you allow Select Access to automatically restart IIS, only the Web server is restarted. Ensure you manually restart all services when you are done installing and configuring your IIS Enforcer plugin.
<b>WSE Enforcer plugin</b>	Select Access's decision-enforcement component for .NET Web services. <b>Note:</b> The WSE Enforcer plugin is only available for installation if you have previously installed the Microsoft .NET Framework, the Web Services Enhancements 1.0 add-on, and the General Assembly Cache tool ( <code>gac_util.exe</code> ). For information on installing these components, refer to your .NET documentation.
<b>Axis Enforcer plugin</b>	Select Access's decision-enforcement component for Java Web services.
<b>Servlet Enforcer plugin</b>	Select Access's decision-enforcement component for any servlet engine.
<b>TCP Enforcer plugin</b>	Select Access's decision-enforcement component for Unix services configured in <code>Inetd</code> .

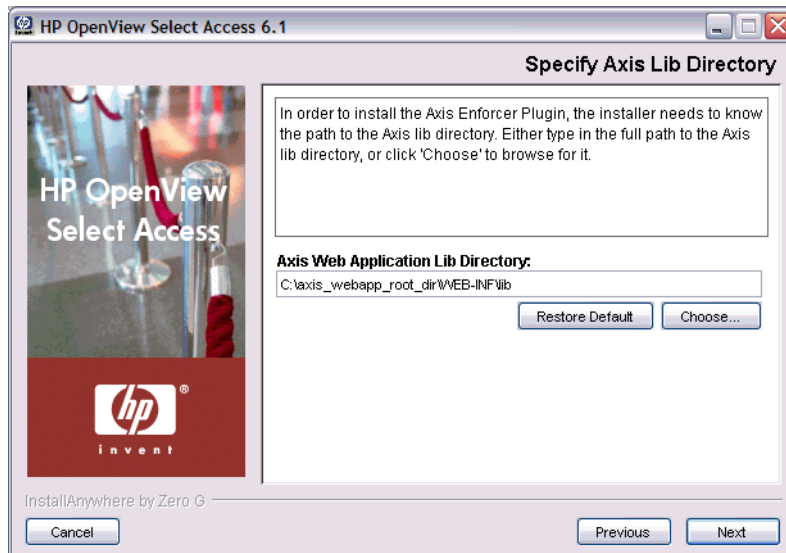
- 7 Click **Next**. If any Select Access services are running, the installer displays a warning message. Click **OK** to let the installer automatically stop them for you. Otherwise, stop them manually now.



On Windows, if you have any Enforcer-protected Web servers running, the installer also stops these servers. For the IIS Admin Service, all its dependent services are also stopped.

On Unix, the installer detects whether an Enforcer-protected Web server is running. However, you can only manually stop the Web servers. The installer cannot do this automatically on these hosts.

- 8 Click **Next**.
- If you are adding the Axis Enforcer plugin as part of your upgrade, the **Specify Axis Lib Directory** screen appears. Go to step 9.
  - If you are not adding the Axis Enforcer plugin, the **Pre-Installation Summary** screen appears. Go to step 10.
- 9 If you are adding the **Axis Enforcer plugin** as part of your upgrade, the **Specify Axis Lib Directory** screen appears, as shown in [Figure 14](#).



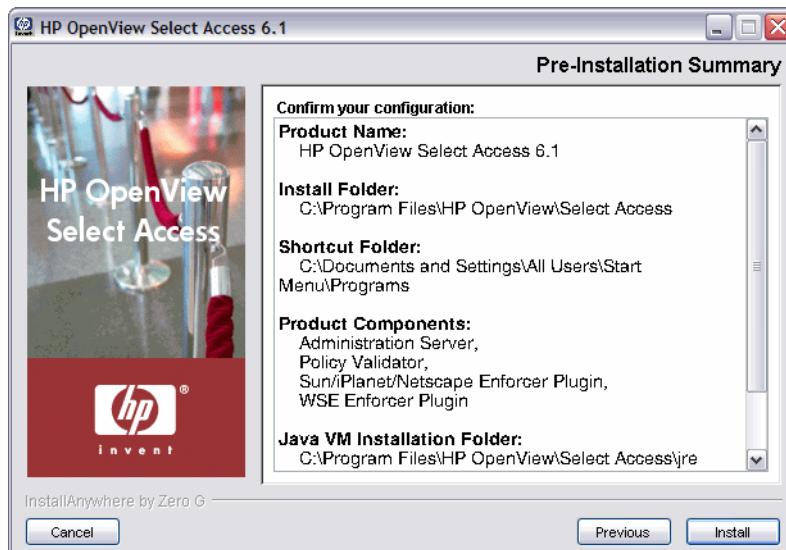
**Figure 14 Specify Axis Lib Directory Screen**

The installer installs the Axis Enforcer plugin directly into the Axis lib directory. In order to do so, however, the installer must be able to correctly locate this directory. This screen allows you to specify the full path to the required directory.

In the **Specify Axis Lib Directory** screen, either type the path to the root Axis directory or click the **Choose** button to browse for it. The new directory appears in the **Axis Web Application Lib Directory** field.

- ▶ The path you configure must already exist. The installer does not allow you to specify a non-existent location.
- ▶ If you mistakenly changed the default location, click the **Restore Default** button to restore the Select Access default.

10 Click **Next**. The **Pre-Installation Summary** screen appears, as shown in [Figure 15](#).



**Figure 15 Pre-Installation Summary Screen**

The **Pre-Installation Summary** screen creates a digest of the following installation information you provided to this point:

- The name and version of the product (that is, HP OpenView Select Access 6.1)
- The install path of Select Access.

On Windows, the default install path is:

```
C:\Program Files\HP OpenView>Select Access
```

On Unix, the default install path is:

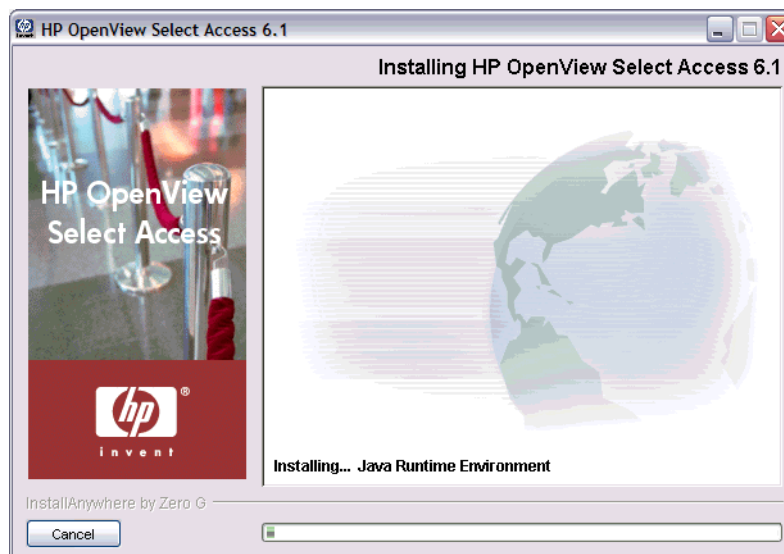
```
/opt/OV/SelectAccess
```

- The folder that holds the program shortcuts for the Select Access administration tools.
  - The Select Access components you selected to install on this computer.
  - The installation location of the Java Virtual Machine that the Select Access Install Wizard has automatically installed. The Java Virtual Machine is required to run both the maintenance program as well as Select Access components—with the exception of the Policy Validator and the Enforcer plugins.
  - The amount of disk space required for the components you selected to install. If the disk space required exceeds what is available on this computer, free up space or adjust what you are currently intending to install.
- 11 Review this information. If your installation details are acceptable, click **Install** to begin the installation.



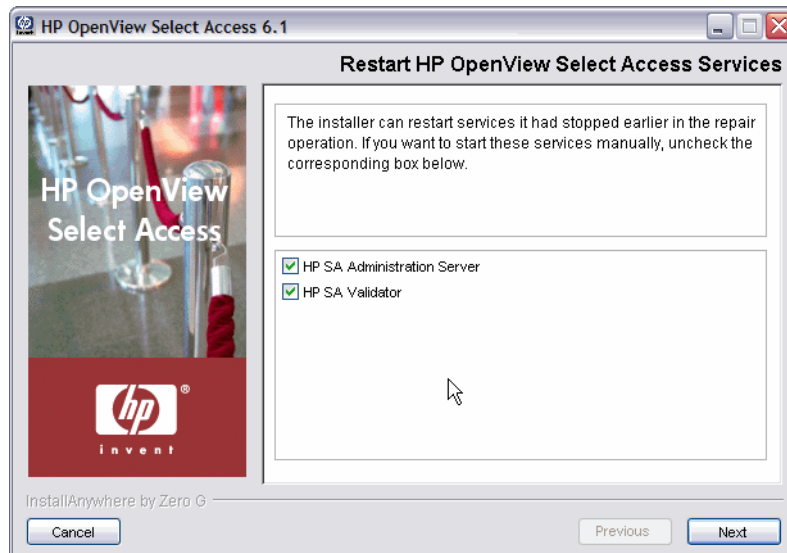
If you want to make changes, click **Previous** to change the install settings as required.

The **Installing HP OpenView Select Access 6.1** screen appears and outlines the installation progress of the components you selected to install.



**Figure 16 Installing HP OpenView Select Access 6.1 Screen**

- 12 On completion, if the installer automatically stopped services for you, the **Restart HP OpenView Select Access Services** screen appears.



**Figure 17 Restart HP OpenView Select Access Services Screen**

This screen prompts you to restart the components it had automatically stopped. To start a component, check the corresponding box beside the component's name.

- If you let the installer stop the IIS Admin Service, you are also prompted to restart it as well as any IIS dependent services that the installer also stopped. Depending on whether or not you installed these dependencies on the same host computer as the IIS Admin service, the IIS dependent services include: the World Wide Web Publishing service, the FTP Publishing service, the Simple Mail Transport Protocol (SMTP), and the Network News Transport Protocol (NNTP).
- ⚠ If a Select Access Administration server appears in the, HP recommends that you not restart it until you reconfigure it once the installer exits. You must reconfigure your Administration server because old Keytools crypto libraries have been replaced by the Bouncy Castle Crypto API.

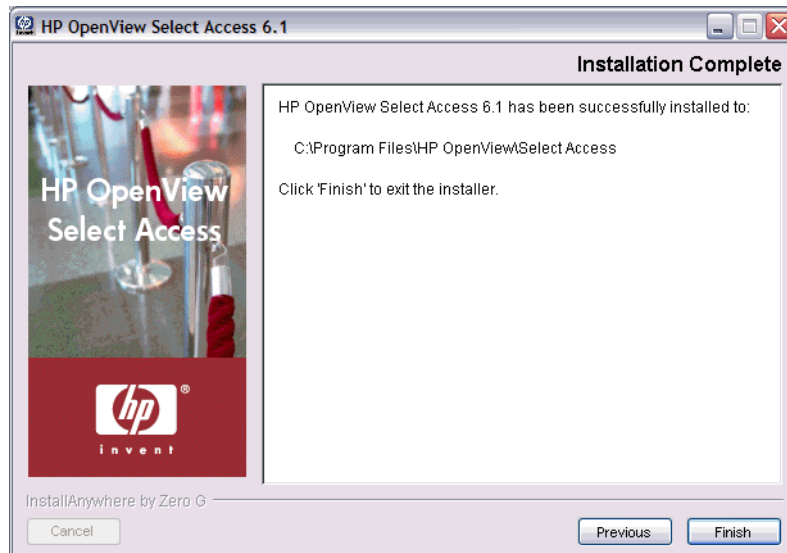
If you stopped your own services before repairing Select Access, skip to step 15. Ensure that you restart the services that you had stopped manually after you exit this wizard.

13 Click the corresponding option that determines whether or not you want to restart the host machine now:

- **Yes I want to restart now.**
- **No I will restart later.**

- You do not need to reconfigure your upgraded Select Access components unless you choose to do so.
- If you have not already restarted your services, do so now.

When you are finished installing and/or configuring Select Access components, the **Installation Complete** screen appears.



**Figure 18 Installation Complete Screen**

- 14 Click **Finish** to complete the installation of the product. The installer then:
  - Creates a global configuration file called `selectaccess.conf` in your installation directory root. For details, see [About the selectaccess.conf File](#) on page 56.
  - Cleans up all temporary installation files.

### To run the installer in Console mode on a clean host machine

- 1 From either the command line or command shell, change directories to your CD drive.
- 2 At the command prompt, run the corresponding Unix installer with the console command line argument. For example, on Solaris, you enter:

```
./setup_solaris -i console
```

where `-i console` tells the installer to run in console mode.

- ▶ Run installers as root. This allows the installer to set up all the required symbolic links. These links are removed when you uninstall all or part of Select Access.

- 3 At the `Welcome to HP OpenView Select Access Installation` prompt, press **Enter** to continue to the `License Agreement` prompt.
- 4 Read the license agreement. When you understand and agree to the terms, type **Y** at the `DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT?` prompt.
- 5 Define Select Access's installation folder by either:
  - Typing the *absolute* path to the folder you wish to use.
  - Pressing **ENTER** to accept Select Access's default folder. The default install path is:
 

```
/opt/OV/SelectAccess
```
- 6 Components are defined by a number:
  - 1- Administration Server
  - 2- Secure Audit Server



- 3- Policy Validator
- 4- Sun/iPlanet/Netscape Enforcer Plugin
- 5- Apache 2 Enforcer Plugin
- 6- Axis Enforcer Plugin
- 7- Servlet Enforcer Plugin
- 8- TCP Enforcer Plugin

Choose the components you wish to install by typing a comma-separated list that represents the components to be installed. For example, 1, 3 tells the installer to install the Administration server and the Policy Validator only.

- 7 The installer gives you a pre-installation summary for the components you defined. This summary provides a digest of the following installation information:
  - The name of the product (that is, Select Access).
  - The install path of Select Access.
  - The Select Access components you selected to install on this computer.
  - The installation location of the Java Virtual Machine that the Select Access Install Wizard has automatically installed. The Java Virtual Machine is required to run both the maintenance program as well as Select Access components—with the exception of the Policy Validator and the Enforcer plugins.
  - The amount of disk space that is required for the components you selected to install. If the disk space required exceeds what is available on this computer, free up space or adjust what you are currently intending to install.
- 8 If this information is correct, press **ENTER** to continue installing these components. If the information is not correct, type **back** to redefine which components you want to install.
- 9 When the installer is finished, an `Installation Complete` message appears. Press **ENTER** to exit the installer.

## To configure a component installed by Console mode

- 1 If the host is a Unix computer, `cd` to the `<install_path>/shared/setuptools` folder. and type the following command from any directory:

```
./setuptools
```



HP recommends that you set up the corresponding component on Windows or a Unix computer that has X-Windows or VNC.



Select Access requires that you configure the Administration server on the local host computer. Do not run the Setup Tool on another host and copy the configuration file to the host computer, as you might do for other Select Access components. This is because specific settings for the Administration server require that the Setup Tool run locally so the correct parameters are populated accordingly.

- 2 For all platforms, perform a **Custom** configuration for it. For details on running the Setup Tool, see [Chapter 4, Configuring Select Access](#).
- 3 In the component's **ID** setup screen, define the ID as one that correctly represents the target host.
- 4 Configure remaining screens as needed

- 5 Ensure that you do *not* do the following:
  - Choose to start the service automatically, by checking the corresponding box on the component's **Finish** setup screen.
  - If you are configuring a template for the Domino Enforcer plugin, do not integrate the Domino Enforcer plugin automatically by checking the corresponding box on the plugin's **Finish** setup screen. Instead, perform changes on your Web server's configuration files manually. For details, see [Chapter 3, Transparently Supported Web Server Integrations](#) in the *HP OpenView Select Access 6.1 Network Integration Guide*.
- 6 Click the **Finish** button to commit changes to both the Policy Store and a component's XML configuration file. This file is located in the `<install_path>/shared` folder.
- 7 Copy this XML configuration file to the target host computer's `<install_path>/shared` folder.

# 4 Configuring Select Access

Select Access is considered a management-free system. That means that a wizard, known as the Setup Tool, guides you through configuration options for components you have installed. It then manages this setup through the directory server, which enables you to effortlessly add additional components for real-time scalability. New components are registered in the directory, and component configurations are automatically downloaded from the directory. This chapter provides an overview of how to configure Select Access with the wizard-based Setup Tool.

## Chapter Overview

Select Access setup requires that you record data to specific files and directory locations. Topics in this chapter describe how this works with the Setup Tool:

- [Where Data is Recorded](#) on page 55
- [About the selectaccess.conf File](#) on page 56
- [Understanding Setup Methods and Parameter Types](#) on page 56
- [Using the Setup Tool](#) on page 57
- [Things to Check Before You Finish](#) on page 61

## Where Data is Recorded

Depending on your particular setup of Select Access, configuration data is written to the following locations:

- **The `selectaccess.conf` file:** This file, created by the installer, is a global configuration file. It is used to define specific details and/or files required by various Select Access components. By default, the installer stores `selectaccess.conf` in the root of your Select Access installation directory.



Do not move or rename this file, unless you are using an alternate file for testing and/or development purposes. Otherwise, Select Access components will not be able to locate this configuration file to find vital information they need.

For details, see [About the selectaccess.conf File](#) on page 56.

- **The components' XML bootstrap files:** These files, created by the Setup Tool, contain a number of parameters that you configure with this interface. It also includes some parameters that the Setup Tool sets transparently with default values. Parameters in this file are the settings a component needs on startup and therefore cannot be written to the Policy Store.
  - ⚠ These bootstrap files contain startup and general configuration information for their respective Select Access component. Modifying or moving these files could result in one or more Select Access components being unable to start correctly. You should ensure that you protect these files using both logical and physical controls.
  - If you change the values of any of these parameters, restart the component.
- **The Policy Store:** The information recorded in the Policy Store by the Administration server via the Setup Tool contains all other parameters that the server manages from this centralized location. These are parameters that are not required by a component at startup.

## About the selectaccess.conf File

The `selectaccess.conf` file is a global configuration file that describes where components can locate specific files on a specific host computer. Components read this file at startup to locate their XML configuration files. The Setup Tool also uses this file to detect which components have been installed and to display components' configuration. For example, on Windows, this file contains the following lines by default:

```
SELECTACCESS_HOME=C:\Program Files\HP OpenView\Select Access\  
SELECTACCESS_CONFIGS=C:\Program Files\HP OpenView\Select Access\bin\  
SELECTACCESS_BIN=C:\Program Files\HP OpenView\Select Access\bin\  
SELECTACCESS_LIB=C:\Program Files\HP OpenView\Select  
Access\lib\SELECTACCESS_CONTENT=C:\Program Files\HP OpenView\Select  
Access\content\  

```

- ⚠ If you move any of the files required by Select Access components, ensure you modify this file accordingly. For example, the forms required by Enforcer plugins are stored in Select Access's `content` folder. If you move the forms in this folder to a different location, then modify the value of this `SELECTACCESS_CONTENT` parameter to reflect this change. Otherwise, the Enforcer plugin cannot display the forms required.

## Understanding Setup Methods and Parameter Types

Table 1 illustrates the relationship between the setup methods available with Select Access and the parameter types that can be set with these methods.

- If you are creating override settings, they take precedence over group values, even if the default common values are changed with the Policy Builder.

**Table 1 Setup Method and Parameter Type Availability**

	Setup Method		
	Setup Tool	Policy Builder— Component Configuration	Manual editing of XML file
<b>Parameter Types</b>			
<p><b>Common parameters:</b> Shared by <i>all</i> Select Access components and initially configured when you set up the Administration server. As of this release, the only common parameters are audit settings. These settings determine how, when, and which type of Select Access events are logged. The Administration server writes these parameters to the Policy Store. Therefore, you can only modify these common parameters with the <b>Component Configuration</b> tool in the Policy Builder.</p>	1st time	•	
<p><b>Default group parameters:</b> Parameters that are inherited by a group of component types, such as the Policy Validator and Enforcer plugins. The Administration server writes custom parameters to either a bootstrap file or to the Policy Store, depending on whether or not groups of components require these values at the component’s startup time.</p>	•	•	•
<p><b>Override parameters:</b> Parameters that take precedence over any parameter shared by the group of components. The Administration server writes override parameters to either a bootstrap file or to the Policy Store, depending on whether or not the component requires the values at startup time.</p> <p><b>Note:</b> Override parameters appear in bold type in the Setup Tool and the Policy Builder configuration screens.</p>		•	•

## Using the Setup Tool

The Setup Tool is a graphical tool that allows you to quickly configure Select Access, without needing to manually edit a component’s configuration file. Technically, outside of setting up connection parameters, you can configure the entire Select Access component suite without

setting any specific parameters. This minimal setup occurs when you perform what is known as a **Typical** configuration. A **Typical** configuration has been designed to meet the needs of most environments.



If you are uninstalling, installing, upgrading, or configuring Select Access components on a Windows host computer, ensure that you do not have the Services window—or any other Control Panel application open. This open Control Panel application triggers conflicts that cause the installer and Setup Tool to behave abnormally.

## How to Set up Select Access

There are two conditions that determine how you configure Select Access:

- **What mode did you install Select Access in?** If you have installed a component in Console mode, HP recommends that you run the installer over VNC or X-Windows. For all other components except the Administration server, you can run the installer on another host computer and copy the resulting configuration XML file to the local host computer. For details on how to configure a component that you have installed in this mode, see [To configure a component installed by Console mode](#) on page 53.



Select Access requires that you configure the Administration server in GUI mode on the local host computer. This is because specific settings for the Administration server require that the Setup Tool run locally so the correct parameters are populated accordingly.

- **How much involvement do you want in setting up your components?** If you want to set up Select Access without configuring most parameters for it, you will probably want to perform a **Typical** install, which is suitable for most business and network environments. A **Custom** install increases the complexity of your setup, because it requires more involvement from you to configure your components.



The Secure Audit server only follows a single configuration path that requires you review all configuration options and set the component up accordingly.

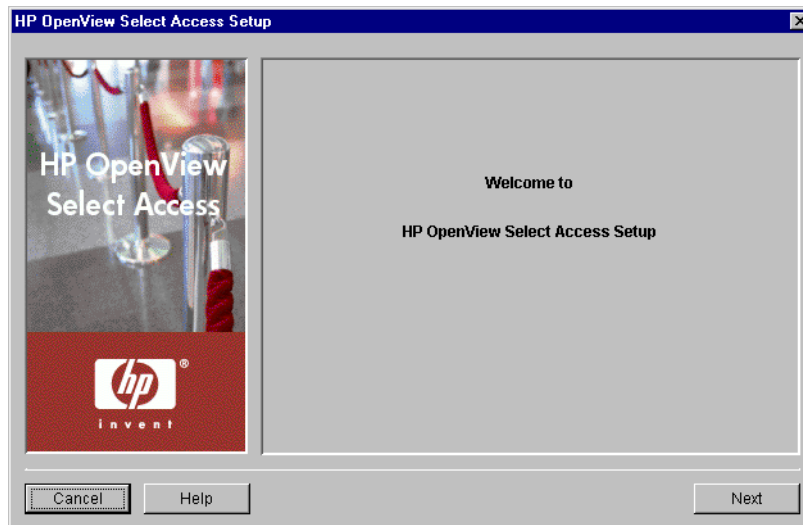
For details on whether or not to perform a **Typical** or a **Custom** install, see the corresponding sections that follow:

- [The Administration Server's Main Setup Types](#) on page 64
- [Configuring the Policy Validator](#) on page 117
- [Configuring the Enforcer Plugin](#) on page 129

### To configure Select Access with the Setup Tool

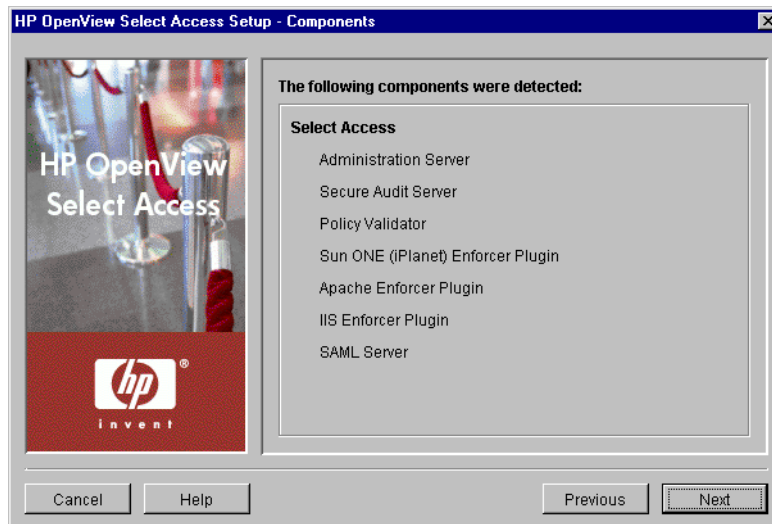
- 1 Launch the Setup Tool. You can run the Setup Tool from either of the following locations:
  - From the installer by answering **Yes** to the question, “Would you like to configure Select Access components now?”
  - From the **Start**→**Programs**→**HP OpenView**→**Select Access**→**Setup Tool** menu.

The **Welcome to HP OpenView Select Access** setup screen appears.



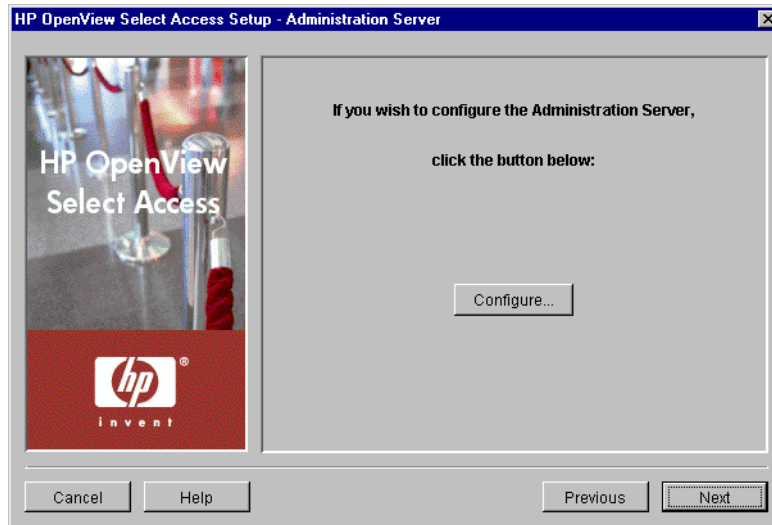
**Figure 1 Welcome to HP OpenView Select Access Setup Screen**

- 2 Click **Next**. The **Components** screen appears and summarizes the Select Access components that were installed on the current host computer. The Setup Tool configures the components in the order they appear on this screen.



**Figure 2 Components Setup Screen**

- 3 Click **Next**. Depending on what components you have installed, the corresponding component's first configuration screen appears, asking whether or not you want to configure that component now.
  - To configure that component, click **Configure**.
  - To skip a component and configure the next one, click **Next**.

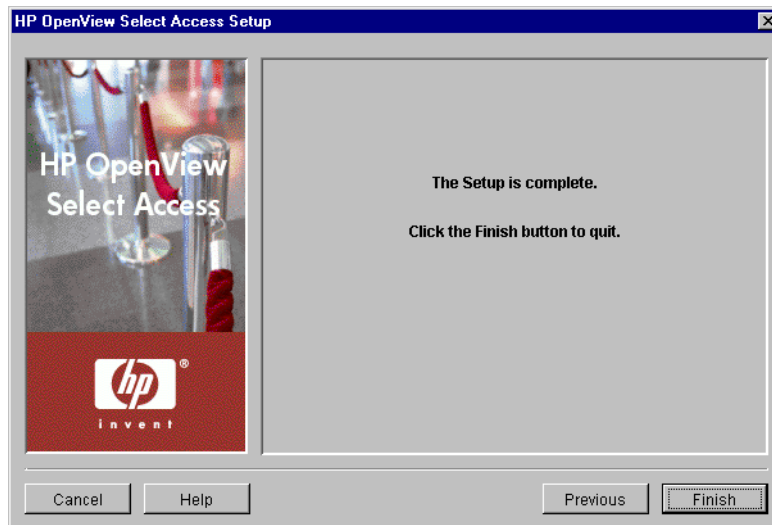


**Figure 3 Administration Server Setup Screen**

- 4 If you clicked the **Configure** button, follow the setup screens presented by the wizard to configure that component. For details, see the corresponding chapter:
  - [Chapter 5, Configuring the Administration Server](#)
  - [Chapter 6, Configuring the Secure Audit Server](#)
  - [Chapter 7, Configuring the Policy Validator](#)
  - [Chapter 8, Configuring the Enforcer Plugins](#)

When you have finished configuring the component, click the wizard's **Finish** button. Depending on which components you have installed on this host, the next component's configuration wizard appears.

- 5 When you have configured the last component, the **Setup Complete** screen appears. Click the **Finish** button to exit the Setup Tool.





#### Figure 4 Setup Complete Screen

- ▶ Once you have configured Select Access, you can localize it to suit your business environment.

**Note:** On Unix, you can only localize the Select Access product on Solaris.

## Things to Check Before You Finish

Before you finish configuring Select Access with the Setup Tool, ask yourself:

- Is this your first time setting up Select Access components? If so, then click the **Finish** button to complete the configuration process.
- Have you modified the configuration of Select Access components? If so, you need to ensure that your modifications do not affect other components:
  - If you changed Administration server configuration parameters such as directory server connection parameters, administration server connection parameters, SSL settings, or audit settings, ensure you run the wizard for all existing components on your network. Otherwise, the Setup Tool cannot replicate these values to other Select Access components.
    - ▶ A component that does not have the most current set of configuration values behaves unpredictably and can even fail.
  - If you changed Policy Validator configuration parameters such as modifying one or more IDs, you need to run the wizard for all Enforcer plugins on your network. Otherwise the Administration server cannot maintain available Policy Validator lists—a list that all Enforcer plugins require.
    - ▶ An inaccurate list of available Policy Validators can cause authentication and/or authorization failures.



# 5 Configuring the Administration Server

The Administration server is the first component you need to set up. The Administration server handles SSL details and configuration information. Without an Administration server configured and running, you are not allowed to configure your remaining Select Access components—except the Secure Audit server. This chapter describes how to deploy this component on your network.

- ▶ Run the Administration server as the same identity who installed it. For example, if you install the Administration server as root, you must run the Administration server as root, otherwise it behaves unpredictably.
- ▶ You can only have one Administration server running on your network at a time. Multiple Administration servers cannot write to the Policy Store at the same time.

## Chapter Overview

This chapter outlines how to configure the Administration server. Topics in this chapter include:

- [What the Administration Server Does](#) on page 63
- [Configuring the Administration Server](#) on page 64
- [Failing Over to Another Administration server](#) on page 86
- [Adding Delegated Administration CA Certificates](#) on page 86

## What the Administration Server Does

As the configuration engine for Select Access components, the Administration server coordinates all setup details by:

- Collecting common parameters
  - Handling requests sent by the Setup Tool to read/write component configuration information to/from the Policy Store
  - Defining the Select Access common parameters that all components inherit
  - Managing setup parameters among different Select Access components
- ▶ The setup of the Administration server writes most parameters to a local XML file. These parameters are bootstrap parameters. The Administration server requires these parameters at startup, which is why it writes them to this local file.



Every time you reconfigure your Administration server, your Enforcer plugin for delegated administration is also reconfigured so that properties required by the Select Access system is propagated correctly. To get this updated configuration information, you should disable and then re-enable delegated administration in the Policy Builder. This is particularly important if you have updated the number of Policy Validators deployed on your network. For details, see [To enable delegation](#) on page 206 in the *HP OpenView Select Access 6.1 Policy Builder Guide*.

## Configuring the Administration Server

The Administration server settings are initially configured via the Select Access Setup Tool. Because the Setup Tool is installed with the Select Access components, you can modify your settings at any time.



You can also modify certain parameters that the Administration server writes to the Policy Store via the **Tools**→**Configure Components** command in the Policy Builder. For details, see [Chapter 16, Modifying Components' Central Configuration Parameters](#), in the *HP OpenView Select Access 6.1 Policy Builder Guide*.

## The Administration Server's Main Setup Types

Before you begin, you need to understand the difference between two of the general setup types you can make.

- **Typical:** Use HP's recommended setup values. A **Typical** setup reduces the number of steps and minimizes the complexity of the Administration server's setup.
- **Custom:** Modify recommended values to meet the needs of your network and/or business environment. A **Custom** setup increases the number of steps and the complexity of the Administration server's setup.

Whether you choose one over the other depends on how much you need to customize the configuration of the Administration server. You can use the recommended values that are automatically configured by a **Typical** setup. To allow you to more easily identify what type of setup you need to perform, [Table 1](#) on page 66 compares the Administration server's setup tasks from a high level.



If you modify any of the parameters that affect the configuration of the Policy Store at any time, you must reconfigure your Policy Validators as well; this ensures that the Setup Tool propagates all corresponding configuration changes to them.

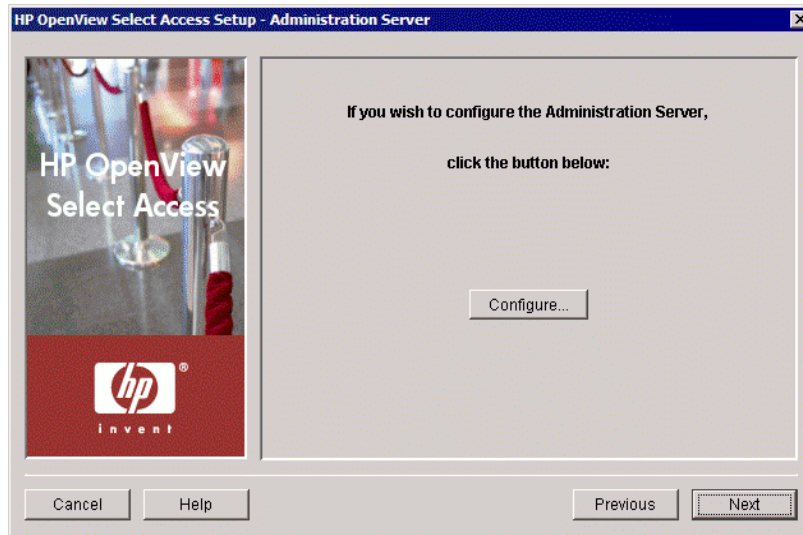
## Using the Setup Tool to Configure the Administration server

If you choose to configure your Select Access components directly from the installer, the Setup Tool will be started for you automatically.

If you choose to configure your Select Access components at a later time, or want to modify your configuration settings, you can run the Setup Tool and access the Administration server's configuration settings at any time.

## To configure the Administration server

- 1 If the Setup tool is not already started, click **Start**→**Programs**→**HP OpenView**→**Select Access**→**Setup Tool**. The **Component Setup Tool** window appears.
- 2 Click **Next** until you reach the Setup Tool's **Administration server** setup screen, as shown in Figure 1.



**Figure 1 Administration Server Setup Screen**

- 3 Click the **Configure** button. The Administration server setup process starts and the **Administrator** setup screen appears.
- 4 Complete the setup screens of the Administration server setup process, listed in [Table 1](#), as necessary.

▶ When you first run the new Administration server, it automatically connects to the directory server and detects if data from a previous installation exists. If so, it updates the data to use Select Access 6.1 formats as well as upgrades the schema to support new features (if permitted by the directory server).

Once this upgrade process happens, you cannot use an earlier version of Select Access with this data.

**Table 1 Overview of Administration Server Setup Process**

<b>Setup screen</b>	<b>Description</b>	<b>Default Value(s)</b>
<b>Administrator</b> setup screen	Allows you to define the administrator's login credentials. See <a href="#">Defining the Administrator Credentials</a> on page 68.	administrator-defined
<b>Directory Server</b> setup screen	If the Administration server does not detect policy data on this server, this screen allows you to define connection information for the directory server that holds the Policy Store. See <a href="#">Defining your Policy Store</a> on page 69.	administrator-defined
<b>Policy Data Location</b> setup screen	Allows you to define where the policy data will be stored. See <a href="#">Specifying the Policy Data Location</a> on page 70.	administrator-defined
<b>Identity Location</b> setup screen	Allows you to define a default identity location. The Policy Matrix displays these identity profiles along the Identities Tree when you first launch the Policy Builder. If you do not define an identity location with the Setup Tool, you can always add one or more later with the Policy Builder. See <a href="#">Preconfiguring an Identity Location</a> on page 71.	Identity location to be defined in the Policy Builder.
<b>General</b> setup screen	Allows you to choose one of two setup types: <ul style="list-style-type: none"> <li>• <b>Typical:</b> Use HP's recommended setup values.</li> <li>• <b>Custom:</b> Modify the recommended values to meet the needs of your network and/or business environment.</li> </ul> See <a href="#">Choosing your Setup Type</a> on page 73.	Typical
<b>Connection</b> setup screen	Displayed for Custom setup type only. Allows you to define the connection information Select Access components will use to connect to the Administration server. See <a href="#">Defining the Administration Server Connection Information</a> on page 74.	auto-defined
<b>Administration</b> setup screen	Displayed for Custom setup type only. Allows you to define the ports used by the Policy Builder's Administration and Delegated Administration. See <a href="#">Configuring the Policy Builder Administration Modes</a> on page 75.	auto-defined
<b>Web Administration</b> setup screen	Displayed for Custom setup type only. Allows you to define the ports used by the web-based administrative services, Web Administration and Self Administration. See <a href="#">Configuring the Web-based Administration Services</a> on page 76	auto-defined

**Table 1 Overview of Administration Server Setup Process (cont'd)**

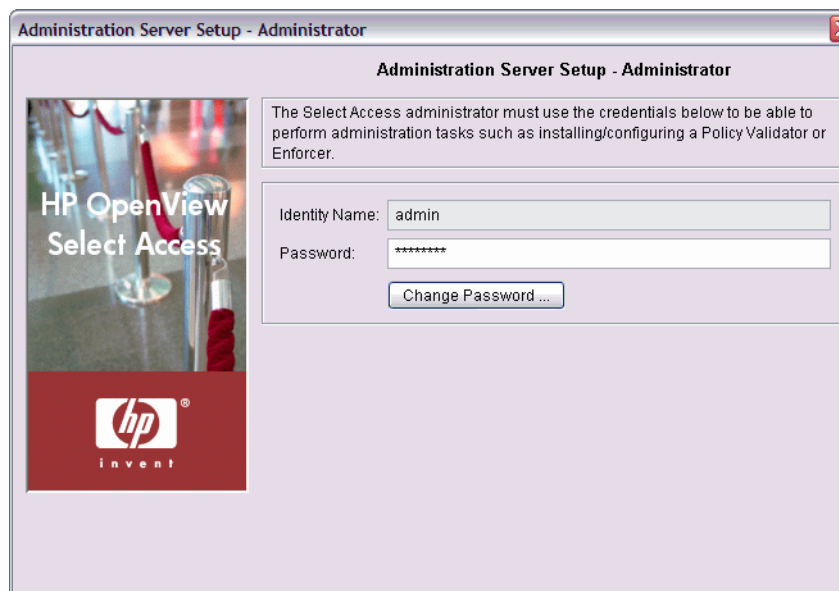
<b>Setup screen</b>	<b>Description</b>	<b>Default Value(s)</b>
<b>SSL Server Certificate</b> setup screen	Displayed for Custom setup type only. Allows you to define how the Administration server handles certificates required to encrypt sessions between administrators and the Administration server. See <a href="#">Setting up SSL Connection Handling</a> on page 77	handled by Select Access
<b>Directory Server Certificate</b> setup screen	Displayed for Custom setup type <i>only</i> when connections with the directory occur over SSL. Allows you to customize the verification of the Select Access components' certificates when they connect to the directory server that holds Policy Store data—over SSL only. See <a href="#">Configuring the Directory Server's Certificate</a> on page 78.	administrator-defined
<b>Policy Signing</b> setup screen	Displayed for Custom setup type only. Allows you to define whether or not the Administration server uses digital signatures to sign policy data in order to establish a level of irrefutability. See <a href="#">Configuring Policy Store Data Signing</a> on page 79.	disabled
<b>Signer CA Certificate</b> setup screen	Displayed for Custom setup type only. Allows you to customize data signing verification process. You can allow unknown CAs or you can require that they be authenticated. See <a href="#">Verifying the Signer's Certificate</a> on page 81.	allow unknown CAs
<b>Replicated Directory Servers</b> setup screen	Displayed for Custom setup type only. Allows you to create a list of replicated directory servers. Components can connect to a backup directory server if the master directory server fails. See <a href="#">Creating a Replicated Directory Servers List</a> on page 82.	replication not used

**Table 1 Overview of Administration Server Setup Process (cont'd)**

Setup screen	Description	Default Value(s)
<b>Default Audit Settings</b> setup screen	Displayed for Custom setup type only. Allows you to set the default audit client settings. Select Access components are clients of the Secure Audit server, which you configure separately. See <a href="#">Configuring Global Audit Settings</a> on page 83.	auto-defined to log all runtime errors
<b>Database Reporting</b> setup screen	Displayed for Custom setup type only. Allows you to enable or disable database reporting. Database logging and reporting is one of the features you can use with your auditing settings. See <a href="#">Configuring Database Reporting</a> on page 84.	disabled
<b>Finish</b> setup screen	Allows you to commit your configuration settings to the Policy Store and the Administration server's bootstrap XML file, and to automatically start the server. See <a href="#">Completing the Administration Server Setup Process</a> on page 85	enable server restart

## Defining the Administrator Credentials

The Administrator setup screen, shown in [Figure 2](#), allows you to set the login credentials used to connect to the Administration server.



**Figure 2 Administrator Setup Screen**

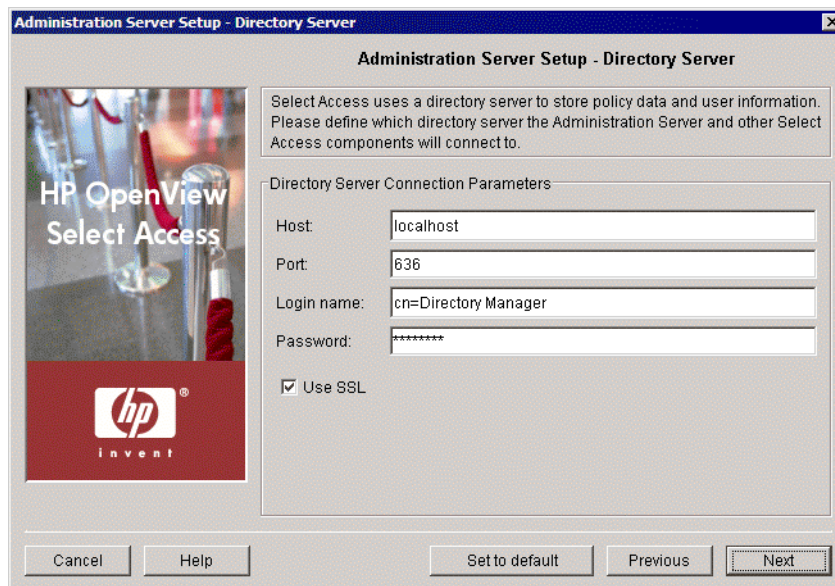


## To set the Administrator credentials

- 1 In the **Identity Name** field, enter the name of the administrator that is installing and configuring Select Access on your network.
- 2 Create the password of the administrator installing and configuring Select Access on your network. Click the **Change Password** button to set this password.
  - ▶ You can change the Administration server's password at any time by clicking the **Change Password** button.
- 3 Click **Next**. The **Directory Server** setup screen appears. For details on how to configure this screen, see [Defining your Policy Store](#) on page 69.

## Defining your Policy Store

The **Directory Server** setup screen, shown in [Figure 3](#), allows you to define connection information for the directory server that holds the Policy Store. You only need to populate data if it has not already been automatically filled for you.



The screenshot shows a window titled "Administration Server Setup - Directory Server". On the left is a logo for "HP OpenView Select Access" with the HP logo and the word "invent" below it. The main area contains the following text: "Select Access uses a directory server to store policy data and user information. Please define which directory server the Administration Server and other Select Access components will connect to." Below this is a section titled "Directory Server Connection Parameters" with the following fields: "Host" (localhost), "Port" (636), "Login name" (cn=Directory Manager), and "Password" (masked with asterisks). There is also a checkbox labeled "Use SSL" which is checked. At the bottom of the window are buttons for "Cancel", "Help", "Set to default", "Previous", and "Next".

**Figure 3** Directory Server Setup Screen

## To configure a directory server to store Select Access policy

- 1 Define values for the connection parameters in the **Directory Server Connection Parameters** group.
  - **Host:** Required. Enter the name or IP address of the host computer on which you installed the directory server.

- **Port:** Optional. Enter the port the directory server runs on. A valid port number ranges from 1 to 65535. If you do not provide a port value, the Administration server uses a value of 636. This is typically the default port used for SSL connections.
  - Using port 389 disables the use of SSL. This is typically the default port used for non-SSL connections. If you are sure your directory has been configured to use SSL on port 389, ensure that you recheck the **Use SSL** box.
- **Login Name:** Required. Enter the directory administrator's login name.
- **Password:** Required. Enter the directory administrator's password.
- **Use SSL:** Optional. Check this box if you want to encrypt the data exchange between the Administration Server and this directory server by using Secure Sockets Layer (SSL). If your directory server supports SSL connections, we recommend that you use SSL. For more details on SSL, see [Authenticating Identities with Certificates](#) on page 47, in the *HP OpenView Select Access 6.1 Network Integration Guide*.
  - If you are using an Active Directory server, you need to temporarily disable SSL the first time you configure it.

The Administration server uses this information to establish a connection with the corresponding directory server.

- 2 When you have finished configuring the directory server connection parameters, click **Next**. At this point, the Administration server tries to:
  - Connect to the directory server.
  - Automatically update its schema, if possible.

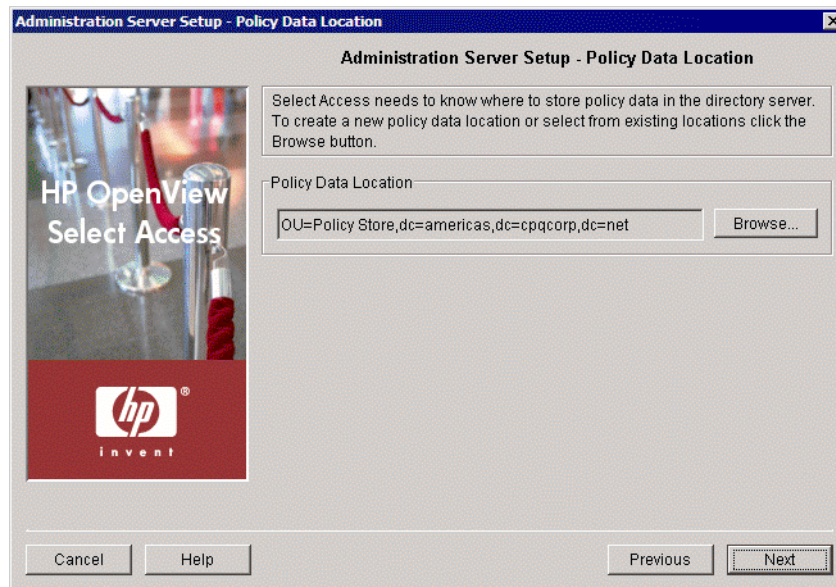
If this is successful, the **Policy Data Location** setup screen appears. See [Specifying the Policy Data Location](#) on page 70.

- If the Administration server cannot automatically update the schema, you cannot continue to set up Select Access components. Certain directory servers require manual intervention before the schema integrates with Select Access. For details on those directory servers, see [Chapter 2, Directory Server Integrations](#), in the *HP OpenView Select Access 6.1 Network Integration Guide*.

## Specifying the Policy Data Location

The Policy Data Location setup screen, shown in [Figure 4](#), allows you to select the folder on the directory server that acts as your Policy Store and holds all of your policy data.

- If the Administration server detects policy data, the values are automatically populated by the Setup Tool.



**Figure 4 Policy Data Location Setup Screen**

## To choose a policy data location

- 1 Select the folder in the directory server that is your Policy Store in the **Policy Data Location** group.

➤ If you change the policy data location in the future, ensure that you reconfigure all Policy Validators on your Select Access-protected network. Otherwise, the Administration server cannot replicate this location change to the remaining Select Access components.

To do this:

- a Click **Browse**. The **Select Location** dialog box appears.
- b To use a location that already exists for your Policy Store, select the folder, then click **OK**.
- c To define a location that has not yet been created and allocated for your Policy Store, click **New** and create that folder now.

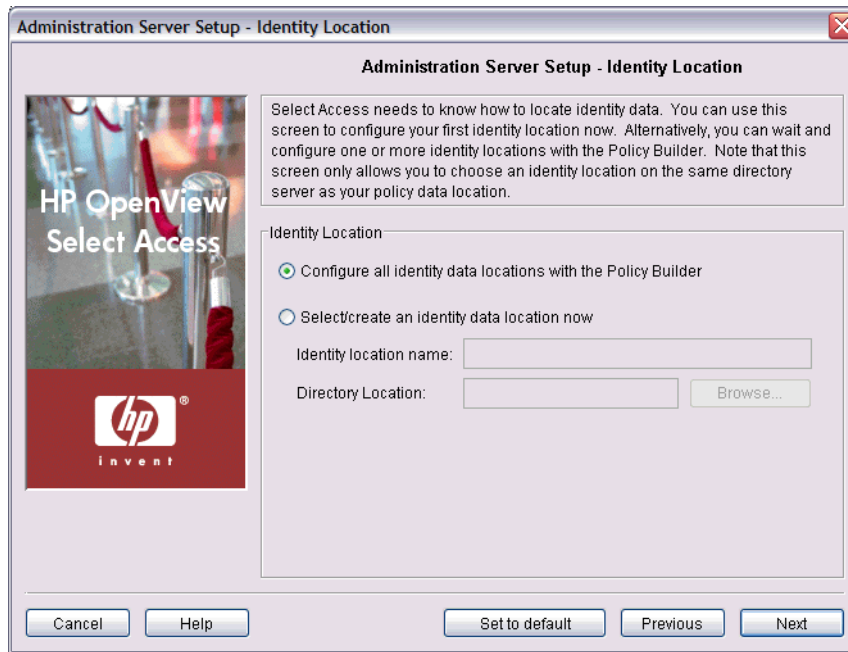
For details on the Policy Store, see [Chapter 15, Managing your Policy Data](#) in the *HP OpenView Select Access 6.1 Policy Builder Guide*. For details on how to preconfigure your directory server to work with Select Access, see [Chapter 2, Directory Server Integrations](#), in the *HP OpenView Select Access 6.1 Network Integration Guide*.

- 2 When you have finished configuring the policy data location, click **Next**. The **Identity Location** setup screen appears. See [Preconfiguring an Identity Location](#) on page 71.

## Preconfiguring an Identity Location

The **Identity Location** setup screen, shown in [Figure 5](#), allows you to preconfigure an identity location that the Policy Builder uses to render an initial set of identity profiles along the Identities Tree.

If you choose not to configure an identity location at this time, you can do so when you first run the Policy Builder. Until you configure an identity location, the Identities Tree will contain no profiles and you can set no policies.



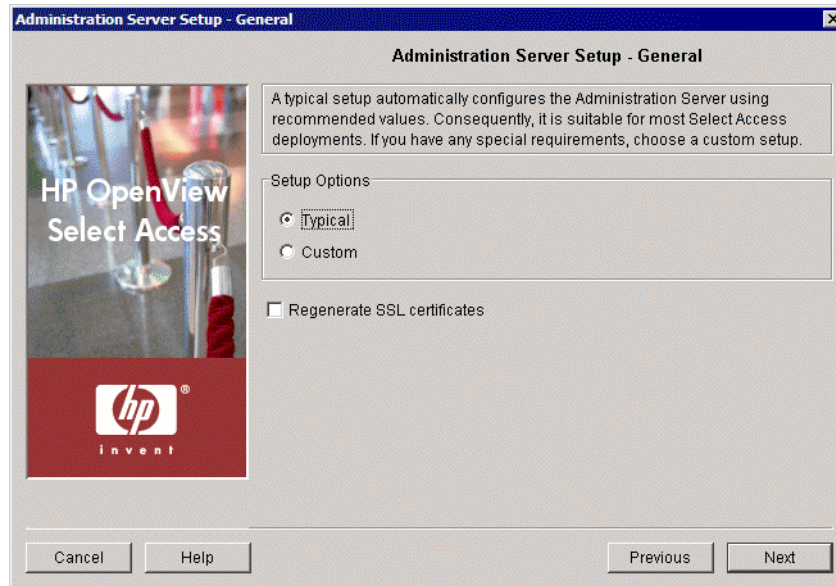
**Figure 5 Identity Location Setup Screen**

### To preconfigure an identity location

- 1 Choose whether or not you want to configure an initial identity data location by choosing the corresponding option:
  - **Configure all identity data locations with the Policy Builder:** Choosing this option means that when you first run the Policy Builder, your Identities Tree appears empty. You therefore need to define at least one identity location in the Policy Builder before being able to set access policies. Skip to [step 4](#).
  - **Select/create an identity data location now:** Choosing this option means that when you first run the Policy Builder, the Policy Builder uses the data in this location to render an initial set of profiles on the Identities Tree. You can change this identity data location or add new ones with the Policy Builder.
- 2 If you are creating an identity data location now, type a text string in the **Identity location name** field. The Policy Builder uses this string to name the new identity data location branch on the Identities Tree. Naming branches is particularly important if you decide to add more identity locations to the Identities Tree at a later date.
- 3 Click the **Browse** button and select the folder on the directory server that holds identity data. This location appears in the **Directory Location** field.
  - ▶ This identity location must be on the same directory server you configured for your Policy Store.
- 4 Click **Next**. The **General** setup screen appears. See [Choosing your Setup Type](#) on page 73.

## Choosing your Setup Type

The **General** setup screen, shown in [Figure 6](#), allows you to choose whether you want to perform a **Typical** or a **Custom** setup.



**Figure 6** General Setup Screen

### To choose your setup type

- 1 Select one of the setup options:
  - **Typical:** By choosing this option, you are essentially setting up this component without needing to configure it. HP's recommended values are appropriate for most environments.
  - **Custom:** By choosing this option, you can customize the Administration server's setup.
    - ▶ A **Custom** setup increases the number of steps and increments the complexity of the Administration server's setup. If you misconfigure any of the setup parameters documented in these steps, you can return to HP's recommended values by clicking the **Set to Default** button on any of the ensuing screens.
- 2 If you are reconfiguring or reinstalling one or more components, a **Regenerate SSL certificate** check box appears. Check this box to regenerate the SSL certificates used by the components on your network. This ensures that you synchronize SSL certificates despite the change in your deployment.
  - ⚠ If you check this box, you must regenerate certificates for all remaining components on your network—including the Enforcer plugin used for delegated administration. Otherwise, components' certificates cannot be synchronized and SSL connections will fail.



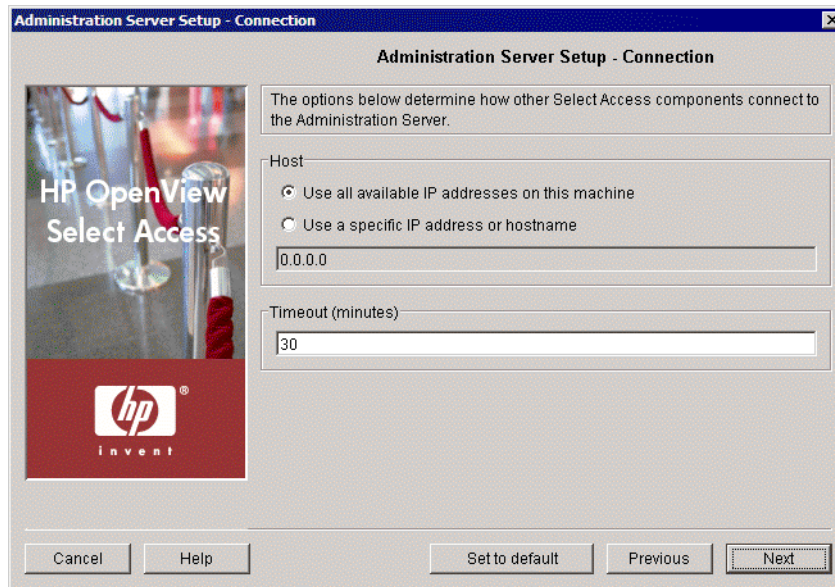
If you have upgraded from an unpatched version of Select Access 5.0, you should regenerate certificates for all components as well. This synchronizes changes that were made to certificates since Select Access 5.0 Patch 1. Otherwise, you cannot perform basic Select Access functions that require SSL connections (for example, flushing the Policy Validator cache from the Policy Builder).

For information on how to avoid regeneration when you need to reinstall a component, see [Authenticating Identities with Certificates](#) on page 47, in the *HP OpenView Select Access 6.1 Network Integration Guide*.

- 3 Click **Next**. Depending on which setup type you chose, one of two screens will appear:
  - If you are performing a **Typical** setup, the **Finish** screen appears. See [Completing the Administration Server Setup Process](#) on page 85.
  - If you are performing a **Custom** setup, the **Connection** setup screen appears. See [Defining the Administration Server Connection Information](#) on page 74.

## Defining the Administration Server Connection Information

The **Connection** setup screen, shown in [Figure 7](#), allows you to define connection information for the Administration server. Other Select Access components use this information as they try to connect to the Administration server and download their configuration parameters at runtime.



**Figure 7** Connection Setup Screen

### To set connection information for the Administration server

- 1 Review HP's recommended values. To customize these values, modify any of the screen's fields as needed.

**Host:** Required. Choose which IP address is used to connect to the host computer of the Administration server.

- Click **Use all available IP addresses on this machine** to try all IP addresses configured for the host computer. HP recommends you use this option: if one address happens to become unavailable, Select Access components try other addresses to find one that is available.
- Click **Use a specific IP address or hostname** to use a single address only and enter the details in the corresponding text box that follows this option.

**Timeout (minutes):** Required. Specify how long the Administration server will wait for a response before timing out.

- 2 Click **Next**. The **Administration** setup screen appears. See [Configuring the Policy Builder Administration Modes](#) on page 75.

## Configuring the Policy Builder Administration Modes

The Policy Builder has different administrative modes, each of which must access the Administration server via its own port:

- **Administration:** For use exclusively by the Select Access super administrators, this mode offers full Policy Builder functionality. It should be used for initial setup, including enabling delegation, and for emergencies only.
- **Delegated Administration:** For use by all delegated administrators, this mode offers only as much functionality as has been granted by the delegating administrator.



You can also configure Web Administration. For details, see [Configuring the Web-based Administration Services](#) on page 76.

When you access the Policy Builder in full administration mode, the delegated modes are listed as services of the Administration server when you access the Policy Builder.

The **Administration** screen, shown in [Figure 8](#), allows you to set the ports used by each of the three modes. They also allow you to customize how the Administration server services are displayed in the Resources Tree.

**Administration Server Setup - Administration**

The Select Access administrator and the delegated administrators must use the corresponding ports below to access administration and delegated administration functionality respectively when using Policy Builder.

**Administration**  
Port: 9986

**Administration Server**  
Folder Name: Administration Server

**Delegated Administration**  
Port: 9987  
Service Name: Delegated Administration

Cancel Help Set to default Previous Next

**Figure 8 Administration Setup Screen**

## To configure the Policy Builder administration modes

- 1 In the **Administration** group, specify the port used to access the Policy Builder in root/full administration mode. By default, this mode uses port 9986.
- 2 In the **Administration Server** group, specify the name of the folder which will contain the Administration server resources (delegated administration, web administration, and self administration). This folder will be added to the Resources Tree in the Policy Builder in full administration mode, where you can enable and disable the individual administrative resources.

By default, the folder containing these resources is named Administration Server.

▶ The Administration Server resources are only displayed in the Resource Access tree when the Policy Builder is run in full administration mode.

- 3 In the **Delegated Administration** group, review the default delegated administration values and modify them as necessary. You can modify the following values:

- **Port:** Specifies the default port used by the Policy Builder in delegated administration mode. By default, this mode uses port 9987.
- **Service Name:** Specifies the resource name for delegated administration. By default, the service is named Delegated Administration.

▶ The Administration server resources are only displayed in the Resource Access tree when the Policy Builder is run in full administration mode.

- 4 Click **Next**. The **Web Administration** screen appears. See [Configuring the Web-based Administration Services](#) on page 76.

## Configuring the Web-based Administration Services

The **Web Administration** setup screen, shown in [Figure 9](#), allows you to configure the ports and service names for Select Access' web-based administration services.

Administration Server Setup - Web Administration

**Administration Server Setup - Web Administration**

The web administrators and the self administrators must use the corresponding ports below to access web administration and self administration functionality respectively when using a web browser.

Web Administration

Port: 9991

Service Name: Web Administration

Self-Administration

Port: 9992

Service Name: Self Administration

Registration Resource: self\_registration

Management Resource: self\_management

Password Reset Resource: password\_reset

HP OpenView Select Access

hp invent

**Figure 9** Web Administration Setup Screen



## To configure Web and Self Administration

- 1 In the **Web Administration** group, review the default Web Administration values and modify them as necessary. You can modify the following values:
  - **Port:** Specifies the default port used by Web Administration. By default, this Web Administration uses port 9991.
  - **Service Name:** Specifies the resource name for this service. By default, the service is named Web Administration.

➤ The Administration Server resources are only displayed in the Resource Access tree when the Policy Builder is run in full administration mode.
- 2 In the **Self Administration** group, review the default Web Administration values and modify them as necessary. You can modify the following values:
  - **Port:** Specifies the default port used by Web Administration. By default, this Self Administration uses port 9992.
  - **Service Name:** Specifies the resource name for this service. By default, the service is named Self Administration.
  - **Registration Resource:** Specifies the path to the self-registration resource.
  - **Management Resource:** Specifies the path the to the self-management resource.
  - **Password Reset:** Specifies the path the to the password reset resource.
- 3 Click **Next**. The **SSL Server Certificate** setup screen appears. See [Setting up SSL Connection Handling](#) on page 77.

## Setting up SSL Connection Handling

The **SSL Server Certificate** setup screen, shown in [Figure 10](#), allows you to choose how you want the Administration server to handle SSL connections between the administrator's browser and the Policy Builder applet.



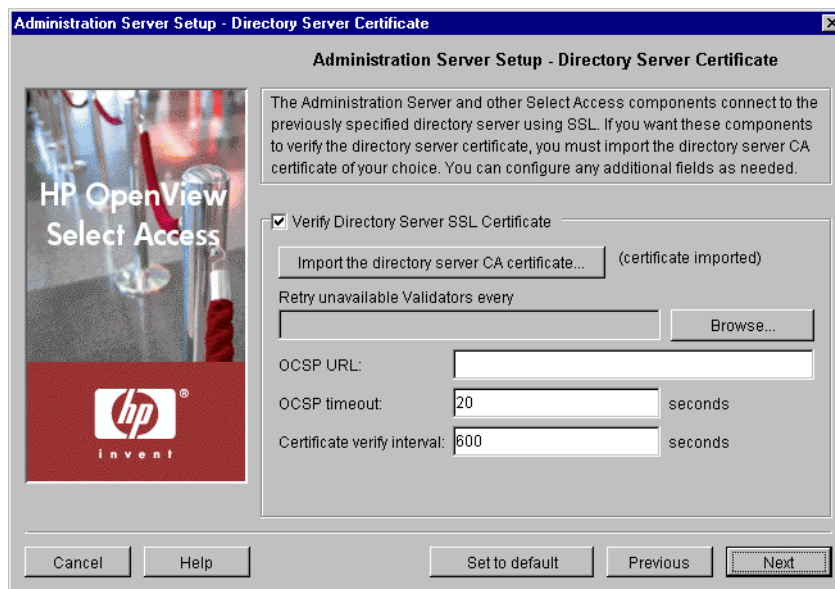
**Figure 10** SSL Server Certificate Setup Screen

## To set how the Administration server handles SSL connections

- 1 The SSL certificate encrypts Policy Builder sessions with the Administration server. Choose how you want the Administration server to handle the SSL server certificate. You must choose between either of these parameters.
  - **Let Select Access handle SSL server certificate:** Choose this option if you want Select Access to manage the certificate.
  - **Import SSL server certificate:** Choose this option if you want to use your own certificate and key. Click the **Import signer certificate** button to choose the corresponding SSL certificate.
- 2 Click **Next**. Depending on whether or not you chose to use SSL, one of two screens will appear:
  - If you checked the **Use SSL** box in the **Directory Server** setup screen, the **Directory Server Certificate** setup screen appears. See [Configuring the Directory Server's Certificate](#) on page 78.
  - If you are not using SSL, the **Policy Signing** setup screen appears. See [Configuring Policy Store Data Signing](#) on page 79.

## Configuring the Directory Server's Certificate

The **Directory Server Certificate** setup screen, shown in [Figure 11](#), allows you to customize the verification of the Select Access components' certificates when they connect to the directory server that holds Policy Store data—over SSL only.



**Figure 11** Directory Server Certificate Setup Screen

## To configure the directory server's certificate

- 1 Review HP's recommended values. To customize these values, modify any of the screen's fields as needed.

- **Verify directory server SSL certificate:** Optional. Check this box if you want Select Access components to verify the directory server acting as the Policy Store before opening an SSL session with it.
    - ▶ If you want Select Access components to allow self-signed certificates (where the issuer and the recipient are one and the same) and unknown CAs, do not check this box.
  - **Import the directory server CA certificate:** Required if you have checked the previous box. Click this button to import the directory server's CA certificate. The directory server uses this X.509 compliant certificate to encrypt SSL sessions between it and Select Access components.
  - **Revocation list DN:** Optional. If you are using a certificate revocation list, select the root location of your list in the Policy Store. This list is used to determine the revocation state of an identified certificate. If the LDAP certificate appears on the CRL, the Administration server considers it invalid.
  - **OCSP URL:** Optional. If you are using an OCSP server, enter the URL of your Online Certificate Status Protocol server. The Administration server and other Select Access components use this URL to determine the revocation state of an identified certificate.
  - **OCSP timeout:** Optional. Enter a time limit (in seconds) that determines how long the Administration server and other Select Access components wait for a reply, before closing their connection to the OCSP server.
    - ▶ When the Administration server and other Select Access components issue a status request query to this OCSP server, it suspends component access to the Policy Store directory server until the certificate in question is verified.
  - **Certificate verify interval:** Optional. Enter the time limit (in seconds), that determines how long the certificate remains valid (that is, cached by the component) after the component verifies it. The validity of the certificate expires after this time.
- 2 Click **Next**. The **Policy Signing** setup screen appears. See [Configuring Policy Store Data Signing](#) on page 79.

## Configuring Policy Store Data Signing

The **Policy Signing** setup screen, shown in [Figure 12](#), allows you to take advantage of digital signatures in order to quickly identify when any unauthorized change to the Policy Store has occurred. By using a signature, entries are validated when the correct signature has been applied to it. Additions or modifications to entries are considered to be unauthorized when the wrong signature was used or no signature was used at all.



**Figure 12 Policy Signing Setup Screen**

### To enable or disable policy signing

- 1 Review HP's recommended values. To customize these values, modify any of the screen's fields as needed.
  - **Sign Policy:** Optional. Check this box to sign all data that you add to the Policy Store. By signing policy data, you prevent unauthorized changes from being made. You must then choose one of the following options:
    - **Let Select Access handle signer's certificate and key:** Optional. Choose this option if you want Select Access to handle the certificate and key that the Administration server uses to sign data in the Policy Store.
    - **Import signer's certificate and key:** Optional. Choose this option if you want to use your own certificate and key used by the Administration server to sign data in the Policy Store.

If you choose this option, you must click the **Import signer certificate** button to locate your PEM format certificate. Also enter the DN of the authorized administrator who has the authorization to sign data entries via Policy Builder in the **Policy Signer DN** field. If you have correctly configured the **Import Signer CA** dialog box, the Administration server saves the CA certificate and the private key in its bootstrap configuration file, and stores the signer's certificate in the Policy Store.

- Ensure that the administrator's profile contains a signer certificate, private key, and a CA certificate. Also ensure that the DN in the **Policy Signer DN** field matches the CN used in the subject field of the PEM format certificate.

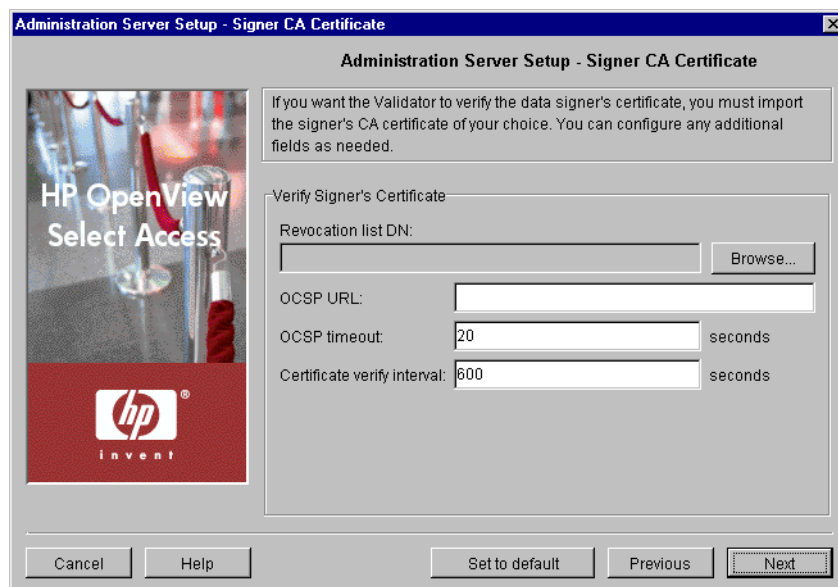
For more details on signing policy data, see [Chapter 15, Managing your Policy Data](#), in the *HP OpenView Select Access 6.1 Policy Builder Guide*.

- 2 Click **Next**. Depending on whether or not you are importing your own signer CA, one of two screens will appear:

- If you selected **Import signer's certificate and key**, the **Signer CA Certificate** setup screen appears. See [Verifying the Signer's Certificate](#) on page 81.
- If you chose not to sign policy data, or selected **Let Select Access handle signer's certificate and key**, the **Replicated Directory Servers** setup screen appears. See [Creating a Replicated Directory Servers List](#) on page 82.

## Verifying the Signer's Certificate

The **Signer CA Certificate** setup screen, shown in [Figure 13](#), allows you to setup verification of the data signer's certificate. By configuring the fields of this screen, you give the Policy Validator the ability to confirm the validity of this certificate.



**Figure 13 Signer CA Certificate Setup Screen**

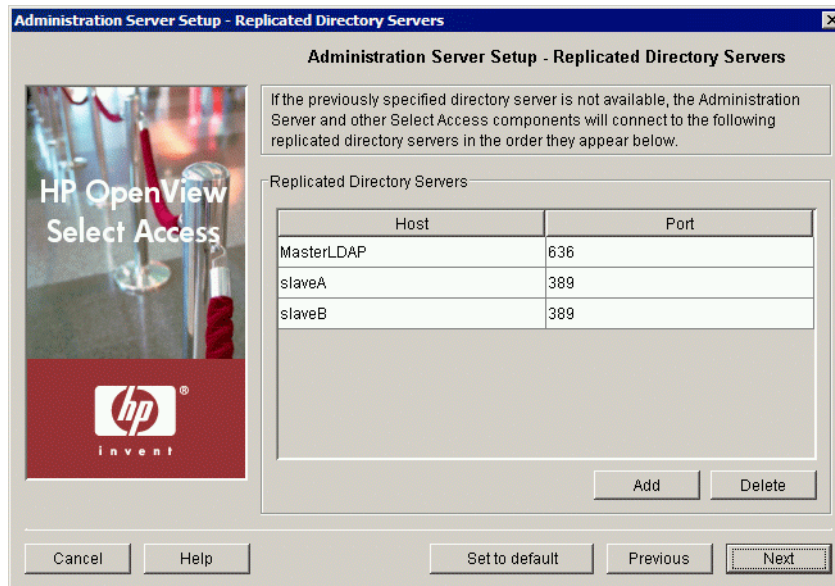
### To enable the Policy Validator to verify the signer's certificate

- 1 Review HP's recommended values. To customize these values, modify any of the screen's fields as needed:
  - **Revocation list DN:** Optional. If you are using a certificate revocation list, you must select the root location in the Policy Store where your list is located. The Administration server uses this list to determine the revocation state of an identified certificate. If the LDAP certificate appears on the CRL, it is considered invalid.
  - **OCSP URL:** Optional. If you are using an OCSP server, enter the URL of your Online Certificate Status Protocol server. The Administration server and other Select Access components use this OCSP server to determine the revocation state of an identified certificate.

- **OCSP timeout:** Optional. Enter a time limit (in seconds) that determines how long the Administration server and other Select Access components wait for a reply, before closing their connection to the OCSP server.
    - When the Administration server and other Select Access components issue a status request query to this OCSP server, it suspends component access to the Policy Store directory server until the certificate in question is verified.
  - **Certificate verify interval:** Optional. Enter the time limit (in seconds), that determines how long the certificate remains valid for (that is, cached by the component) after the component verifies it. The validity of the certificate expires after this time.
- 2 Click **Next**. The **Replicated Directory Servers** setup screen appears.

## Creating a Replicated Directory Servers List

The **Replicated Directory Servers** setup screen, shown in [Figure 14](#), allows you to define the connection parameters for replicated Policy Store directory servers. Select Access components use replicated directory servers when the master directory server for the Policy Store fails.



**Figure 14 Replicated Directory Servers Setup Screen**

### To create a replicated directory servers list

- 1 If you have replicated the directory server that acts as your Policy Store, enter the connection parameters for those host computers. That way, if the master directory server fails, Select Access components connect to the replicas in the order they appear.
  - **Host:** Required. Click a cell below this column and type the name or IP address of the host computer on which the directory server has been replicated.
  - **Port:** Required. Click a cell below this column and type the port the replicated directory server is running on.
- 2 Click the **Add** button to create additional rows for other replicas you have on your network. The Setup Tool adds a row below the row that currently has focus.

- 3 Select a row, then click the **Delete** button to remove an empty or populated row.

For more details on how Select Access supports directory server replication, see [Chapter 2, Directory Server Integrations](#), in the *HP OpenView Select Access 6.1 Network Integration Guide*.

- 4 Click **Next**. The **Default Audit Settings** setup screen appears.

## Configuring Global Audit Settings

The **Default Audit Settings** setup screen, shown in [Figure 15](#), allows you to configure auditing settings for all Select Access components. Components use these settings to determine which events to log, unless one has been created for a component-specific pool, or you override these settings for an individual component.



Default (or Global) Audit Settings do not just affect the Administration server. All Select Access components use these settings. You can change these defaults from the Policy Builder in the future.



**Figure 15 Default Audit Settings Setup Screen**

### To configure default/global auditing settings for Select Access components

- 1 Review HP's recommended audit settings. To customize global audit settings used by all Select Access components at runtime, change the settings as required. By default, Select Access components log all runtime errors to the system log.
  - To create or modify audit settings rows, click **Add** or **Properties** respectively. The **New Event Log** dialog box appears displaying two tabs, **Audit Trail** and **Audit Policy**. These tabs correspond to the columns of the **Default Audit Settings** setup screen.
    - ▶ If you log events to the Secure Audit server, the Administration server component becomes a client of it. Ensure that you have configured the Secure Audit server before continuing. For details, see [Chapter 6, Configuring the Secure Audit Server](#).

- If you log events to a database, ensure you enable database reporting as well. To enable database reporting, see [Configuring Database Reporting](#) on page 84.
  - When you configure the tabs of the **New Event Log** dialog box, then click **OK**, the Administration server adds a new row below the one you have selected and it populates the cells automatically. For details, see [Configuring an Audit Policy](#) on page 110.
    - 🚩 The Administration server's Audit Policy can include both Policy and Operation components.
  - To remove an empty or populated row, select the entry in question and click **Delete**.
- 2 Click **Next**. The **Database Reporting** setup screen appears. See [Configuring Database Reporting](#) on page 84.

## Configuring Database Reporting

The Database Reporting setup screen, shown in [Figure 16](#), allows you to set up a JDBC-compliant database if you intend to use it to write component runtime messages to it.

- 🚩 If you are enabling database reporting, you need to enable database logging as well. To log to a database, ensure that you have configured a database as an Audit Trail in the Administration server. See [Configuring Global Audit Settings](#) on page 83 for details.
- Oracle and MSSQL server scripts changed with the release of Select Access 5.1. If you used a previous version of Select Access, you need to migrate the data to use this new format. Otherwise, your data will be truncated and database reporting will be problematic.
- Database reporting requires that you set up database tables correctly. To do this, run the corresponding SQL script installed with Select Access. For details, see [Configuring a Database](#) on page 104.



**Figure 16 Database Reporting Setup Screen**



## To configure database reporting

- 1 Customize any of the following as needed.
  - **Enable Database Reporting:** Check this box to enable one or more Select Access components to log to a JDBC-compliant database and to create reports from that source.
  - **JDBC Driver:** Click **Choose** and locate the JDBC driver's archive file. Refer to your driver's documentation if you are unsure what file to use. Select Access components use this class to write events to the database.
    - If you need to list multiple driver files, you cannot use the **Choose** button. Instead, you need to type the path and filename to all files, separating each file with a semicolon (;). If the paths and/or filenames include a space, they must be surrounded by quotation marks. For example, if you are using a Microsoft database, you would type the filenames like this:

```
"C:\Program Files\MS_JDBC\lib\msbase.jar; C:\Program Files\MS_JDBC\lib\mssqlserver.jar; C:\Program Files\MS_JDBC\lib\msutil.jar"
```
    - If you are configuring an MS JDBC driver, note that the version tested against Select Access is version 2.2.0022. To check which version you are using, open the `read.me` file shipped with the driver. The version number appears in the document's header.
  - **Entry Point:** Enter the name of the JDBC Driver class name contained in the JDBC driver file you just defined.
    - Entry points can vary among different platforms. For example, for Oracle on Windows, an entry point is `oracle.jdbc.driver.OracleDriver`. On Unix, that same entry point is `oracle.jdbc.OracleDriver`.
- 2 Click **Next**. The **Finish** setup screen appears. See [Completing the Administration Server Setup Process](#) on page 85.

## Completing the Administration Server Setup Process

The **Finish** setup screen informs you that you have completed all setup tasks for the Administration server and allows you to automatically restart the server.

- When you first run the new Administration server, it automatically connects to the directory server and detects if data from a previous installation exists. If so, it updates the data to use Select Access 6.1 formats as well as upgrades the schema to support new features (if permitted by the directory server).

Once this upgrade process happens, you cannot use an earlier version of Select Access with this data.

## To complete the Administration server configuration

- 1 If you want to start the Administration server immediately after your configuration parameters have been recorded, check the **Start now** box.
- 2 Click **Finish** to commit your configuration to both:

- The Policy Store you defined at the beginning of the Administration server’s setup.  
AND
- The bootstrap XML file



This bootstrap file contains startup and general configuration information for the Administration server. Modifying or moving this file could result in the Administration server being unable to start correctly. You should ensure that you protect this file using both logical and physical controls.

As soon as you run the new Administration server for the first time, it automatically connects to the directory server and detects if data from a previous installation has been used. If so, it updates the data to use Select Access 6.1 formats. Once this upgrade process happens, you cannot use an earlier version of Select Access with this data.

- 3 If you plan to delegate administration responsibility, you still need to manually upload a CA certificate to the Administration server. For details, see [Adding Delegated Administration CA Certificates](#) on page 86.
- 4 If you have installed any other components on this computer, the next component’s setup screen appears. For details, see [To configure Select Access with the Setup Tool](#) on page 58.

## Failing Over to Another Administration server

Currently, you can only have one Administration server running on a Select Access-protected network at a time. However, if your current Administration server fails, you need to install a new Administration server—either on the same or a different host computer. For details on how to fail over to another Administration server, see [Chapter 10, Maintaining Select Access: Failovers, Repairs, and Updates](#).



If you choose the same policy data location as the Administration server that has failed, Select Access warns you that another Administration server is using the Policy Store. Proceed with caution and ensure the previous installation of the Administration server is not running. Two Administration servers *cannot* write to the same Policy Store at the same time.

## Adding Delegated Administration CA Certificates

If you plan to delegate administration authority to one or more remote identities and you want to authenticate their identity with certificates, you need to ensure you upload the corresponding CA certificate to the Administration server. Otherwise, when it runs the Policy Builder applet in delegated administration mode, it cannot compare the delegated administrator’s client certificate.

## Different Certificate Types

There are two types of CA certificates you can employ:

- *Standard certificates:* The certificates installed with Select Access. They include common CA certificates from authorities like:

Commercial Certification Authority	Certisign
Deutsche Telekom	CyberTrust
Entrust	Digitrust
EUnet International	Equifax Secure Global eBusiness
First Data	FESTE
IPS Servidores	GlobalSign
Microsoft	KeyWitness
Post.Trust	NetLock
SecureNet	Saunalahden Serveri
SIA Secure Client	SecureSign
TrustCenter	SwissKey
ValiCert	UserTrust
	VeriSign

Standard certificates are DER- or PEM-encoded X.509 certificates from one or more PKCS#7 files. For a complete list of standard certificates shipped with Select Access, see [Standard Certificates Installed with the Administration server](#) on page 87 in the *HP OpenView Select Access 6.1 Installation Guide*.

- *Custom certificates:* Any other DER- or PEM-encoded X.509 CA certificates not included in the standard certificate list.

### To upload a CA certificate for delegated administration

If you are using a standard certificate, you have already installed and uploaded the certificate on the Administration server's host computer. By default, you install these PKCS#7 certificates to the following directory on the host computer:

```
<install_path>/shared/jetty/etc/certs/standard
```

However, if you need to use a custom certificate, ensure you copy the file to the following directory on the host computer:

```
<install_path>/shared/jetty/etc/certs/custom
```

### Standard Certificates Installed with the Administration server

Select Access automatically installs the following certificates by default. If your certificate is not listed here, ensure you add it to the `Custom` folder on the Administration server's host computer.

- CA Certificate: CN=GTE CyberTrust Root,O=GTE Corporation,C=US

- CA Certificate: EMAIL=ca@digsigtrust.com, CN=Xcert EZ by DST,O=Xcert EZ by DST,L=Salt Lake City,ST=Utah,C=US
- CA Certificate: OU=VeriSign Trust Network,OU=(c) 1998 VeriSign Inc. - For authorized use only,OU=Class 1 Public Primary Certification Authority - G2,O=VeriSign Inc.,C=US
- CA Certificate: OU=VeriSign Individual Software Publishers CA,O=VeriSign Inc.,L=Internet
- CA Certificate: CN=VeriSign Class 4 Public Primary Certification Authority - G3,OU=(c) 1999 VeriSign Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign Inc.,C=US
- CA Certificate: CN=VeriSign Class 3 Public Primary Certification Authority - G3,OU=(c) 1999 VeriSign Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign Inc.,C=US
- CA Certificate: CN=VeriSign Class 2 Public Primary Certification Authority - G3,OU=(c) 1999 VeriSign Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign Inc.,C=US
- CA Certificate: CN=VeriSign Class 1 Public Primary Certification Authority - G3,OU=(c) 1999 VeriSign Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign Inc.,C=US
- CA Certificate: CN=UTN-USERFirst-Network Applications,OU=http://www.usertrust.com,O=The USERTRUST Network,L=Salt Lake City,ST=UT,C=US
- CA Certificate: CN=UTN-USERFirst-Client Authentication and Email,OU=http://www.usertrust.com,O=The USERTRUST Network,L=Salt Lake City,ST=UT,C=US
- CA Certificate: EMAIL=personal-freemail@thawte.com,CN=Thawte Personal Freemail
- CA,OU=Certification Services Division,O=Thawte Consulting,L=Cape Town,ST=WesternCape,C=ZA
- CA Certificate: EMAIL=personal-basic@thawte.com,CN=Thawte Personal Basic CA,OU=Certification Services Division,O=Thawte Consulting,L=Cape Town,ST=Western Cape,C=ZA
- CA Certificate: EMAIL=certificate@trustcenter.de,OU=TC TrustCenter Class 4 CA,O=TC TrustCenter for Security in Data Networks GmbH,L=Hamburg,ST=Hamburg,C=DE
- CA Certificate: CN=Swisskey Root CA,L=Zuerich,OU=Public CA Services,OU=008510000000500000192,O=Swisskey AG,C=CH
- CA Certificate: CN=SIA Secure Client CA,L=Milano,O=SIA S.p.A.,C=IT
- CA Certificate:0.9.2342.19200300.100.1.3=correo\_cert@correo.com.uy,CN=SERVICIOS DE CERTIFICACION - A.N.C.,OU=SERVICIOS ELECTRONICOS,O=ADMINISTRACION NACIONAL DE CORREOS,C=UY
- CA Certificate: CN=SecureSign RootCA3,O=Japan Certification Services Inc.,C=JP
- CA Certificate: CN=SecureSign RootCA2,O=Japan Certification Services Inc.,C=JP

- CA Certificate: CN=SecureSign RootCA1,O=Japan Certification Services Inc.,C=JP
- CA Certificate: O=SecureNet CA SGC Root,C=au
- CA Certificate: O=SecureNet CA Root,C=au
- CA Certificate: O=SecureNet CA Class B,C=au
- CA Certificate: O=SecureNet CA Class A,C=au
- CA Certificate: EMAIL=silver-certs@saunalahti.fi,CN=Saunalahden Serveri CA,O=Saunalahden Serveri Oy,L=Helsinki,C=FI
- CA Certificate: 0.9.2342.19200300.100.1.3=ca@ptt-post.nl,CN=PTT Post Root CA,OU=KeyMail,O=PTT Post,C=NL
- CA Certificate: CN=Post.Trust Root CA,OU=Post.Trust Ltd.,O=An Post,C=IE
- CA Certificate: CN=NetLock Uzleti (Class B) Tanusitvanykiado,OU=Tanusitvanykiadok,O=NetLock Halozatbiztonsagi Kft.,L=Budapest,C=HU
- CA Certificate: CN=NetLock Kozjegyzoi (Class A) Tanusitvanykiado,OU=Tanusitvanykiadok,O=NetLock Halozatbiztonsagi Kft.,L=Budapest,ST=Hungary,C=HU
- CA Certificate: CN=NetLock Expressz (Class C) Tanusitvanykiado,OU=Tanusitvanykiadok,O=NetLock Halozatbiztonsagi Kft.,L=Budapest,C=HU
- CA Certificate: CN=Microsoft Root Certificate Authority,DC=microsoft,DC=com
- CA Certificate: CN=Microsoft Root Authority,OU=Microsoft Corporation,OU=Copyright (c) 1997 Microsoft Corp.
- CA Certificate: CN=Microsoft Authenticode(tm) Root Authority,O=MSFT,C=US
- CA Certificate: CN=KeyWitness 2048 Root,2.5.4.46=OID.1.2.840.113549.1.1.1,O=KeyWitness International Inc.,C=US
- CA Certificate: EMAIL=ips@mail.ips.es,CN=IPS SERVIDORES,OU=Certificaciones,O=IPS Seguridad CA,L=BARCELONA,ST=BARCELONA,C=ES
- CA Certificate: EMAIL=info@valicert.com,CN=http://www.valicert.com/,OU=ValiCertClass 2 Policy Validation Authority,O=ValiCert Inc.,L=ValiCert Validation Network
- CA Certificate: CN=GTE CyberTrust Root,O=GTE Corporation,C=US
- CA Certificate: CN=GTE CyberTrust Root,OU=GTE CyberTrust Solutions Inc.,O=GTECorporation,C=US
- CA Certificate: CN=GTE CyberTrust Global Root,OU=GTE CyberTrust Solutions Inc.,O=GTE Corporation,C=US
- CA Certificate: CN=GlobalSign Root CA,OU=Root CA,O=GlobalSign nv-sa,C=BE
- CA Certificate: OU=FNMT Clase 2 CA,O=FNMT,C=ES

- CA Certificate: CN=First Data Digital Certificates Inc. Certification Authority,O=First Data Digital Certificates Inc.,C=US
- CA Certificate: EMAIL=feste@feste.org,CN=FESTE Verified Certs,O=Fundacion FESTE,L=Barcelona,ST=Barcelona,C=ES
- CA Certificate: EMAIL=feste@feste.org,CN=FESTE Public Notary Certs,O=Fundacion FESTE,L=Barcelona,ST=Barcelona,C=ES
- CA Certificate: CN=EUnet International Root CA,O=EUnet International
- CA Certificate: CN=Equifax Secure Global eBusiness CA-1,O=Equifax Secure Inc.,C=US
- CA Certificate: OU=Equifax Secure eBusiness CA-2,O=Equifax Secure,C=US
- CA Certificate: CN=Equifax Secure eBusiness CA-1,O=Equifax Secure Inc.,C=US
- CA Certificate: OU=Equifax Secure Certificate Authority,O=Equifax,C=US
- CA Certificate: OU=DST-Entrust GTI CA,O=Digital Signature Trust Co.,C=US
- CA Certificate: OU=DSTCA E2,O=Digital Signature Trust Co.,C=US
- CA Certificate: OU=DSTCA E1,O=Digital Signature Trust Co.,C=US
- CA Certificate: EMAIL=ca@digsigtrust.com,CN=DST RootCA X2,OU=DSTCA X2,O=DigitalSignature Trust Co.,L=Salt Lake City,ST=Utah,C=us
- CA Certificate: EMAIL=ca@digsigtrust.com,CN=DST RootCA X1,OU=DSTCA X1,O=DigitalSignature Trust Co.,L=Salt Lake City,ST=Utah,C=us
- CA Certificate: EMAIL=ca@digsigtrust.com,CN=DST (UPS) RootCA,OU=United Parcel Service,O=Digital Signature Trust Co.,L=Salt Lake City,ST=Utah,C=us
- CA Certificate: EMAIL=ca@digsigtrust.com,CN=DST (NRF) RootCA,OU=National RetailFederation,O=Digital Signature Trust Co.,L=Salt Lake City,ST=Utah,C=us
- CA Certificate: OU=DST (ANX Network) CA,O=Digital Signature Trust Co.,C=US
- CA Certificate: CN=Deutsche Telekom Root CA 2,OU=T-TeleSec Trust Center,O=Deutsche Telekom AG,C=DE
- CA Certificate: CN=Deutsche Telekom Root CA 1,OU=T-TeleSec Trust Center,O=Deutsche Telekom AG,C=DE
- CA Certificate: OU=Commercial Certification Authority,O=RSA Data Security Inc.,C=US
- CA Certificate: CN=Class 3TS Primary CA,O=Certplus,C=FR
- CA Certificate: CN=Class 3P Primary CA,O=Certplus,C=FR
- CA Certificate: OU=Class 3 Public Primary Certification Authority,O=VeriSign Inc.,C=US
- CA Certificate: OU=Class 3 Public Primary Certification Authority,O=VeriSign Inc.,C=US
- CA Certificate: CN=Class 3 Primary CA,O=Certplus,C=FR

- CA Certificate: OU=Class 2 Public Primary Certification Authority,O=VeriSign Inc.,C=US
- CA Certificate: OU=Class 2 Public Primary Certification Authority,O=VeriSign Inc.,C=US
- CA Certificate: CN=Class 2 Primary CA,O=Certplus,C=FR
- CA Certificate: OU=Class 1 Public Primary Certification Authority,O=VeriSign Inc.,C=US
- CA Certificate: OU=Class 1 Public Primary Certification Authority,O=VeriSign Inc.,C=US
- CA Certificate: CN=Class 1 Primary CA,O=Certplus,C=FR
- CA Certificate: OU=Certisign Autoridade Certificadora AC3S,O=Certisign Certificadora Digital Ltda.,L=Rio de Janeiro,ST=Rio de Janeiro,C=BR
- CA Certificate: OU=Certisign Autoridade Certificadora AC1S,O=Certisign Certificadora Digital Ltda.,C=BR
- CA Certificate: OU=Certisign - Autoridade Certificadora - AC4,O=Certisign Certificadora Digital Ltda.,C=BR
- CA Certificate: OU=Certisign - Autoridade Certificadora - AC2,O=Certisign Certificadora Digital Ltda.,C=BR
- CA Certificate: CN=Certiposte Serveur,O=Certiposte,C=FR
- CA Certificate: CN=Certiposte Classe A Personne,O=Certiposte,C=FR
- CA Certificate: OU=CA 1,OU=CA Data,O=ViaCode,C=GB
- CA Certificate: O=C&W HKT SecureNet CA SGC Root,C=hk
- CA Certificate: O=C&W HKT SecureNet CA Root,C=hk
- CA Certificate: O=C&W HKT SecureNet CA Class B,C=hk
- CA Certificate: O=C&W HKT SecureNet CA Class A,C=hk
- CA Certificate: 0.9.2342.19200300.100.1.3=info@e-trust.be,CN=Belgacom E-Trust Primary CA,OU=MTM,O=Belgacom,C=be
- CA Certificate:  
0.9.2342.19200300.100.1.3=ca@digsigtrust.com,CN=Baltimore EZ byDST,O=Digital Signature Trust Co.,C=US
- CA Certificate: O=Colegio Nacional de Correduria Publica Mexicana A.C.,CN=Autoridad Certificadora del Colegio Nacional de Correduria Publica Mexicana A.C.,C=MX
- CA Certificate: O=Asociacion Nacional del Notariado Mexicano A.C.,CN=Autoridad Certificadora de la Asociacion Nacional del Notariado Mexicano A.C.,C=MX
- CA Certificate: EMAIL=admin@digsigtrust.com,CN=ABA.ECOM Root CA,O=ABA.ECOM INC.,L=Washington,ST=DC,C=US





# 6 Configuring the Secure Audit Server

The Secure Audit server is a tamper-resistant method for monitoring stability, data integrity, and corporate security—all via a centralized server. This chapter describes how to deploy the Secure Audit server, so that it records all access and authorization actions, as well as all policy administrative changes.



Select Access does not support the Secure Audit server on Windows 98.

## Chapter Overview

This chapter outlines how to configure the Secure Audit server. Topics in this chapter include:

- [Understanding the Secure Audit Server](#) on page 93
- [Setting up Server-based Auditing](#) on page 94
- [Configuring the Secure Audit Server](#) on page 95
- [Configuring an Audit Trail](#) on page 101
- [Configuring an Audit Policy](#) on page 110

## Understanding the Secure Audit Server

You can configure your Select Access components—or even third-party applications—to become clients of the server. If you'd like non-Select Access applications to log to the Secure Audit server as well, you must use the Logging API that is included with the SDK to enable this functionality in third-party products. For details, refer to the *HP OpenView Select Access 6.1 Developer's Reference Guide* and the *HP OpenView Select Access 6.1 Developer's Tutorial Guide*.

The configuration of the Secure Audit server appears immediately after the Administration server for a reason: you must configure and start the Secure Audit server before other Select Access components can log to it. While the configuration is similar to the global/default audit settings you configure in the Administration server, the Secure Audit server does not use these settings. This is because the Secure Audit server does not connect to the Policy Store and therefore cannot retrieve default settings. Furthermore, best practices for setting up a

Secure Audit server dictate that you typically configure your Secure Audit server to output events to different destinations than those global settings you configured for Select Access components.



You can create reports from the runtime messages that you have logged—preferably from a non-refutable, digitally signed administrative XML log. Currently, the only two Select Access output destinations that you can create reports from are file and database audit trails. For more details on how to create a report, see [Chapter 14, Creating Reports from Secure Audit Server Output](#), in the *HP OpenView Select Access 6.1 Policy Builder Guide*.

Note, however, that if you are using a signed audit log from a Select Access 5.0 release, the log may not be accepted by Select Access 6.1 unless you installed Patch 2 for Select Access 5.0. This patch resolved a data signing issue that existed in Select Access 5.0, which prevents 6.1 components from using signed logs prior to Patch 2.

## Differences in Message Types

Select Access components can forward messages about:

- System events
- Runtime transactions
- Policy changes with digitally signed entries for a tamper-resistant record of events

You can configure the Secure Audit server to save events to any combination of outputs, including databases, UNIX syslog, Windows event log, and/or files. The Secure Audit server allows you to filter log output; that is, you can configure different output destinations for the following types of audit data:

- Audit component (that is, administration session, authentication, access query)
- Event level (for example, information or warning)

This differentiation allows you to recall significant events that impact your business, including:

- Who accessed a resource.
- What operations an administrator performed during a given period of time.
- What Select Access components generated errors.

## Setting up Server-based Auditing

Select Access components' global/default audit settings (that is, those that you configure at the time of the Administration server's setup) output to the system log by default. Unless you change these common audit settings to log to the Secure Audit server, or unless you create new group settings and/or specific instance overrides, the Secure Audit server is not used.

However, if you do log to the Secure Audit server, configuring a Select Access auditing system involves the steps outlined in [Table 1](#).

**Table 1 Auditing Overview**

Setup Step	Details
<p>1 <i>Setting up the server side:</i> When you install the Secure Audit server, you must configure how it manages incoming logs. The Secure Audit server Configuration Editor allows you to:</p> <ul style="list-style-type: none"> <li>— Separate the incoming messages into different files or databases on the Secure Audit server host.</li> <li>— Forward certain messages to other Secure Audit servers.</li> </ul>	<p>To set up the <a href="#">Secure Audit server</a> on page 95</p>
<p>2 <i>Setting up the client side:</i> When you install and configure any Select Access component, you must configure the audit settings for that component. You can do this with the component's <b>Audit Settings</b> setup screen, so that each Select Access component knows what to do with the log information that you have configured it to collect. If you want the component to log to the Secure Audit server and become one of its clients, you need to output their runtime messages to the Secure Audit server. You can do this via the <b>Audit Trail</b> tab in the <b>Audit Entry</b> dialog box.</p> <p><b>Note:</b> You can configure unique audit settings for each component, or you can use the common settings that you defined when you set up the Administration server.</p>	<p>To set <a href="#">Policy Validator-specific audit settings</a> on page 124 OR To set <a href="#">enforcer-specific audit settings</a> on page 147</p>

## Configuring the Secure Audit Server

The configuration of the Secure Audit server is different from that of other Select Access components in that it does not require the Administration server to manage its configuration parameters. Instead, the Setup Tool stores all configuration parameters in the Secure Audit server's local `auditserver.xml` configuration file. As a result, you cannot modify the Secure Audit server's configuration from the Policy Builder, as the Setup Tool does not write any parameters to the Policy Store.

### Using the Setup Tool

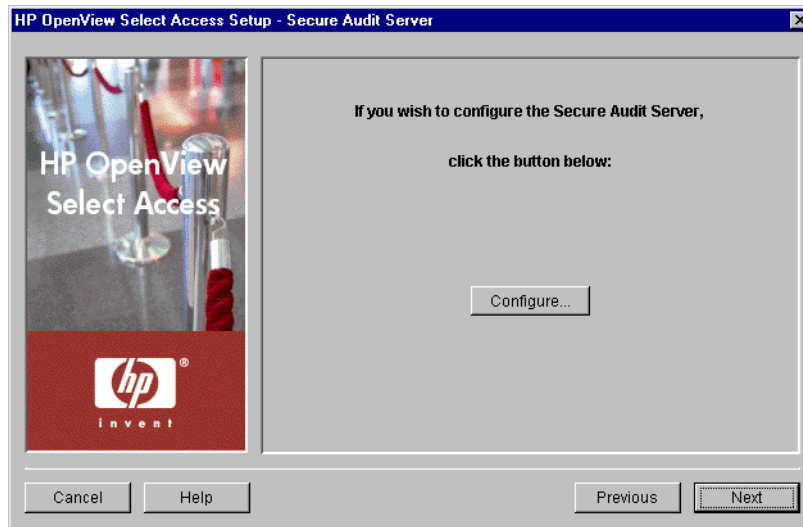
If you choose to configure your Select Access components directly from the installer, the Setup Tool is started for you automatically.

If you choose to configure your Select Access components at a later time, or want to modify your configuration settings, you can run the Setup Tool and access the Secure Audit server's configuration settings at any time.

#### To set up the Secure Audit server

- 1 If the Setup tool is not already started, click **Start**→**Programs**→**HP OpenView**→**Select Access**→**Setup Tool**. The **Component Setup Tool** window appears.

- Click **Next** until you reach the Setup Tool's **Secure Audit server** setup screen, as shown in Figure 1.



**Figure 1 Secure Audit Server Setup Screen**

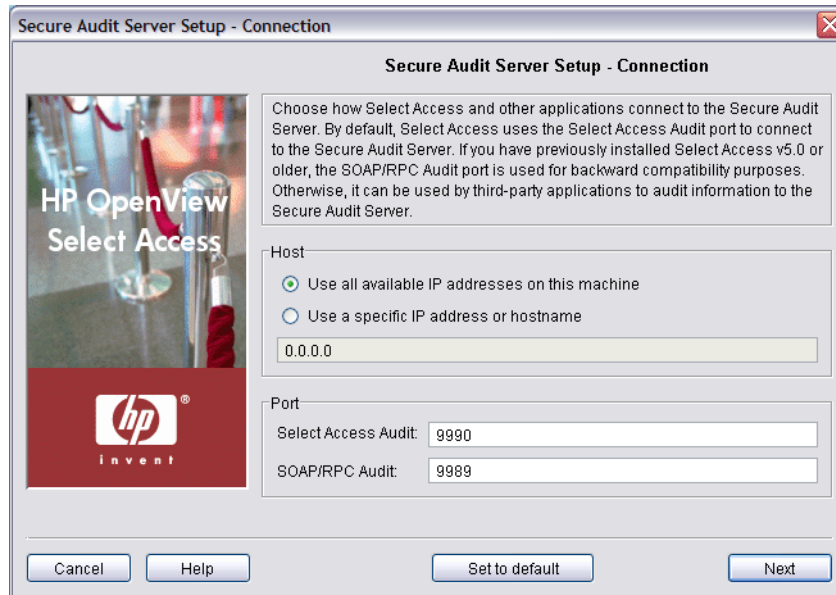
- Click the **Configure** button. The Secure Audit server setup process starts and the **Connection** setup screen appears.
- Complete the setup screens of the Secure Audit server setup process, listed in Table 2, as necessary.

**Table 2 Overview of Secure Audit Server Setup Process**

Setup Screen	Description	Default value(s)
<b>Connection</b> setup screen	Allows you to define the connection information Select Access components will use to connect and forward events and messages to the Secure Audit server. See <a href="#">Configuring the Secure Audit Server Connection Information</a> on page 97.	auto-defined
<b>Audit Settings</b> setup screen	Allows you to configure audit settings specific to the Secure Audit server. See <a href="#">Configuring Server-Specific Audit Settings</a> on page 98.	auto-defined to log all runtime errors
<b>Audit Stream Signing</b> setup screen	Allows you to define whether or not the Secure Audit server uses digital signatures to sign audit entries in your file or database logs. This ensures a level of irrefutability of the audit data. See <a href="#">Configuring Audit Stream Signing</a> on page 99.	disabled
<b>Finish</b> setup screen	Allows you to commit your configuration settings to the Secure Audit server's bootstrap XML file, and automatically restart the server. See <a href="#">Completing the Secure Audit server Setup Process</a> on page 100.	enables server restart

## Configuring the Secure Audit Server Connection Information

The **Connection** setup screen, shown in [Figure 2](#), allows you to define connection information for the Secure Audit server. Other Select Access components that are clients of the Secure Audit server use this information to forward events and messages.



**Figure 2** Connection Setup Screen

### To set connection information for the Secure Audit server

- 1 Review HP's recommended values. To customize these values, modify any of the screen's fields as needed.
  - **Host:** Required. Choose which IP address Select Access components use to connect to the host computer of the Secure Audit server.

Click **Use all available IP addresses on this machine** to try all IP addresses configured for the host computer. HP recommends you use this option: if one address happens to become unavailable, Select Access components try other addresses to find one that is available.

Click **Use a specific IP address or hostname** to use a single address only and enter the details in the corresponding text box that follows this option.

- **Port:** Required. Enter the port(s) that Select Access components and possibly other third-party components use to audit to the Secure Audit server.

If you are installing Select Access for the first time or are upgrading from Select Access 6.0, configure the **Select Access Audit** port. The default value for this port is 9990.

- ▶ Select Access components should log to this port whenever possible. Because the protocol is a proprietary protocol unique to Select Access, network performance is approximately two times faster than the SOAP/RPC protocol.

The SOAP/RPC protocol should be restricted to third-party application logging. For details on how to extend auditing to third-party applications with Select Access' Logging API, refer to the *HP OpenView Select Access 6.1 Developer's Reference Guide* and the *HP OpenView Select Access 6.1 Developer's Tutorial Guide*.

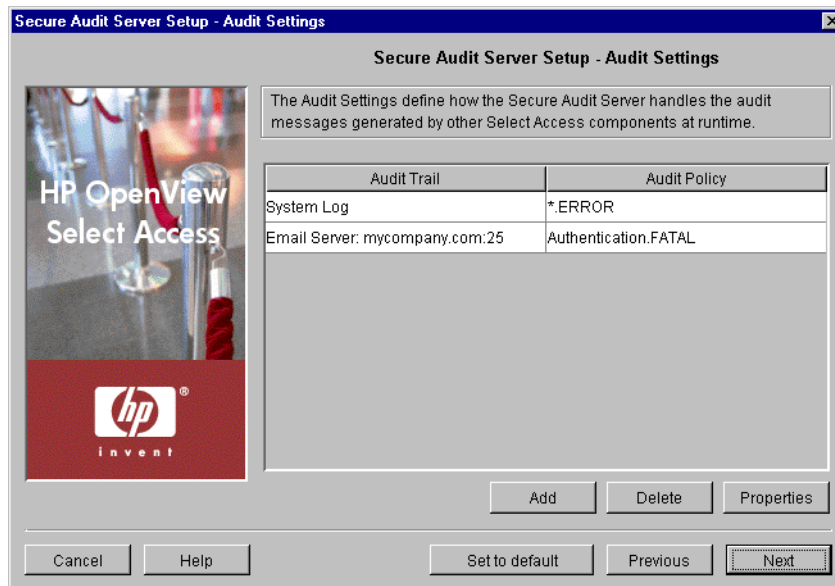
If you are upgrading Select Access from a version previous to Select Access 6.0 or would like your third-party components to audit to the Secure Audit server, configure the **SOAP/RPC Audit** port. The default value for this port is 9989.

- 2 Click **Next**. The **Audit Settings** setup screen appears. See [Configuring Server-Specific Audit Settings](#) on page 98.

## Configuring Server-Specific Audit Settings

The **Audit Settings** setup screen, shown in [Figure 3](#), allows you to configure auditing settings for the Secure Audit server only. The Secure Audit server uses these unique settings to determine which events to log.

- ▶ The Secure Audit server does not use the default settings you configured during the Administration server's setup. This is because the Secure Audit server does not connect to the Policy Store and therefore cannot retrieve default settings. Furthermore, best practices for setting up a Secure Audit server dictate that you typically configure your Secure Audit server differently than other Select Access components.



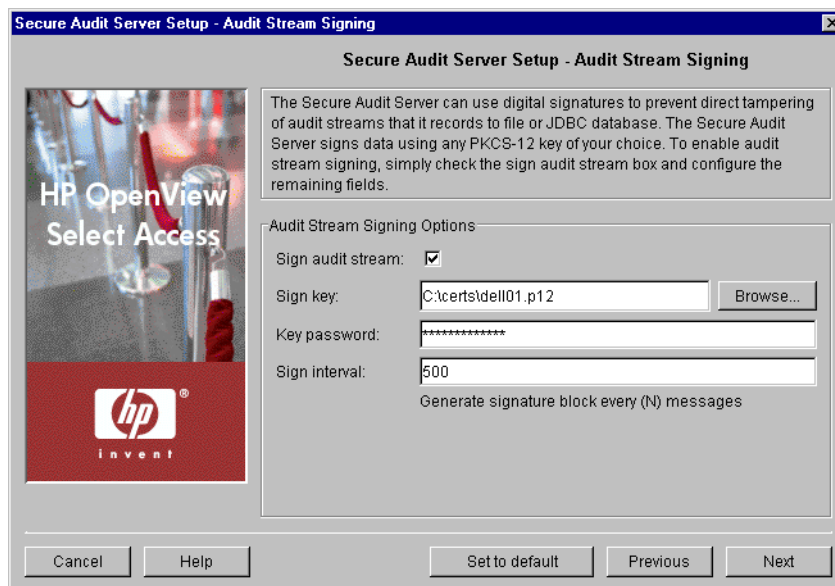
**Figure 3** Audit Settings Setup Screen

## To configure Secure Audit server-specific audit settings

- 1 To create or modify audit settings rows, click **Add** or **Properties** respectively. The **New Audit Entry** dialog box appears displaying two tabs, **Audit Trail** and **Audit Policy**. These tabs correspond to the columns of the **Default Audit Settings** setup screen.
- 2 Configure the tabs of the **New Audit Entry** dialog box as necessary.
  - For information on configuring audit trail settings, see [Configuring an Audit Trail](#) on page 101
  - For information on setting audit policy, see [Configuring an Audit Policy](#) on page 110When you configure the tabs of the **New Audit Entry** dialog box, then click **OK**, the wizard adds a new row below the one you have selected and the Setup Tool automatically populates the cells.
- 3 To remove an empty or populated row, select the entry in question and click **Delete**.
- 4 Click **Next**.
  - If you plan to output collected component logs to either a database or file, the **Audit Stream Signing** setup screen appears. See [Configuring Audit Stream Signing](#) on page 99.
  - If you plan to output collected component logs to any other destination, skip to step [Completing the Secure Audit server Setup Process](#) on page 100.

## Configuring Audit Stream Signing

The **Audit Stream Signing** setup screen, shown in [Figure 4](#), allows you to configure whether or not you want to sign your file or database logs. This prevents tampering of data recorded to these log outputs.



**Figure 4** Audit Stream Signing Setup Screen

## To configure audit stream signing

- 1 Review HP's recommended values. To customize these values, modify any of the screen's fields as needed.
  - **Sign audit stream:** Optional. Check this box to enable signing of your text file or database logs.
  - **Sign key:** Required when you check the previous box. Select the PKCS#12 certificate. It generally has an extension like `.p12` or `.pfx`.
    - ▶ If you do not currently have a PKCS-formatted certificate, export one from your browser (if it exists), or contact your CA about obtaining one.
  - **Key password:** Required when you check the first box. Enter the password required to decrypt the private key and enable signing.
  - **Sign interval:** Required when you check the first box. Enter the number of messages that the server signs at a time. The narrower the signing interval, the easier it is for you to identify when someone has tampered with one or more messages. However, the narrower the signing interval, the higher the network overhead. In most cases, a value between 500-1000 is sufficient.
- 2 Click **Next**. The **Finish** setup screen appears. See [Completing the Secure Audit server Setup Process](#) on page 100.

## Completing the Secure Audit server Setup Process

The **Finish** setup screen informs you that you have completed all setup tasks for the Secure Audit server and allows you to automatically restart the server.

### To complete the Secure Audit server setup

- 1 If you want to configure other components, click the **Start now** box. By checking this box, the Setup Tool starts the Secure Audit server immediately after it records the configuration parameters you have just set.
- 2 Click **Finish** to commit the parameters to the Secure Audit server's local bootstrap file and start this component as a service on Windows or as a daemon on Unix.



This bootstrap file contains startup and general configuration information for the Secure Audit server. Modifying or moving this file could result in the Secure Audit server being unable to start correctly. You should ensure that you protect this file using both logical and physical controls.



This bootstrap file also contains a configuration parameter that is not configurable by the Setup Tool: the Timeout parameter. The Timeout parameter specifies the amount of time to elapse when a connection attempt is made to the Secure Audit server before the connection is terminated. The default value for this parameter is 15 seconds. If you modify this value, it is not overwritten with subsequent reconfigurations using either the Setup Tool or the Policy Builder



If you have installed any other components on this computer, the next component's setup screen appears. For details, see [To configure Select Access with the Setup Tool](#) on page 58.

## Configuring an Audit Trail

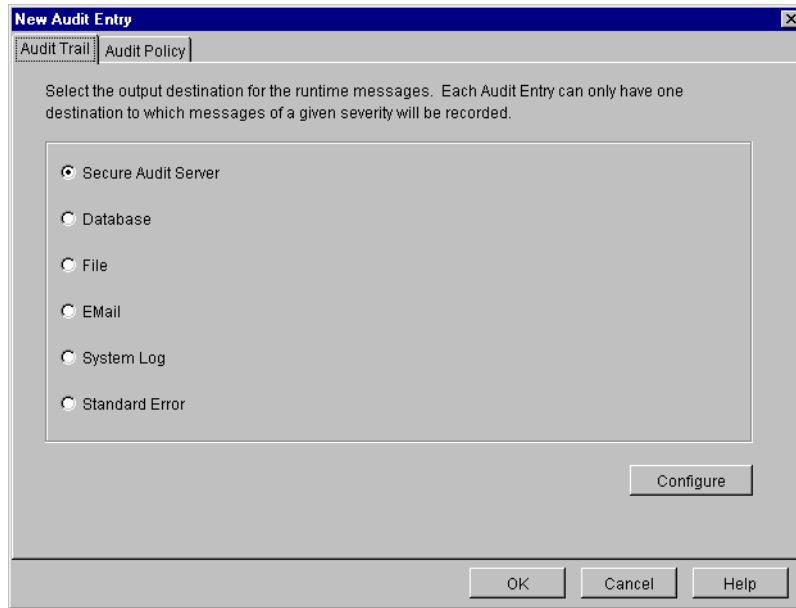
An **Audit Trail** defines the output destination of the logged information. An audit trail is just one half of an audit entry. Each audit entry line can only have one audit trail to which specific component messages of a given severity are recorded.

- ▶ Different audit policies, however, can have different audit trails configured for them. By configuring overlapping audit policies, you can send events to more than one destination.

### To choose an Audit Trail

- 1 Run the Setup Tool as described in [To configure Select Access with the Setup Tool](#) on page 58.
- 2 From the Setup Tool, click **Next** until you reach the setup screen for either the:
  - Secure Audit server, to configure server-side audit settings. Once you have set up the Secure Audit server, you need to set up the client side as well.
  - Another Select Access component, to configure client-side audit settings. You can set the component to either become a client of the Secure Audit server, or you can set it to record events to another destination.
- 3 Do one of the following:
  - To create a new **Audit Setting**, click **Add**.
  - To modify an existing **Audit Setting**, select a row and click **Properties**.

The corresponding **Audit Entry** dialog box appears displaying the **Audit Trail** tab as shown in [Figure 5](#).



**Figure 5 Audit Trail Tab**

- 4 Select the output destination for the event you are configuring, and click the **Configure** button to set up that destination. The table below summarizes the differences between these options.

➤ You can configure different audit trails for different events.

**Table 3 Configuring the Audit Trail Tab**

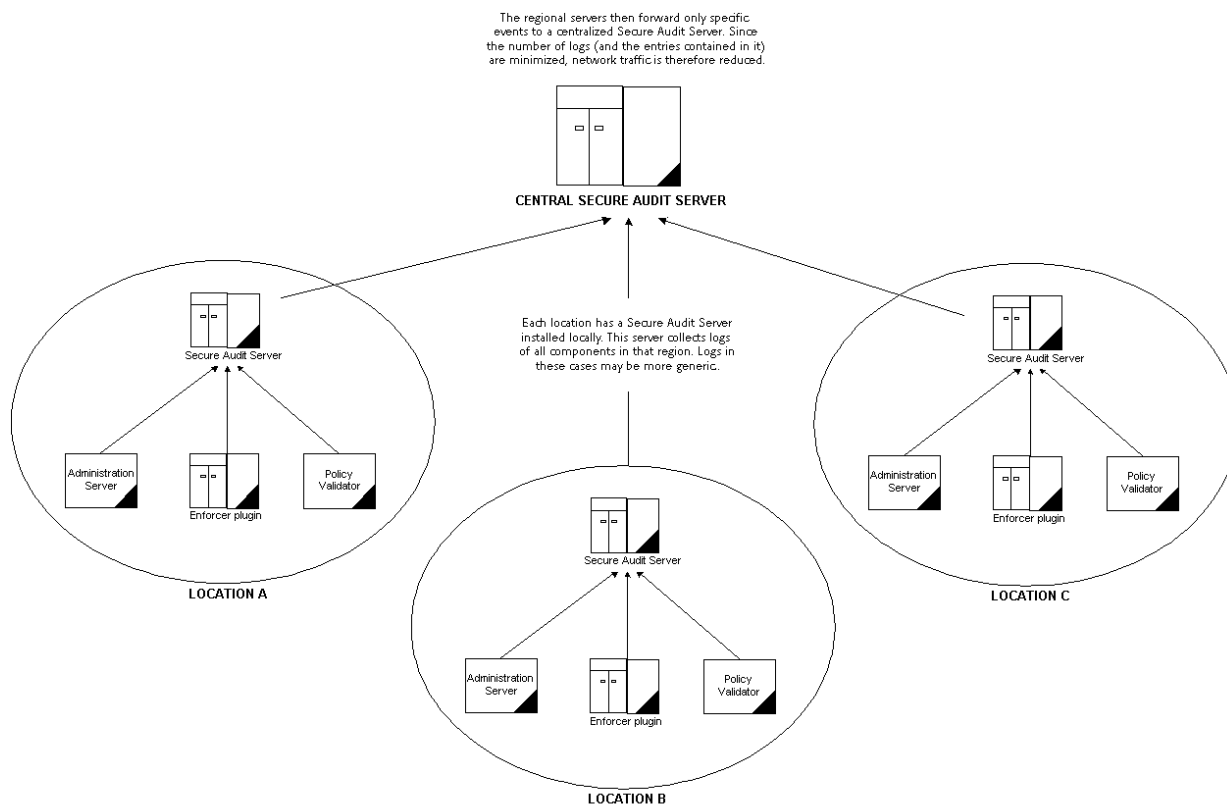
<b>Output Destination</b>	<b>Description</b>
<b>Secure Audit Server</b>	Outputs to a Secure Audit server. In some cases you may want to forward messages from one server to another. For example, all Select Access components at a site might send their messages to a site-wide server, and their site-wide server in turn send critical errors to a central enterprise-wide server.
<b>Database</b>	Outputs to a Java DataBase Connectivity (JDBC) compliant database.
<b>File</b>	Outputs to a text file. For example, you can send less important messages to a file to reduce network overhead.

**Table 3 Configuring the Audit Trail Tab (cont'd)**

Output Destination	Description
Email	Outputs to one or more email addresses. For example, if a Policy Validator or an Enforcer plugin experiences a failure, you can configure email alerts so an administrator is immediately notified.
System Logging	Outputs to a Windows or Unix system log. Select Access components log to the system log by default.
Standard Error	Outputs to an error stream. For example, you want to troubleshoot a specific instance of a component, and choose to display events to a window.

## Configuring a Secure Audit Server

Instead of recording to a log file or to a database, select this option to record events to a Secure Audit server. A Secure Audit server allows you to consolidate output from Select Access components distributed across your network. This method allows you to minimize network traffic: logs that only record a specific type of event are forwarded to a single, centralized destination, as shown by the graphic below.

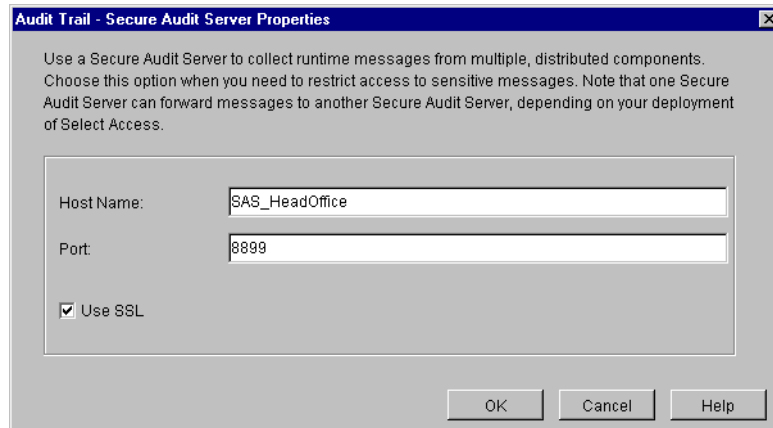


**Figure 6 Secure Audit Server Pools Forwarding Events to a Central Server**

## To configure a Secure Audit server

- 1 From the **Audit Trail** tab on the **New Audit Entry** dialog box:
  - Choose the **Secure Audit server** option.
  - Click the **Configure** button.

The **Audit Trail—Secure Audit server Properties** dialog box appears.



**Figure 7 Audit Trail—Secure Audit server Properties Dialog Box**

- 2 In the **Host Name** field, enter either the host name or IP address of the server.
- 3 In the **Port** field, enter the port on which the server will listen for messages. By default, the port for the Secure Audit server is 8899.
- 4 Click **OK**.

## Configuring a Database

A JDBC database is a more flexible alternative to log files or system logs. Choose this output destination if you have a database installed and want to take advantage of its abilities. You must also choose this option if you enabled database reporting when you configured your Administration server. Currently, Select Access supports two database types:

- MS SQL
- Oracle

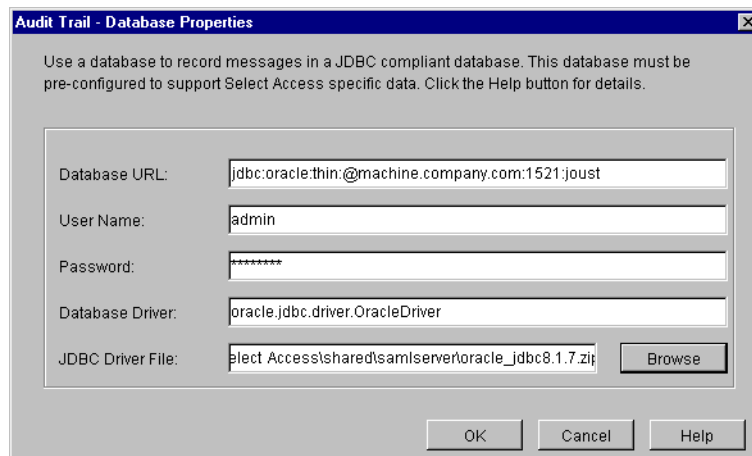
To facilitate this ability to review data more easily, Policy Builder allows you to create reports from the runtime messages your database contains.

## To configure a database

Using a database requires that you set it up correctly. This entails enabling database reporting when you configured the Administration server during a custom configuration. It also entails creating database tables correctly. For details, see [Creating Database Tables](#) on page 106. For more details on the conditions that allow you to create a report from your database, see [Chapter 14, Creating Reports from Secure Audit Server Output](#), in the *HP OpenView Select Access 6.1 Policy Builder Guide*.

- 1 Ensure you have done the following:
  - Run the correct SQL script for your database. For details, see [Creating Database Tables](#) on page 106.
  - Enabled database reporting when setting up the Administration server. For details, see [Configuring the Administration Server](#) on page 63.
- 2 From the **Audit Trail** tab on the **New Audit Entry** dialog box:
  - Choose the **Database** option.
  - Click the **Configure** button.

The **Audit Trail—Database Properties** dialog box appears.



**Figure 8 Audit Trail—Database Properties Dialog Box**

- 3 In the **Database URL** field, enter a URL for the database. The URL must be configured using syntax that is specific to your JDBC driver. For example, if you are using Oracle, the syntax for that driver is:

```
<client>:@<machine.domain.com>:<port>:<SID>
```

Where:

- `client` is the name of the JDBC client you want the Secure Audit server to use.
- `machine.domain.com` is the DNS name of the computer that is hosting the database.
- `port` is the port number of the database. By default, 1521 is the port for JDBC databases.

- `SID` is the system identifier for the database instance. A database can have multiple instances.

▶ If you are unsure what the required URL syntax for your database is, refer to your driver's documentation.

- 4 In the **User Name** field, specify a username for this database. You need this to set up the driver.
- 5 In the **Password** field, specify a password for this database. You need this to set up the driver.
- 6 In the **Database Driver** field, enter a database driver class name. This driver is used to accept generic commands from Select Access and translate them into specialized commands for the database you are using.
- 7 In the **JDBC Driver File** field, click **Browse** and locate the JDBC driver's archive file. Select Access components use this class to write events to the database.

▶ The database driver value is case-sensitive. Be sure you configure this parameter carefully or the JDBC database will not work correctly.

▶ If you are unsure what the required class name for your database is, refer to your driver's documentation.

▶ If you are configuring an MS JDBC driver, note that the version tested against Select Access is v2.2.0022. To check which version you are using, open the `read.me` file shipped with the driver. The version number appears in the document's header.

If you need to list multiple driver files, you cannot use the **Browse** button. Instead, you need to type the path and filename to all files, separating each file with a semi-colon (;).

▶ If any of the paths or filenames include a space, all files must be surrounded by quotation marks.

For example, if you are using a Microsoft database, you would type the filenames like this:

```
"C:\Program Files\MS_JDBC\lib\msbase.jar; C:\Program
Files\MS_JDBC\lib\mssqlserver.jar; C:\Program
Files\MS_JDBC\lib\msutil.jar"
```

- 8 Click **OK**.

## Creating Database Tables

Select Access has included small SQL scripts that automate much of the process of creating database tables. By default, these scripts are installed in the `<install_path>/shared` folder.

- `OracleLogSetup.sql`: Creates and sets up the requisite tables in an Oracle database so Select Access components can log messages to it.
- `MSSQLLogSetupTable.sql`: Creates the requisite tables in a Microsoft database so Select Access components can log messages to it.
- `MSSQLLogSetupView.sql`: Sets up the tables in the Microsoft database that were created with the previous script.

Use these utilities to automatically create tables in the JDBC database that you are going to use. By using the utilities rather than creating the tables manually, you ensure that your database is compatible with the Secure Audit server. Unless tables are set up correctly, the Secure Audit server cannot log events to this database.

### To run your setup SQL script

- 1 Copy the corresponding SQL file(s) to the SQL client computer.
- 2 Create an account for the Select Access component that writes to the database.
- 3 Log into the database with that account, using an SQL client.
  - ▶ Use the username and password you configured in the **Database Properties** dialog box.
- 4 Run the corresponding SQL file(s) to create and configure database tables correctly. If you have a Microsoft database, run the following scripts in this order:
  - MSSQLLogSetupTable.sql
  - MSSQLLogSetupView.sql

### Configuring a Log File

A log file is a simple Windows or Unix text file that captures log messages in XML. You can use the file you select to create reports from the runtime messages these log files contain.

- ▶ When running IIS6 with the IIS Enforcer plugin on Windows 2003, the Enforcer plugin is unable to log messages to a file unless the proper permissions have been assigned. In order to configure IIS6 to log to a file, the NETWORK\_SERVICE account must have write permission to the log file.
- ▶ If IIS6 is configured for Integrated Windows Authentication, then write permission must be given to all possible users if you have configured the IIS Enforcer plugin to log to a file. The reason for this is because IIS will impersonate the user and serve the request under that user account. Because the IIS Enforcer plugin code is not executed until after the impersonation takes place, the user must have write permission to the log file in order for messages to be logged there.

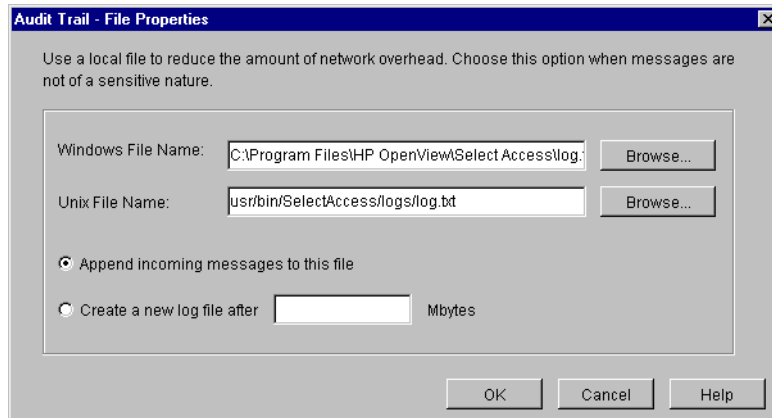
For more details on how to create a report, see [Chapter 14, Creating Reports from Secure Audit Server Output](#), in the *HP OpenView Select Access 6.1 Policy Builder Guide*.

- 

### To configure a log file

- 1 From the **Audit Trail** tab on the **New Audit Entry** dialog box:
  - Choose the **File** option.
  - Click the **Configure** button.

The **Audit Trail—File Properties** dialog box appears.



**Figure 9 Audit Trail—File Properties Dialog Box**

- 2 Specify a log file local to the Secure Audit server.
  - Configure the **Windows File Name** field, if your server is on a Windows host computer.
  - Configure the **Unix File Name** field, if your server is on a Unix host computer.
- 3 Enable one of the following options:
  - If you want to use a single file on each platform, click the **Append incoming messages to this file** option.
  - If you want to create multiple files on each platform, click the **Create new log file after** option. If you select this option, specify a maximum file size in megabytes between one megabyte and two gigabytes.

When a file reaches the configured size, the Select Access component looks to see what filenames exist. For example, if your filename is `PB.LOG`, it looks for `PB.LOG`, `PB.LOG.1`, `PB.LOG.2`, and so on until it finds a file number that does not exist yet. Only then does it write to that new file, and increments the name by one. Once a log file reaches the specified size, it creates a new file. The sequence keeps increasing as long as the audit server is running.

➤ For components other than the Secure Audit server, the files generated by the **Create new log file after** option are Unix-like syslog logs. You cannot view these logs using the Select Access Audit Report Viewer or other standard XML viewers.

- 4 Click **OK**.

## Configuring an Email Alert

An email alert is a message sent to the addresses you specify, to notify them of a specific (usually severe) event that has been triggered.

- You can also configure an email alert using an alert decision point in the Rule Builder.
- 🚩 HP recommends that you limit the number of events that use this method to minimize the amount of network overhead that can occur as a result.





The Secure Audit server does not support sending emails to a Microsoft Exchange server if you have enabled authentication on the Exchange server.

## To configure an email alert

- 1 From the **Audit Trail** tab on the **New Audit Entry** dialog box:
  - Choose the **Email** option.
  - Click the **Configure** button.

The **Audit Trail—Email Properties** dialog box appears.

Audit Trail - Email Properties

Set up either the Audit Server or Administration Server to send an Email that alerts one or more recipients of significant runtime events.

SMTP Server Name: SMTPserver1.mycompany.com

SMTP Server Port: 25

To Address(es): it@mycompany.com  
Separate multiple Email addresses with commas.

From Address: sa@mycompany.com

From Name: Select Access

OK Cancel Help

**Figure 10 Audit Trail—Email Properties Dialog Box**

- 2 In the **SMTP Server Name** field, enter the fully qualified name or IP address of the SMTP server that you use as your email server.
- 3 In the **SMTP Server Port** field, enter the port number used by your email server. The default SMTP server port is 25.
- 4 In the **To Address(es)** field, enter the administrator’s email address to which the Select Access component sends a message when it triggers an event. You can enter multiple email addresses by separating them with a comma (,).
  - ▶ If you incorrectly format an email address, or separate it with the wrong character, Select Access highlights the line in red.
- 5 In the **From Address(es)** field, enter the email address from which the component sends a message when it triggers an event.
  - ▶ You can only enter one address in this field. If you enter more than one email address, Select Access highlights the line in red.
- 6 In the **From Name** field, enter the sender alias that the component uses to send the email message.
- 7 Click **OK**.

## Configuring System Logging

A system log records Select Access-specific events to your operating system's log. The log Select Access components record messages to depends on whether it is output on a Windows or Unix host computer.



Carefully manage the Windows Event log if you intend to use it over long periods of time—especially when it contains sensitive information.



The Unix syslog log has a 1024 byte limit on log messages. Many Select Access audit messages are longer and can be truncated.

### To configure system logging

- 1 From the **Audit Trail** tab on the **New Audit Entry** dialog box, choose the **System Log** option.  
Select Access components automatically output events to this location depending on the host computer of the component:
  - Windows Event Log
  - Unix syslog
- 2 Click **OK**.

## Configuring a Standard Error Stream

You can output to a systems standard error stream. Select Access components discard standard errors by the operating system as it is meant as a short-term method of capturing runtime messages.



Ensure you only output events to this output destination under the recommendation of the HP OpenView Select Access Support Team.

### To log to standard error

- 1 From the **Audit Trail** tab on the **New Audit Entry** dialog box, choose the **Standard Error** option.
- 2 Click **OK**.

## Configuring an Audit Policy

An **Audit Policy** defines the components and levels of events that components record to the configured destination.

### How you create audit policies

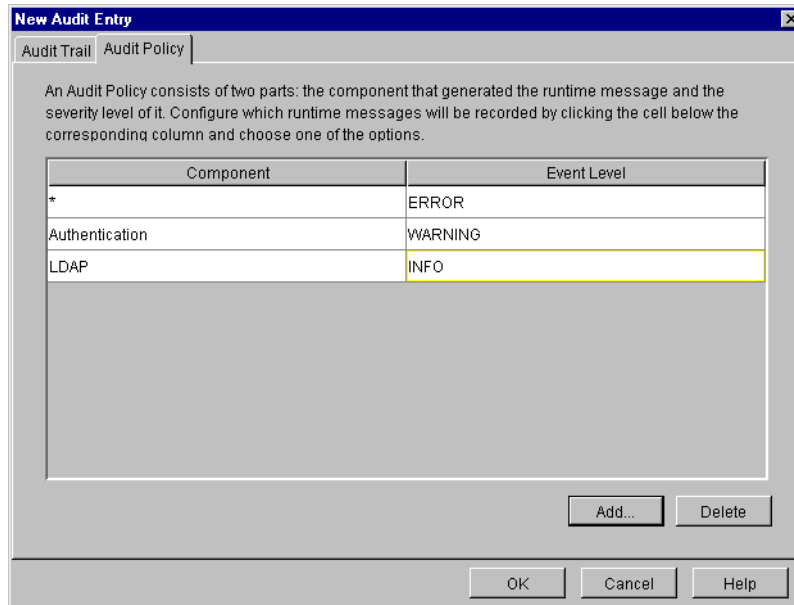
You configure an audit policy via the **Audit Entry** dialog box. There are two cells:

- **Component:** Click this cell to select the Select Access stream that you want to log events and messages from.

- **Event Level:** Click this cell to filter events and messages based on their level of severity.



Different audit policies can have different audit trails configured for them. By configuring overlapping audit policies, you can send events to more than one destination.



**Figure 11 New Audit Entry Dialog Box: Audit Policy Tab**

### To create an Audit Policy

- 1 For either the Setup Tool or the Setup Wizard, click **Next** until you reach the **Audit Settings** setup screen.
- 2 Do one of the following:
  - To create a new **Audit Setting**, click **Add**.
  - To modify an existing **Audit Setting**, select a row and click **Properties**.

The corresponding **Audit Entry** dialog box appears.

- 3 Click the **Audit Policy** tab to identify the events you want to record.
- 4 To add a new policy to your list of policies, click **Add**.
- 5 To choose the Select Access stream where you want events and messages logged, click the **Component** cell and choose one of the following:
  - **\***: Records all events and messages for all streams listed below.
  - **Admin Session**: Records events and messages that relate to administration login and logout.
  - **Alert**: Records messages generated from an alert decision point that is part of an existing conditional rule.
  - **Authentication**: Records events and messages that relate to authentication methods and Enforcer plugins.

- **Cache:** Records events and messages that relate to the caching of identity information and access rules in the Policy Validator.
- **Certificate:** Records events and messages that relate to certificates. For example, processing a certificate query involves multiple processes. Occasionally a certificate query for a transient identity (that is, one that has been synthesized because user data is in a different data source) might take priority over another query. If another query is interrupted by a certificate query, you see an informational message that says: short-circuiting. This just means that the Policy Validator is not rerunning the complete certificate verification process.
- **Enforcer plugin:** Records events and messages generated by your plugins on your network.
- **LDAP:** Records events and messages that relate to activity between the directory server and Select Access components.
- **Operation:** Records general operation of Select Access components.
- **Password Management:** Captures any password reset events or messages you require.
- **Policy:** Records events and messages that relate to access policies, when someone adds, deletes, and modifies a policy, and by whom.
- **Query:** Records all queries to Policy Validator. If you choose to log query information, Policy Validator logs a message for every access request. On a busy site, this can result in a lot of data being generated as well as a lot of overhead.
- **SOAP Message:** Records log messages between the Audit server and the respective Select Access component acting as the server's client.
- **System:** Records all system messages.

▶ Select Access also logs to a *Signing stream*. This component stream is not configurable; however, it is used by components to log internal messages with respect to tamper-resistant logging, if you configure a Secure Audit server to sign its logs.

- **Workflow:** Records all workflow events.

6 To filter events and messages based on their level of severity, click the **Event Level** cell and choose one of the following:

▶ When you select a level, you will record all messages and events from that level of severity and higher.

- **DEBUG:** Records debugging and trace messages. You are only to use this option when requested by the HP OpenView Select Access Support team.
- **INFO:** Monitors communication information, administration login and logout, and changes to authentication method, directory entries, rules, and so on.
- **WARNING:** Records warnings that occur.
- **ERROR:** Records all exceptions that occur in the component.
- **FATAL:** Records fatal exceptions only.

7 To delete an audit policy, select a row from the list policies and click the **Delete** button.

▶ For a complete list of supported policy combinations, see [Supported audit policy combinations](#) on page 244 in the *HP OpenView Select Access 6.1 Policy Builder Guide*





---

# 7 Configuring the Policy Validator

The Policy Validator is Select Access's evaluation engine. It decides when and how to authorize identity access to a given resource. This chapter describes how to deploy this component on your network.

## Chapter Overview

This chapter outlines how to configure the Secure Audit server. Topics in this chapter include:

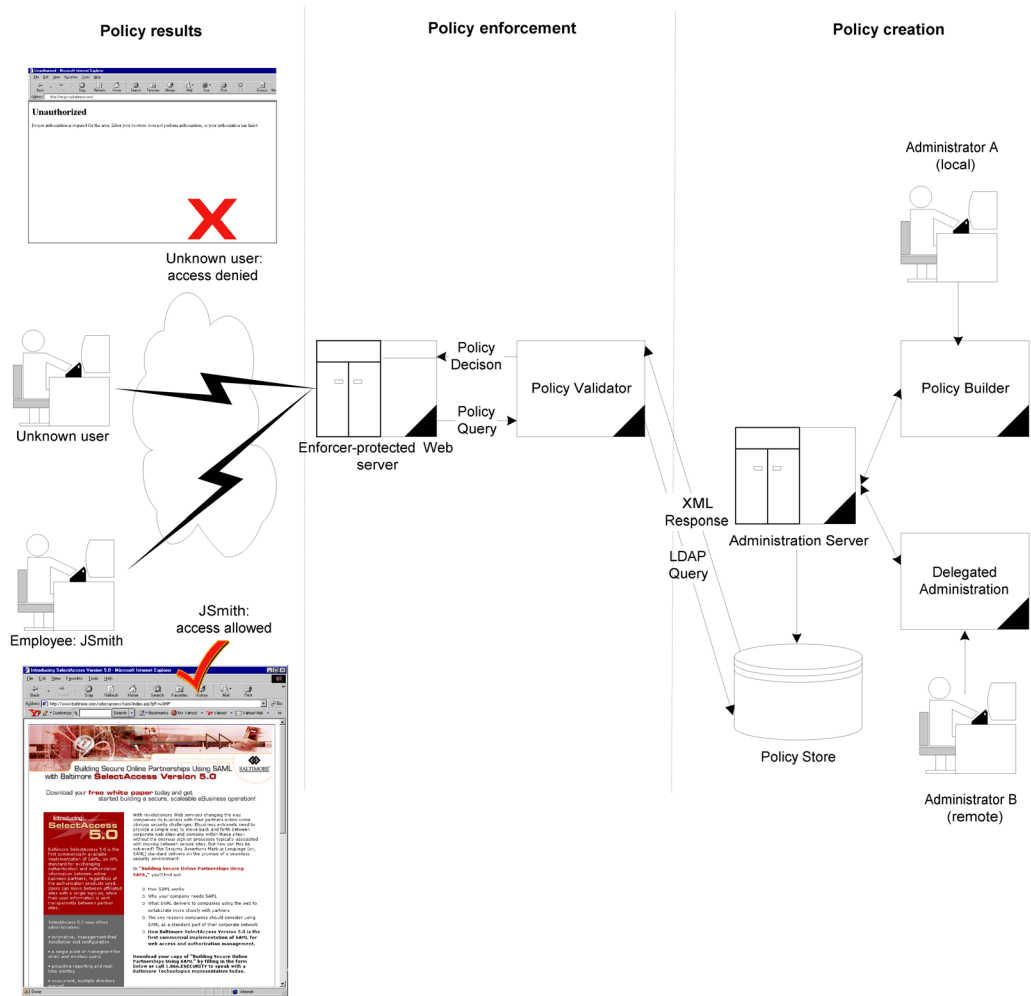
- [How Does the Policy Validator Work?](#) on page 115
- [Configuring the Policy Validator](#) on page 117

## How Does the Policy Validator Work?

Based on information sent to it as XML queries, the Policy Validator reads policies from the directory server and determines whether or not to allow the access request. As shown in [Figure 1](#), once it makes an evaluation and determines an outcome, the Policy Validator passes a response to the Enforcer plugin, which then enforces the decision.



The Policy Validator performs its internal evaluation logic using Validator decider plugins. You can use standard plugins shipped with Select Access, or create new decider plugins with Select Access APIs. For details, see the *HP OpenView Select Access 6.1 Developer's Tutorial Guide* and the *HP OpenView Select Access 6.1 Developer's Reference Guide*.



**Figure 1 How the Policy Validator Works**

If the Policy Validator authenticates an identity, it generates and signs a cookie. When that identity accesses resources, the browser passes the cookie back to the Policy Validator. If this Policy Validator is not the same one that issued the cookie, it goes to the directory server to get public-key information to verify the cookie. If the Policy Validator verifies the cookie, it then allows the identity to access the resource.



If any administrator (local or remote) changes security policies while the Policy Validator is running, ensure they immediately clear the Policy Validator's cache. Otherwise, the Policy Validator is not aware of the change and it can make incorrect access decisions as a result.



## Configuring the Policy Validator

The Policy Validator settings are initially configured via the Select Access Setup Tool. Because the Setup Tool is installed with the Select Access components, you can modify your settings at any time.

▶ You can also modify certain parameters that the Administration server writes to the Policy Store via the **Tools→Configure Components** command in the Policy Builder. For details, see [Chapter 16, Modifying Components' Central Configuration Parameters](#), in the *HP OpenView Select Access 6.1 Policy Builder Guide*.

▶ If you do not configure all your Policy Validators before configuring Enforcer plugins, the Enforcer plugin's bootstrap XML configuration file only includes the names of Policy Validators that were available at that time.

This can be problematic if you create a test or pilot deployment that initially includes only one Policy Validator, but add multiple new Policy Validators during a full Select Access deployment. Potentially, any test Enforcer plugins (as well as your delegated administration Enforcer plugin) will not be able to failover and/or round robin to the new Policy Validators if the test Policy Validator fails. If you must stagger your deployment, you should re-run the Setup Tool for your existing Enforcer plugin to ensure all new Policy Validators are written to its `enforcer.xml` file.

### The Policy Validator's Main Setup Types

Before you begin, you need to understand the difference between two of the general setup types you can choose.

- **Typical:** Use HP's recommended setup values. A **Typical** setup reduces the number of steps and minimizes the complexity of the Policy Validator's setup.
- **Custom:** Modify recommended values to meet the needs of your network and/or business environment. A **Custom** setup increases the number of steps and increments the complexity of the Policy Validator's setup.

Whether you choose one or the other depends on how much you need to customize the configuration of the Policy Validator. You can use recommended values that the Setup Tool automatically configures with a **Typical** setup. To allow you to more easily identify what type of setup you need to perform, [Table 1](#) summarizes the Policy Validator's setup tasks from a high level.

▶ If you modify any of the Administration server's parameters that affect the configuration of the Policy Store at any time, reconfigure and restart your Policy Validators as well. This ensures that the Setup Tool propagates the corresponding configuration changes to them.

### Using the Setup Tool to Configure the Policy Validator

If you choose to configure your Select Access components directly from the installer, the Setup Tool will be started for you automatically.

If you choose to configure your Select Access components at a later time, or want to modify your configuration settings, you can run the Setup Tool and access the Policy Validator's configuration settings at any time.

- ▶ If you modify the Policy Validator's IP address or port, you can adversely affect the Enforcer plugin's ability to communicate with other parts of the Select Access system. If you change either of these configuration parameters, ensure you refresh the Enforcer plugin's configuration by re-running the Setup Tool for each plugin.

## To configure the Policy Validator

- 1 If the Setup tool is not already started, click **Start**→**Programs**→**HP OpenView**→**Select Access**→**Setup Tool**. The **Component Setup Tool** window appears.
- 2 In the Setup Tool, click **Next** until you reach the Setup Tool's **Policy Validator** setup screen.



**Figure 2 Policy Validator Setup Screen**

- 3 Click the **Configure** button. The **Policy Validator** setup process starts and the **Contact the Administration server** setup screen appears.
  - ▶ This screen does *not* appear if you have previously configured the Administration server during your Setup Tool session, as the Setup Tool already has the information needed to connect to it. In this case, the **General** setup screen will appear instead.

- 4 Complete the setup screens of the Policy Validator setup process, listed in [Table 1](#), as necessary.

**Table 1 Overview of Policy Validator Setup Process**

Setup screen	Description	Default value(s)
<b>Contact the Administration Server</b> setup screen	Allows the Setup Tool to connect to the Administration server, so it can manage the Policy Validator's configuration parameters and request the common and/or group configuration parameters for it. See <a href="#">Connecting to the Administration Server</a> on page 120.	auto-defined
<b>General</b> setup screen	Allows you to choose one of two setup types: <ul style="list-style-type: none"> <li>• <b>Typical:</b> Use HP's recommended setup values.</li> <li>• <b>Custom:</b> Modify the recommended values to meet the needs of your network and/or business environment.</li> </ul> See <a href="#">Choosing Your Setup Type</a> on page 121.	Typical
<b>Address, Port and ID</b> setup screen	Displayed for Custom setup type only. Allows you to define the Policy Validator connection parameters. See <a href="#">Setting Connection Parameters for the Policy Validator</a> on page 122.	auto-defined
<b>Audit Settings</b> setup screen	Displayed for Custom setup type only. Allows you to configure audit settings specific to the Policy Validator. See <a href="#">Configuring Validator-Specific Audit Settings</a> on page 124.	inherit common settings defined by the Administration server
<b>Secure Identity Credentials</b> setup screen	Displayed for Custom setup type only. Allows you to define data encryption settings. The Policy Validator uses this information to create cookies and nonces. Select Access components use cookies and nonces to authenticate identities without requiring them to provide identity credentials each time they access a Select Access-protected resource. See <a href="#">Defining Data Encryption Settings</a> on page 125.	auto-defined

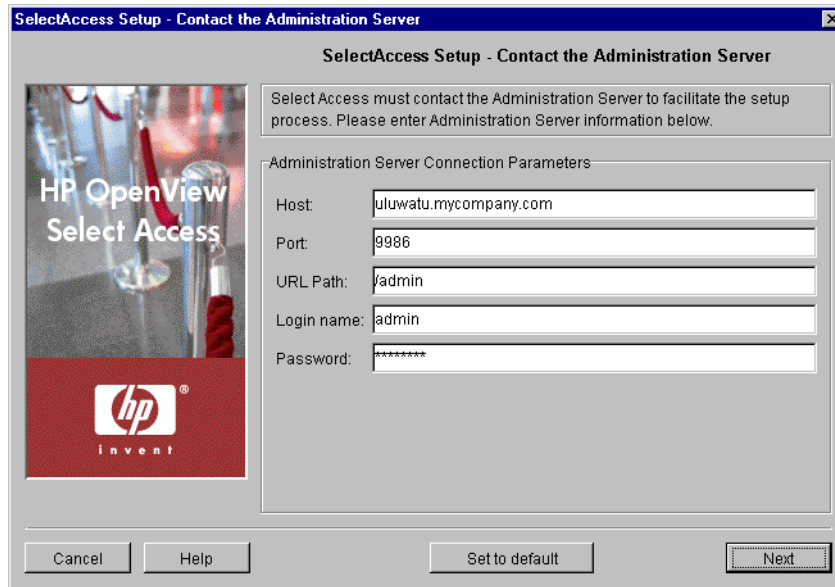
**Table 1 Overview of Policy Validator Setup Process (cont'd)**

Setup screen	Description	Default value(s)
<b>Password Dictionary</b> setup screen	Displayed for Custom setup type only. Allows you to specify a password dictionary, if you intend to use a password policy that prevents passwords from including words defined in that file. See <a href="#">Specifying a Password Dictionary</a> on page 126.	no dictionary used
<b>Tuning Parameters</b> setup screen	Displayed for Custom setup type only. Allows you to specify tuning parameters so you can configure how the Policy Validator performs at runtime. See <a href="#">Tuning your Policy Validator</a> on page 126.	auto-defined
<b>Finish</b> setup screen	Allows you to commit your configuration settings to the Policy Store and the Policy Validator's bootstrap XML file, and to automatically start the Policy Validator. See <a href="#">Completing the Policy Validator Setup Process</a> on page 128.	enable Policy Validator restart

## Connecting to the Administration Server

In order to configure a Policy Validator, the Setup wizard must be able to connect to the Administration server. The Administration server stores and manages the configuration data for all Policy Validators. The **Contact the Administration server** setup screen, shown in [Figure 3](#), allows you to provide the connection parameters.

- If you have installed the Policy Validator on the same computer as the Administration server, most of these fields are automatically populated with the correct information.
- This screen does *not* appear if you have previously configured the Administration server settings during your Setup Tool session, as the Setup tool already has the information needed to connect to it.



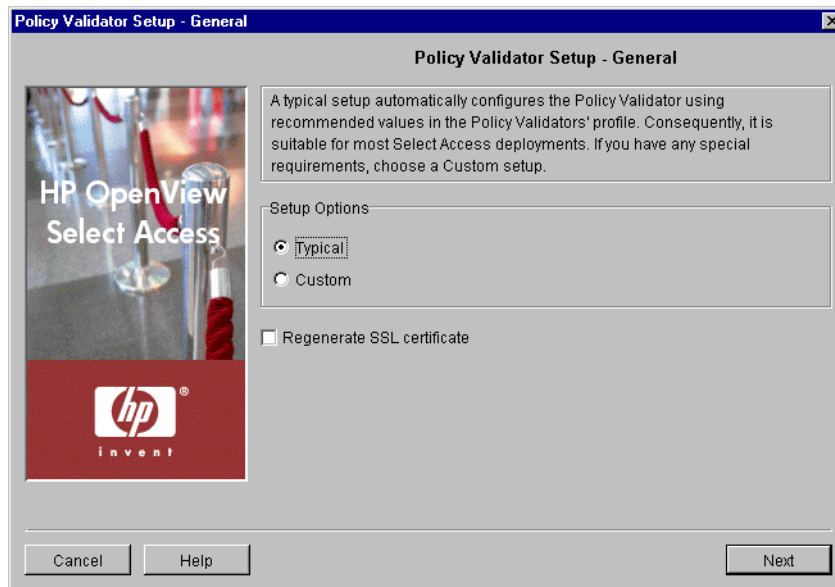
**Figure 3 Contact the Administration Server Setup Screen**

### To connect to the Administration server

- 1 Specify the connection parameters in the **Administration Server Connection Parameters** group.
  - **Host:** Required. Enter the name or IP address of the host computer on which you have installed the Administration Server.
  - **Port:** Required. Enter the port the administration server is running on. By default, the port is 9986.
  - **URL Path:** Required. Enter the path to the Select Access Administration login page. By default, the path is /admin.
  - **Login name:** Required. Enter the ID that logs into the Administration Server.
  - **Password:** Required. Enter the password to log into the Administration Server.
- 2 Click **Next**. The Setup Tool tries to connect to the Administration server. If the Setup Tool connects successfully, the **General** setup screen appears.

### Choosing Your Setup Type

The **General** setup screen, shown in [Figure 4](#), allows you to choose whether you want to perform a **Typical** or a **Custom** setup.



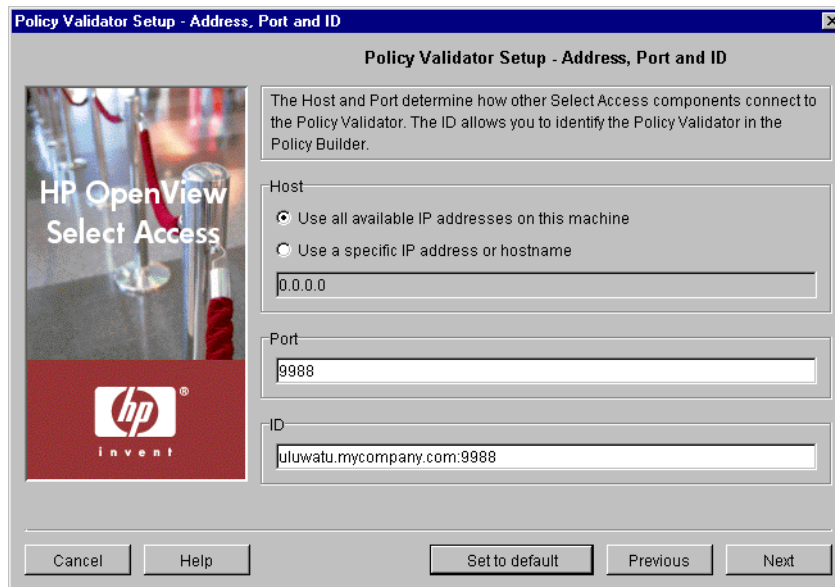
**Figure 4 General Setup Screen**

### To choose your setup type

- 1 Select one of the setup options:
  - **Typical:** By choosing this option, you are essentially setting up this component without needing to configure it. HP’s recommended values are appropriate for most environments.
  - **Custom:** By choosing this option, you can customize the Policy Validator’s setup.
    - A **Custom** setup increases the number of steps and increments the complexity of the Policy Validator’s setup. If you misconfigure any of the setup parameters documented in these steps, you can return to HP’s recommended values by clicking the **Set to Default** button on any of the ensuing screens.
- 2 If you are reconfiguring or reinstalling one or more components, a **Regenerate SSL certificate** option appears. If you regenerated your Administration server’s certificate, check this box to regenerate the SSL certificates used by the components on your network. This ensures that the Setup Tool synchronizes SSL certificates despite the change in your deployment.
- 3 Click **Next**. Depending on which setup type you chose, one of two screens will appear:
  - If you are performing a **Typical** setup, the **Finish** screen appears. See [Completing the Policy Validator Setup Process](#) on page 128.
  - If you are performing a **Custom** setup, the **Address, Port and ID** setup screen appears. See [Setting Connection Parameters for the Policy Validator](#) on page 122.

## Setting Connection Parameters for the Policy Validator

The **Address, Port and ID** setup screen, shown in [Figure 5](#), allows you to define connection information for the Policy Validator.



**Figure 5 Address, Port and ID Setup Screen**

### To set the Policy Validator connection parameters

- 1 Review HP's recommended values. To customize these values, modify any of the screen's fields as needed.



If you are reconfiguring your Policy Validator and you modify its IP address or port, you can adversely affect your Enforcer plugin's ability to communicate with other parts of the Select Access system. If you change either of these configuration parameters, ensure you refresh the Enforcer plugin's configuration by re-running the Setup Tool for each plugin.

- **Host:** Required. Choose which IP address the Policy Validator listens.  
Click **Use all available IP addresses on this machine** to make the Policy Validator available on all IP addresses configured for the host computer. HP recommends you use this option.  
Click **Use a specific IP address or hostname** to use a single address only and enter the details in the corresponding text box that follows this option.
  - **Port:** Optional. Enter the port for the Policy Validator. If you leave it blank, the Policy Validator uses the default port of 9988.
  - **ID:** Required. This allows you to create a unique Policy Validator ID. Select Access components use this unique ID to identify a Policy Validator in the Policy Builder when you modify its configuration, as well as to identify specific Policy Validators for the purposes of creating cookies for single sign-on (SSO). The ID is typically a combination of the host name and port; however, you can change the ID to be more meaningful if you choose—as long as it isn't shared by other Policy Validators. To change the ID, simply delete the existing ID and type a new one.
- 2 Click **Next**. The **Audit Settings** setup screen appears. See [Configuring Validator-Specific Audit Settings](#) on page 124.

## Configuring Validator-Specific Audit Settings

By default, all Select Access components use the audit settings you configured for the Administration server. The **Audit Settings** setup screen, shown in [Figure 6](#), allows you to create custom audit settings for a specific Policy Validator, thereby overriding the common settings.

- ▶ If you log events to the Secure Audit server, the Policy Validator becomes a client of it. Ensure that you have configured the Secure Audit server before continuing. For details, see [Chapter 6, Configuring the Secure Audit Server](#).



**Figure 6** Audit Settings Setup Screen

### To set Policy Validator-specific audit settings

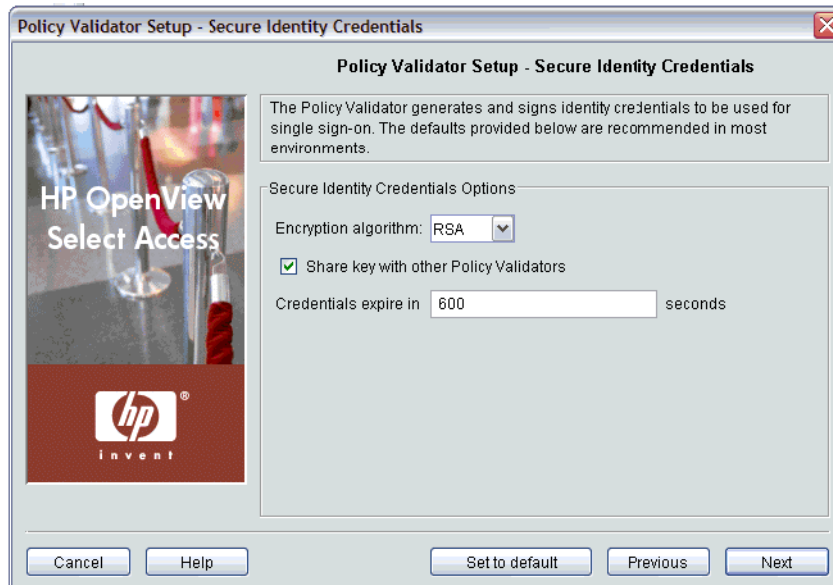
- 1 Review the audit settings that appear. To create custom audit settings for this specific Policy Validator only, change the settings as required.
  - ▶ You can create reports from logged runtime messages—preferably from a non-refutable administrative log that you have digitally signed and output in XML. You create a report with the **Report Viewer**, which is available from the **Audit** menu in the Policy Builder. For details, see [Chapter 14, Creating Reports from Secure Audit Server Output](#), in the *HP OpenView Select Access 6.1 Policy Builder Guide*.
  - a To create or modify audit settings rows, click **Add** or **Properties** respectively. The **New Audit Entry** dialog box appears displaying two tabs, **Audit Trail** and **Audit Policy**. These tabs correspond to the columns of the **Audit Settings** setup screen.

When you configure the tabs of the **New Audit Entry** dialog box, then click **OK**, the Setup Tool adds a new row below the one you have selected, and it populates the cells automatically. For details, see [Configuring an Audit Policy](#) on page 110.
  - b To remove an empty or populated row, select the entry in question and click **Delete**.
- 2 Click **Next**. The **Secure Identity Credentials** setup screen appears. See [Setting Connection Parameters for the Policy Validator](#) on page 122.



## Defining Data Encryption Settings

The **Secure Identity Credentials** setup screen, shown in [Figure 7](#), allows you to configure the digital signature settings the Policy Validator needs to generate cookies and nonces. The Policy Validator uses cookies to create identity credentials to reduce the number of times a person needs to reauthenticate before accessing a Select Access-protected resource. For more details on cookies and nonces, see [Chapter 6, Understanding Authentication](#) of the *HP OpenView Select Access 6.1 Concepts Guide*.



**Figure 7** Secure Identity Credentials Setup Screen

### To define the Policy Validator's data encryption settings

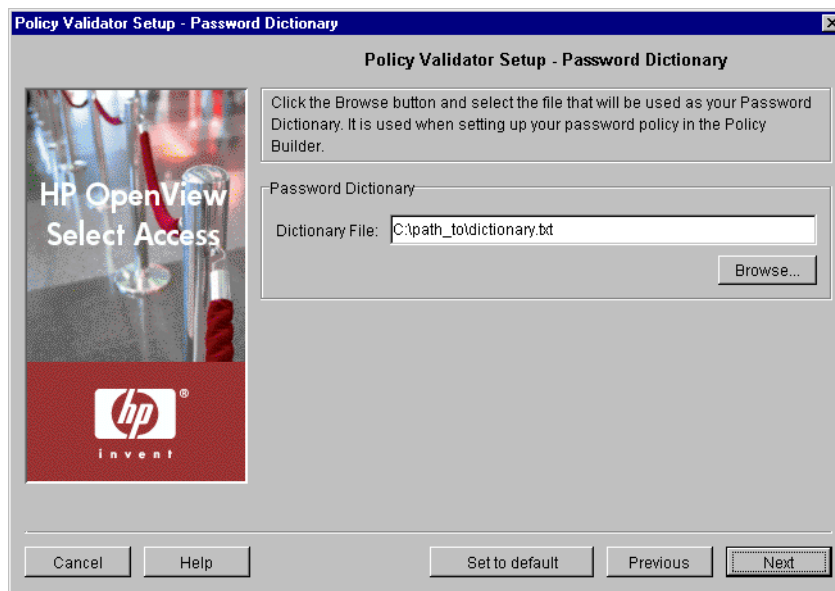
- 1 Review HP's recommended values. To customize these values, modify fields in the **Secure Identity Credential Options** group as needed.
  - **Encryption algorithm:** Required. Choose the algorithm you want to use to encrypt data streams to and from the Policy Validator. By default, RSA is default encryption algorithm for the Policy Validator because it is the more secure of the two. However, if performance is a concern, you can also choose Digest (MD5).
  - **Share key with other validators:** Optional. Controls whether the Policy Validator publishes the key to the directory server so other Policy Validators can share it. If you leave this box unchecked, the Policy Validator does not publish the keys.
    - ▶ Policy Validators need to publish keys if you intend to do either load-balancing or round-robinning. If you do not share your keys, identities must reauthenticate. This is because the keys required to validate cookies are not available to other Policy Validators, so they cannot check cookies for their authenticity.
  - **Credentials expire in:** Required. Determines how long, in seconds, an identity has to access the Web site after authenticating before being required to reauthenticate. Select Access uses cookies to track this interval. For a Web session that takes place over extended periods of time, Select Access renews the cookie when half or more of the interval has passed.

- 2 Click **Next**. The **Password Dictionary** setup screen appears. See [Specifying a Password Dictionary](#) on page 126.

## Specifying a Password Dictionary

The **Password Dictionary** setup screen, shown in [Table 8](#), allows you to specify the file that acts as your password dictionary. The password dictionary is a plain text file of words that identities cannot use within a password. Only one word can appear per line. You must configure a password dictionary before you configure a password policy to check a dictionary file with the Policy Builder.

- ▶ The Policy Validator performs case-insensitive dictionary checks.
- ▶ If you are using a localized dictionary, ensure you encode it in UTF-8.



**Figure 8 Password Dictionary Setup Screen**

### To select a password dictionary

- 1 Locate the path to the file that acts as your password dictionary. For specific details on the contents of your dictionary file, see [Setting Up and Maintaining Password Management](#) on page 185 in the *HP OpenView Select Access 6.1 Policy Builder Guide*.
- 2 Click **Next**. The **Tuning Parameters** setup screen appears. See [Tuning your Policy Validator](#) on page 126.

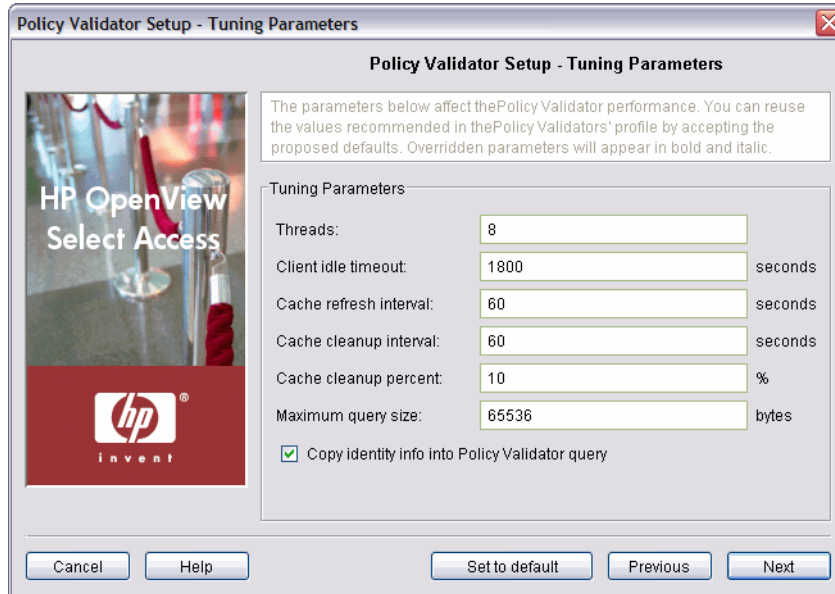
## Tuning your Policy Validator

The **Tuning Parameters** setup screen, shown in [Figure 9](#), allows you to adjust how the Policy Validator behaves at runtime. You can enhance the Policy Validator's performance depending on how you define the following settings.

Text on the **Tuning Parameters** setup screen appears in bold and italics if the Policy Validator you are currently configuring has any override values set for it. You create override values for a specific Policy Validator by configuring one for the specific Policy Validator in the Policy

Builder. If you are creating override settings, they take precedence over group values, even if an administrator changes group values with the Policy Builder. For details, see [Chapter 16, Modifying Components' Central Configuration Parameters](#) in the *HP OpenView Select Access 6.1 Policy Builder Guide*.

The remaining parameters are those that are shared by all Policy Validators.



**Figure 9 Tuning Parameters Setup Screen**

## To tune your Policy Validator

- Review HP's recommended values. To customize these values, modify fields in the **Tuning Parameters** group as needed.
  - Threads:** Optional. Specifies the number of Policy Validator threads that can execute independently.
  - Client idle timeout:** Optional. The length of time, in seconds, before Policy Validator closes an idle client connection.
    - By default, all Delegated Administration session timeouts are tied to the Policy Validator's **Client Idle Timeout** tuning parameter. The default value for this parameter is 10 minutes. If this value is too low, you may want to adjust it accordingly.
  - Cache refresh interval:** Optional. The interval, in seconds, that Policy Validator refreshes its cached identity or policy lookups. When it refreshes the cache, the Policy Validator updates the information it has saved to that point. The default is 60 seconds.
    - 🚩 Use the Policy Builder to clear the cache when you alter policy data or add new identity profiles. This ensures that the Policy Validator updates the identity/policy data. For details, see [Updating Policy Data Cached by the Policy Validator](#) on page 264 in the *HP OpenView Select Access 6.1 Policy Builder Guide*.
  - Cache cleanup interval:** Optional. The interval, in seconds, that Policy Validator clears unused identity profiles from its cache. The default is 60 seconds.

- **Cache cleanup percent:** Optional. The percentage of the cache that the Policy Validator checks for unused profiles.
- **Maximum query size:** Optional. The size limit of XML queries allowed.
- **Copy identity info into Validator query:** Optional. Makes the attribute and value pairs of an identity entry accessible to other Policy Validators when evaluating any LDAP attribute decision point. If you uncheck this box, the Enforcer plugin only adds `authenticated_dn` and `UID` attributes to the query.

➤ If you do not intend to use LDAP attribute decision points in any of your conditional access rules or for personalization, you can improve your site's performance by unchecking this box

- 2 Click **Next**. The **Finish** setup screen appears, informing you that you have completed all setup tasks for the Policy Validator. See [Completing the Policy Validator Setup Process](#) on page 128.

## Completing the Policy Validator Setup Process

The **Finish** setup screen informs you that you have completed all setup tasks and allows you to automatically restart the Policy Validator.

### To complete the Policy Validator setup

- 1 Check **Start now** if you want to start the Policy Validator immediately after the Setup Tool records your configuration parameters.

➤ Policy Validator does not automatically restart after a failure. Select Access Validator is a service that runs on each node of a cluster. In most cases, the Policy Validator restarts automatically. However, because it is not part of a cluster group, it does not automatically restart after a failure. If your Policy Validator fails, remember to restart it manually. For details on starting and stopping the Policy Validator, see [Starting and Stopping the Policy Validator](#) on page 205.

- 2 Click **Finish** to commit your configuration to both:

- The Policy Store you defined at the beginning of the Administration server's setup
- AND
- The bootstrap XML file (`validator.xml`)

➤ This bootstrap file contains startup and general configuration information for the Policy Validator. Modifying or moving this file could result in the Policy Validator being unable to start correctly. You should ensure that you protect this file using both logical and physical controls.

- 3 If you have installed any other components on this computer, the next component's setup screen appears. For details, see [To configure Select Access with the Setup Tool](#) on page 58.

Choose which IP address Policy Validator listens.—as long as it isn't shared by other Policy Validators

# 8 Configuring the Enforcer Plugins

The Enforcer plugin acts as an intermediary between the identity and the service on which it protects content. Because it relays messages to and from the Policy Validator on behalf of the service it protects, it is crucial that you set up this plugin correctly. This chapter describes this process.

## Chapter Overview

This chapter outlines how to configure the Enforcer plugin. Topics in this chapter include:

- [How the Enforcer Plugin Works](#) on page 129
- [Configuring the Enforcer Plugin](#) on page 129
- [Starting Your Enforcer Plugin](#) on page 156
- [Uninstalling the Enforcer plugins](#) on page 160

## How the Enforcer Plugin Works

All Enforcer plugins are responsible for:

- Examining the XML-based response from the Policy Validator
- Enforcing the authorization decision contained in the response
- Querying identities for additional authentication information (for example, secret, password, name, and so on) if required
- Tailoring responses to the application based on results from the Policy Validator.

## Configuring the Enforcer Plugin

The Enforcer plugin settings are initially configured via the Select Access Setup Tool. Because the Setup Tool is installed with the Select Access components, you can modify your settings at any time.



You can also modify certain parameters that the Administration server writes to the Policy Store via the **Tools**→**Configure Components** command in the Policy Builder. For details, see [Chapter 16, Modifying Components' Central Configuration Parameters](#), in the *HP OpenView Select Access 6.1 Policy Builder Guide*.



If you do not configure all your Policy Validators before configuring Enforcer plugins, the Enforcer plugin's bootstrap XML configuration file only includes the names of Policy Validators that were available at that time.

This can be problematic if you create a test or pilot deployment that initially includes only one Policy Validator, but add multiple new Policy Validators during a full Select Access deployment. Potentially, any test Enforcer plugins (as well as your delegated administration Enforcer plugin) will not be able to failover and/or round robin to the new Policy Validators if the test Policy Validator fails. If you must stagger your deployment, you should re-run the Setup Tool for your existing Enforcer plugin to ensure all new Policy Validators are written to its `enforcer.xml` file.

## The Enforcer Plugins' Main Setup Types

Before you begin, you need to understand the difference between the two general setup types you can choose.

- **Typical:** Use HP's recommended setup values. A **Typical** setup reduces the number of steps and minimizes the complexity of the Enforcer plugin's setup.
- **Custom:** Modify recommended values to meet the needs of your network and/or business environment. A **Custom** setup increases the number of steps and increments the complexity of the Enforcer plugin's setup.

Whether you choose one or the other depends on how much you want to customize the configuration of the Enforcer plugin. You can use recommended values that are automatically configured by a **Typical** setup. To allow you to more easily identify what type of setup you need to perform, [Table 2](#) on page 133 summarizes the Enforcer plugin's setup tasks from a high level.

## A Note About Enforcer-Specific Setup Wizards

HP provides a number of Enforcer plugins with the Select Access software. Each installed Enforcer plugin must have a corresponding `enforcer_<type>.xml` bootstrap file in order to communicate with the Policy Validator, identify filenames and domains which do not require Select Access protection, and so on. Select Access provides setup wizards to create this file.

Because each Enforcer plugin protects a different resource, the configuration parameters required may differ slightly. For this reason, where possible, HP has provided enforcer-specific setup wizards.



Each Enforcer plugin must have its own bootstrap file. If you are configuring more than one Enforcer plugin with the generic setup wizard, you must run the setup wizard once for each plugin so that you can set unique bootstrap filenames and Enforcer IDs for each plugin.

However, there are several enforcers available for installation with Select Access that do not have their own setup wizards. For these, and for any custom Enforcer plugins developed using the Enforcer API, you can use the Generic Enforcer plugin setup wizard to create a bootstrap file.

Table 1 lists the Enforcer plugins that can be configured using the Select Access Setup Tool, either with an enforcer-specific setup wizard, or via the Generic Enforcer plugin setup wizard.

**Table 1 Configurable Enforcers**

Enforcer Type	Description
<b>Enforcers that have an enforcer-specific setup wizard:</b>	
Sun/Netscape/iPlanet Enforcer plugin	Secures any of the Sun, Netscape or iPlanet Web servers. Available for Windows or for Unix.
Apache 2 Enforcer plugin	Available on Unix only. Secures any version of the Apache Web server.
IIS Enforcer plugin	Secures the IIS Web server.
WSE Enforcer plugin	Secures .NET web services. <i>Note:</i> If you want this plugin to support Integrated Windows Authentication (IWA), you need to install and configure both the WSE and IIS Enforcer plugins. For more details, see <a href="#">To use IIS's automatic logon mechanism: Integrated Windows Authentication in the HP OpenView Select Access 6.1 Network Integration Guide</a>
Axis Enforcer plugin	Secures Java web services.
<b>Enforcers that require you to run the Generic setup</b>	
TCP Enforcer plugin.	Available on Unix only. Secures services configured in Inetd.
Domino Enforcer plugin.	Secures the Domino Web server.
Oracle Enforcer plugin.	Secures the Oracle Application Server.
servlet Enforcer plugin	Secures any servlet engine.
Any custom plugins created using the Enforcer API.	

## Using the Setup Tool to Configure the Enforcer Plugin

If you choose to configure your Select Access components directly from the installer, the Setup Tool will be started for you automatically.

If you choose to configure your Select Access components at a later time, or want to modify your configuration settings, you can run the Setup Tool and access the Enforcer plugins' configuration settings at any time.

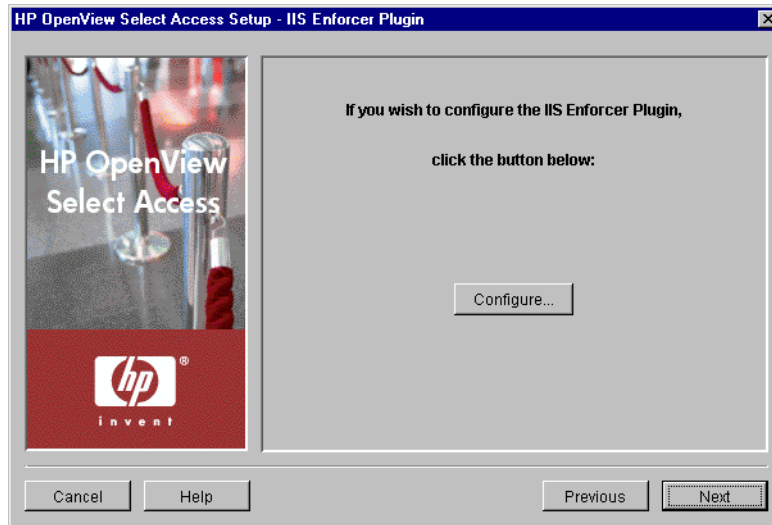


If you modify the Policy Validator's IP address or port, you can adversely affect the Enforcer plugin's ability to communicate with other parts of the Select Access system. If you change either of these configuration parameters, ensure that you refresh the Enforcer plugin's configuration by re-running the Setup Tool for each plugin.

- ▶ You can also modify centrally located parameters that are committed to the Policy Store via the **Tools→Configure Components** command in the Policy Builder. For details, see [Chapter 16, Modifying Components' Central Configuration Parameters](#), in the *HP OpenView Select Access 6.1 Policy Builder Guide*.
- ▶ If you modify the Administration server's or the Policy Validator's parameters that affect the configuration of the Policy Store at any time, reconfigure your Enforcer plugins as well. This ensures that the corresponding configuration changes are propagated to them.

## To configure your Enforcer plugin

- 1 If the Setup Tool is not already started, click **Start→Programs→HP OpenView→Select Access→Setup Tool**. The **Component Setup Tool** window appears.
- 2 Click **Next** until you reach the Setup Tool's setup screen for your corresponding Enforcer plugin.




**Figure 1 Enforcer plugin Setup Screen**

- 3 If you are configuring the Generic Enforcer plugin setup wizard, enter the path and filename in which the bootstrap file will be stored.
  - ▶ Each Enforcer plugin must have its own bootstrap file. If you are configuring more than one Enforcer plugin with the generic setup wizard, you must run the setup wizard once for each plugin so that you can set unique bootstrap filenames and IDs for each.
- 4 Click the **Configure** button. The Enforcer plugin setup process starts and the **Contact the Administration server** setup screen appears, shown in [Figure 2](#).
  - ▶ This screen does *not* appear if you have previously connected to the Administration server during your Setup Tool session, as the Setup tool already has the information needed to connect to it. In this case, the **General** setup screen will appear instead.



- 5 Complete the setup screens of the Enforcer plugin setup process, listed in [Table 2](#), as necessary.

 Depending on which Enforcer plugin you are configuring, the setup screens you need to complete in order to configure your plugin will vary. Each task described in [Table 2](#) identifies the plugins to which the task applies.

**Table 2 Overview of Enforcer Plugin Setup Screens**

Setup screen	Description	Default value(s)
<b>Contact the Administration Server</b> setup screen	Allows the Setup Tool to connect to the Administration server, so it can manage the Enforcer plugin's configuration parameters and request the common and/or group configuration parameters for it. See <a href="#">Connecting to the Administration Server</a> on page 135.	auto-defined
<b>General</b> setup screen	Allows you to choose one of two setup types: <ul style="list-style-type: none"> <li>• <b>Typical:</b> Use HP's recommended setup values.</li> <li>• <b>Custom:</b> Modify the recommended values to meet the needs of your network and/or business environment.</li> </ul> See <a href="#">Choosing Your Setup Type</a> on page 136.	Typical
<b>ID</b> setup screen	Displayed for a Custom setup of <a href="#">all Enforcer plugin types</a> . Allows you to define an enforcer ID which is used to identify the Enforcer plugin. See <a href="#">Defining an Enforcer Plugin ID</a> on page 138.	auto-defined
<b>Single DNS domain SSO</b> setup screen	Displayed for a Custom setup of <a href="#">all Enforcer plugin types excluding the Axis and WSE plugins</a> . Allows you to identify the domain name across which identities authenticate only once—even though they access resources on multiple subdomains. See <a href="#">Setting up Single Domain Single Sign-on</a> on page 139.	not enabled
<b>Multiple DNS domain SSO</b> setup screen	Displayed for a Custom setup of <a href="#">all Enforcer plugin types excluding the Axis and WSE plugins</a> . Allows you to set up SSO across multiple domains (multidomain SSO) by creating a protected domains list that identifies the domains identities can access without being required to reauthenticate with each new server. See <a href="#">Setting up Multiple Domain Single Sign-on</a> on page 140.	not enabled

**Table 2 Overview of Enforcer Plugin Setup Screens**

Setup screen	Description	Default value(s)
<b>Sign SOAP XML</b> setup screen	Displayed for a Custom setup of <a href="#">the WSE Enforcer plugin</a> . Allows you define whether incoming and outgoing SOAP messages should be signed. Signed SOAP messages identify the Web Server from which they came, thereby increasing the trust level. See <a href="#">Setting up SOAP Message Signing</a> on page 141.	not enabled
<b>Encrypt SOAP XML</b> setup screen	Displayed for a Custom setup of <a href="#">the WSE Enforcer plugin</a> . Allows you to define whether outgoing SOAP messages should be encrypted. Encrypted SOAP messages are much more difficult to decipher, and therefore more difficult to tamper with. See <a href="#">Setting up SOAP Message Encrypting</a> on page 142.	not enabled
<b>Ignored Filenames</b> setup screen	Displayed for a Custom setup of <a href="#">all Enforcer plugin types excluding the WSE Enforcer plugin</a> . Allows you to create a list of files to which access does not need to be secured. See <a href="#">Setting up a List of Ignored Filenames</a> on page 143.	not enabled
<b>Pass-through Domains</b> setup screen	Displayed for a Custom setup of <a href="#">all Enforcer plugin types</a> . Allows you to create a list of domains to which access does not need to be secured. See <a href="#">Setting up a list of pass-through domains</a> on page 145.	not enabled
<b>Audit Settings</b> setup screen	Displayed for a Custom setup of <a href="#">all Enforcer plugins</a> . Allows you to configure audit settings specific to the Enforcer plugin. See <a href="#">Configuring Enforcer-Specific Audit Settings</a> on page 146.	inherit common settings defined by the Administration server
<b>Validators</b> setup screen	Displayed for a Custom setup of <a href="#">all Enforcer plugins</a> . Allows you to select which Policy Validators the Enforcer plugin uses to authenticate identities and authorize resource requests. You can also establish whether to use round-robinning to share loads among the Policy Validators you define. See <a href="#">Configuring Policy Validator Settings</a> on page 148.	auto-defined to use all runtime-available Policy Validators listed in the Policy Store. Load balancing is enabled.

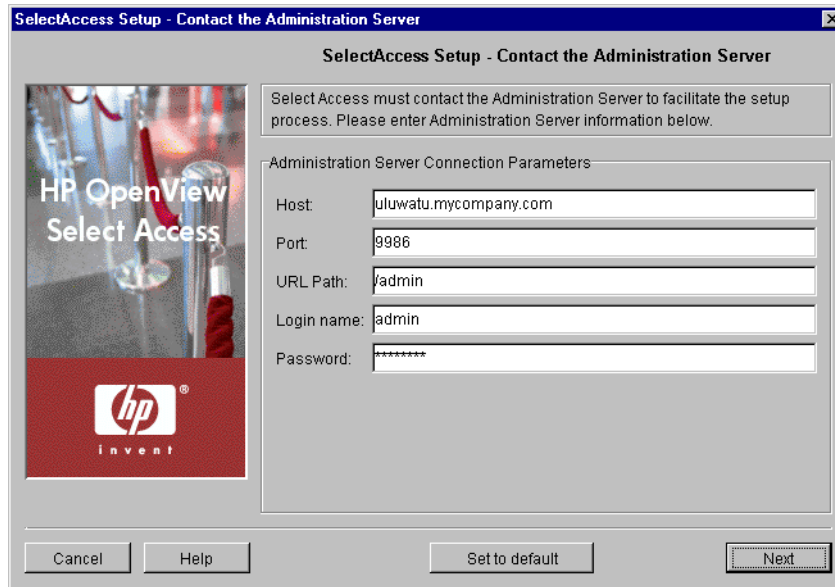
**Table 2 Overview of Enforcer Plugin Setup Screens**

Setup screen	Description	Default value(s)
NAT setup screen	Displayed for a Custom setup of <a href="#">all Enforcer plugins</a> . Allows you to configure the Enforcer so that it can communicate with the Policy Validator even when there is a firewall and/or NAT device on your network between these components. See <a href="#">Mapping Policy Validators to NAT Addresses</a> on page 149.	not enabled
Tuning Parameters setup screen	Displayed for a Custom setup of <a href="#">all Enforcer plugins</a> . Allows you to specify tuning parameters so you can configure how the Enforcer plugin performs at runtime. See <a href="#">Tuning your Enforcer plugin</a> on page 150.	auto-defined
<b>Finish/Update Configuration</b> setup screen (for the WSE Enforcer plugin)	Allows you to commit your configuration settings to the Policy Store and the Enforcer plugin's bootstrap XML file, and to specify whether the Setup wizard changes the server's configuration field to automatically load the Enforcer plugin on startup. See <a href="#">Completing the Enforcer Plugin Setup Process</a> on page 154.	enable Enforcer plugin restart

## Connecting to the Administration Server

In order to configure an Enforcer plugin, the Setup wizard must be able to contact the Administration server. The Administration server stores and manages the configuration data for all Enforcer plugins. The **Contact the Administration Server** setup screen, shown in [Figure 2](#), allows you to provide the connection parameters.

- If you have installed the Enforcer plugin on the same computer as the Administration server, most of these fields are already populated with the correct information.
- This screen does *not* appear if you have previously configured the Administration server settings during your Setup Tool session, since the Setup tool already has the information needed to connect to it.



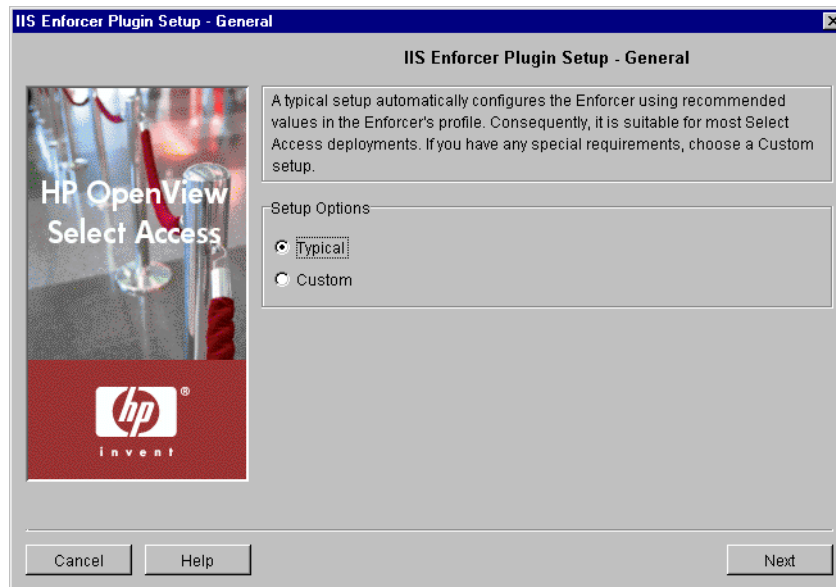
**Figure 2 Contact the Administration Server Setup Screen**

### To connect to the Administration server

- 1 Specify the connection parameters in the **Administration Server Connection Parameters** group.
  - **Host:** Required. Enter the name or IP address of the host computer on which you have installed the Administration Server.
  - **Port:** Required. Enter the port the administration server is running on. By default, the port is 9986.
  - **URL Path:** Required. Enter the path to the Select Access Administration login page. By default, the path is /admin.
  - **Login name:** Required. Enter the Select Access root administrator's login name.
  - **Password:** Required. Enter the password to log into the Administration Server.
- 2 Click **Next**. The Setup Tool tries to connect to the Administration server. If the Setup Tool connects successfully, the **General** setup screen appears.

### Choosing Your Setup Type

The **General** setup screen, shown in [Figure 3](#), allows you to choose whether you want to perform a **Typical** or a **Custom** setup.



**Figure 3 General Setup Screen**

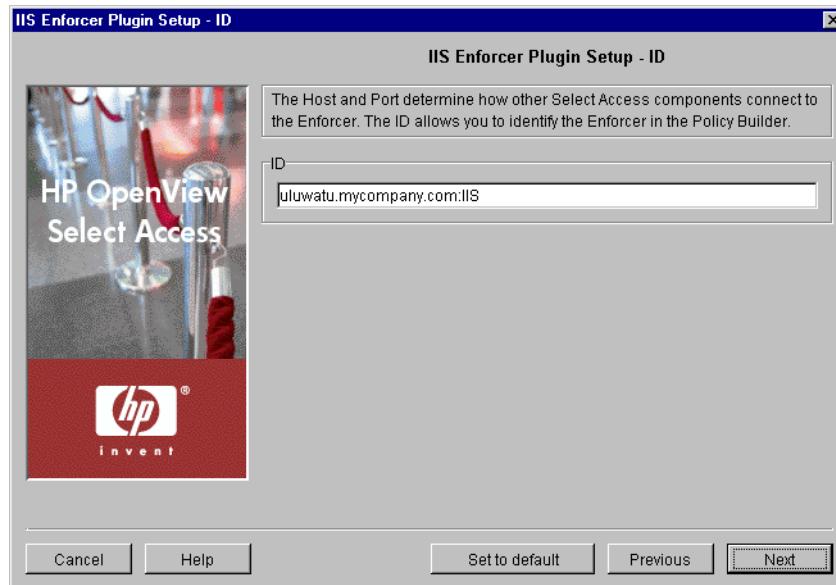
### To choose your setup type

- 1 Select one of the setup options:
  - **Typical:** By choosing this option, you are essentially setting up this component without needing to configure it. HP's recommended values are appropriate for most environments.
  - **Custom:** By choosing this option, you can customize the Enforcer plugin's setup.
    - ▶ A **Custom** setup increases the number of steps and increments the complexity of the Enforcer plugin's setup. If you misconfigure any of the setup parameters documented in these steps, you can return to HP's recommended values by clicking the **Set to Default** button on any of the ensuing screens.
  
- 2 If you are reconfiguring or reinstalling this component after reconfiguring the Administration server, a **Regenerate SSL certificate** option appears. If you regenerated your Administration server's certificate, check this box to regenerate the SSL certificates used by the components on your network. This ensures that the Setup Tool synchronizes SSL certificates despite the change in your deployment.
 

For information on how to avoid regeneration when you need to reinstall a component, see [Authenticating Identities with Certificates](#) on page 47, in the *HP OpenView Select Access 6.1 Concepts Guide*.
  
- 3 Click **Next**. Depending on which setup type you chose, one of two screens will appear:
  - If you are performing a **Typical** setup, the **Finish/Update Configuration** screen appears. See [Completing the Enforcer Plugin Setup Process](#) on page 154.
  - If you are performing a **Custom** setup, the **ID** setup screen appears. See [Defining an Enforcer Plugin ID](#) on page 138.

## Defining an Enforcer Plugin ID

The ID setup screen, shown in [Figure 4](#), allows you to define an Enforcer plugin ID. You can use the ID to identify an Enforcer plugin in the Policy Builder when you modify its configuration. Conversely, Select Access components use the ID to identify specific Enforcer plugins for the purposes of creating cookies for single sign-on (SSO). The ID is typically a combination of the host name and Web server type; however, you can change the ID to be more meaningful if you choose.



**Figure 4 ID Setup Screen**

### To define an Enforcer plugin ID

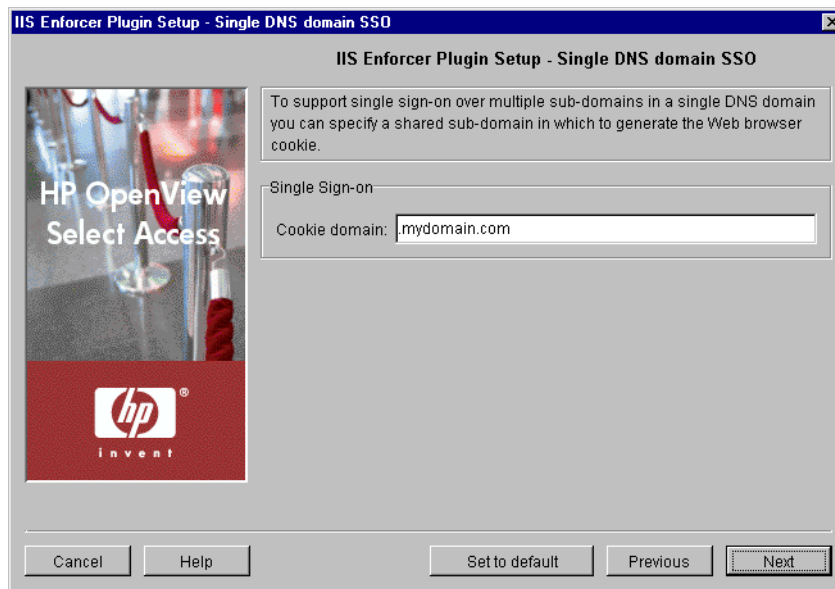
- 1 In the ID group, specify the ID which will be used to identify the Enforcer plugin.
  - ▶ If you are re-running the Setup Tool and are changing the Enforcer plugin's ID, ensure you regenerate the SSL certificates for it. Because the ID is embedded in the certificate, SSL connections between the Enforcer plugin and the Policy Validator cannot be made unless the name in the certificate matches the ID of the registered Enforcer plugin.
- 2 Click **Next**. Depending on which Enforcer plugin you are configuring, one of three screens will appear:
  - If you are configuring the Sun/Netscape/iPlanet Enforcer plugin, Apache 2 Enforcer plugin, IIS Enforcer plugin, or Generic Enforcer plugin, the **Single DNS Domain SSO** setup screen appears. See [Setting up Single Domain Single Sign-on](#) on page 139.
  - If you are configuring the WSE Enforcer plugin, the **Sign SOAP XML** setup screen appears. See [Setting up SOAP Message Signing](#) on page 141.
  - If you are configuring the Axis Enforcer plugin, the **Ignored Filenames** setup screen appears. See [Setting up a List of Ignored Filenames](#) on page 143.

## Setting up Single Domain Single Sign-on

The **Single DNS Domain SSO** setup screen, shown in [Figure 5](#), allows you to set a cookie domain. Once set, your identities only need to be authenticated once to gain access to all subdomains of a single DNS domain.

- ▶ This screen only appears if you are configuring one of the following Enforcers: Sun/Netscape/iPlanet Enforcer plugin, Apache 2 Enforcer plugin, IIS Enforcer plugin, or Generic Enforcer plugin.

For example, if you enter `.mycompany.com` and an identity visits `extranet.mycompany.com` or `www.mycompany.com`, the Enforcer plugin authenticates the identity at the first domain the identity visits only. It then accepts the authenticated cookie on all other domains. That way, the identity does not need to reauthenticate with each new Web server when trying to access content on an enforcer-protected subdomain.



**Figure 5** Single DNS Domain SSO Setup Screen

### To set up single domain single sign-on

- 1 If you want your identities to only authenticate once on all subdomains of a single DNS domain, type a domain in the **Cookie Domain** field. The cookie domain must use the following syntax:

`.mydomain.com`

- ▶ The cookie domain you enter is a single DNS domain; all subdomains share the same cookie that the Policy Validator generates.
- ▶ Internet Explorer browsers have a problem with uppercase characters. Ensure you always enter your **Cookie Domain** in lowercase letters.

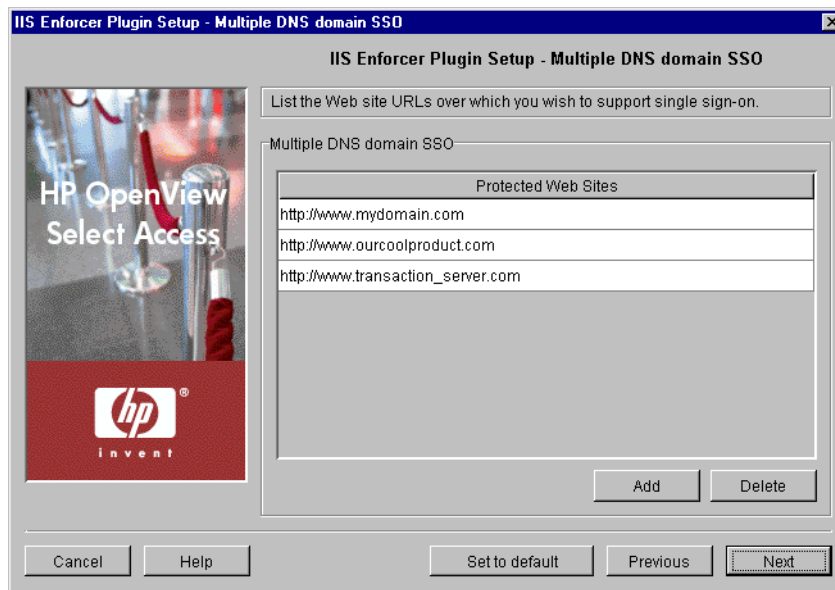
For details on how cookies are used with SSO, see [Chapter 6, Understanding Authentication](#) of the *HP OpenView Select Access 6.1 Concepts Guide*.

- 2 Click **Next**. The **Multiple DNS Domain SSO** setup screen appears. See [Setting up Multiple Domain Single Sign-on](#) on page 140.

## Setting up Multiple Domain Single Sign-on

The **Multiple DNS Domain SSO** setup screen, shown in [Figure 6](#), allows you to set up single sign-on with multiple enforcer-protected Web servers across multiple domains in your organization.

- This screen only appears if you are configuring one of the following enforcers: Sun/Netscape/iPlanet Enforcer plugin, Apache 2 Enforcer plugin, IIS Enforcer plugin, or Generic Enforcer plugin.



**Figure 6 Multiple DNS Domain SSO Setup Screen**

### To set up multidomain single sign-on

- 1 Click **Add** and enter a domain that needs to be part of the **Protected Web Sites** list. Repeat this step as needed to create a complete list.

For example, assume you divide your network into multiple domains to service different functions of your organization. You might have one domain for your corporate information, one for your products, and one for your e-commerce transaction server. Therefore, to ensure all enforcers have all of these domains, create a mutually inclusive protected Web domains list that you share with all Enforcer plugins. In this case, click **Add** and create a list that includes the following domains:

```
http://www.mydomain.com
http://www.ourcoolproduct.com
http://www.mytransaction_server.com
```

- ⚠ All Enforcer plugin-protected Web sites must share exactly the same list. Otherwise, multidomain SSO fails.



- ⚠ Multidomain SSO support only works when an identity is accessing content across Enforcer plugin-protected Web servers concurrently. If an identity tries accessing an Enforcer plugin-protected site from an intermediate unprotected one, the Select Access's multidomain SSO support is not triggered.
- If a Web domain ceases to exist, select the corresponding row in this list and click **Delete** to remove the site from the protected list and replicate this change to all Enforcer plugins.

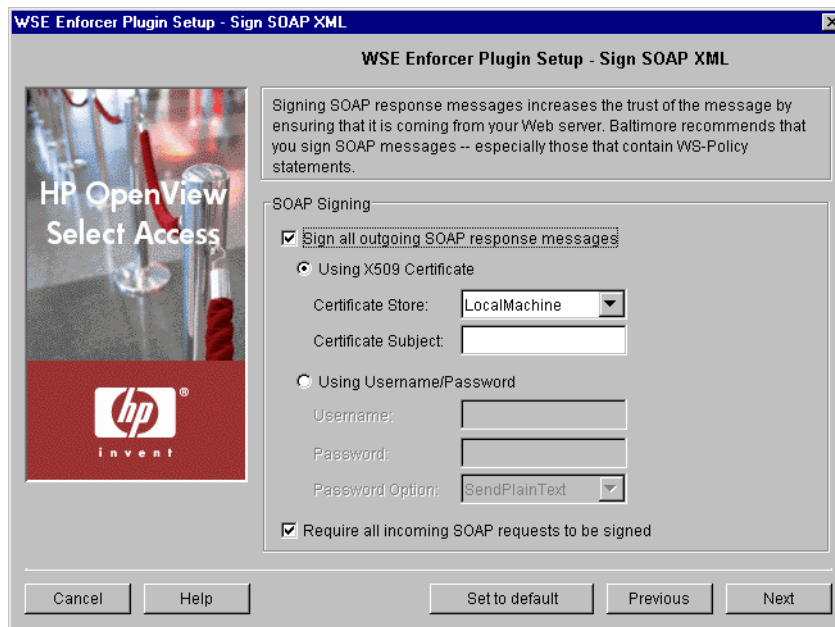
For additional details on setting up multi-domain SSO, see [Configuring SSO on Multiple Internet Domains](#) on page 34 of the *HP OpenView Select Access 6.1 Concepts Guide*.

- 2 Click **Next**. The **Ignored Filenames** setup screen appears. See [Setting up a List of Ignored Filenames](#) on page 143.

## Setting up SOAP Message Signing

The **Sign SOAP XML** setup screen, shown in [Figure 7](#), allows you to specify whether or not outgoing and incoming soap messages should be signed.

- This screen only appears if you are configuring the WSE Enforcer plugin.



**Figure 7 Sign Soap XML Setup Screen**

### To set up SOAP message signing

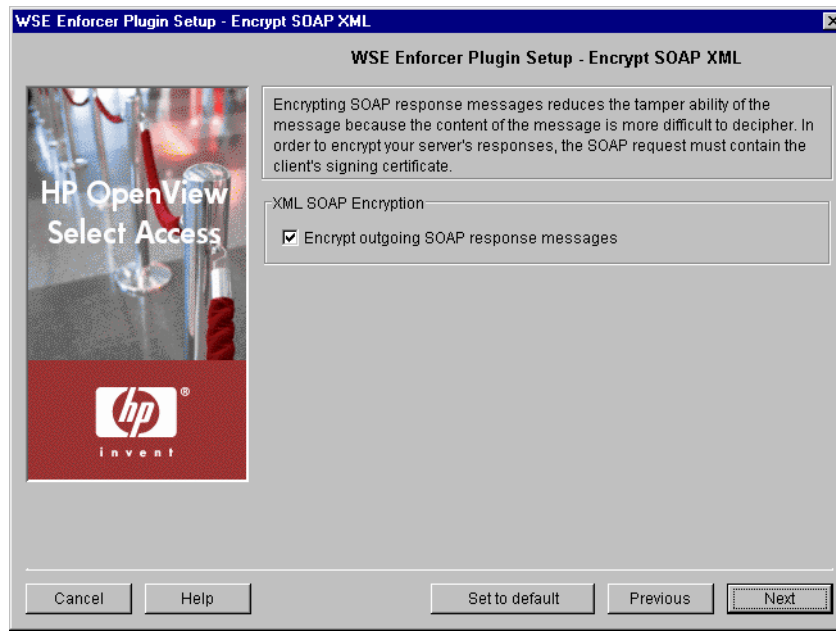
- 1 If you want outgoing messages to be signed, check **Sign all outgoing SOAP response messages**.
- 2 If you want to sign the response with an X509 certificate, check **Using X509 Certificate**, then complete the following options:

- **Certificate Store:** Required. Choose the certificate store in which WSE Enforcer plugin looks for X.509 certificates when it attempts to retrieve or verify a certificate. You can select either **LocalMachine** or **CurrentUser**.
  - **Certificate Subject:** Required. Enter the substring of the subject of the certificate which can be used to uniquely identify the certificate.
- 3 If you want to sign the response with a username and password combination, check **Using Username/Password**. The username and password you provide can be extracted from the SOAP message by the web service client. If you check this option, you must specify the following options:
- **Username:** Required. Specify the username that will be included in the SOAP message.
  - **Password:** Required. Specify the password that will be included in the SOAP message.
  - **Password Option:** Required. Allows you to specify in what form the password will be sent with the SOAP message. You can choose between sending it as plain text, sending it as hashed text, or not sending it at all.
    - ▶ If you do not choose to send the password as plain text, it is expected that password is available to the receiver of the SOAP response, and that it can use it to verify the username.
- 4 To maximize the level of trust for all requests, click **Require all incoming messages to be signed**. This ensures that all requests are signed, and that any unsigned requests are rejected before being passed on to the Policy Validator.
- ▶ If you intend to encrypt all outgoing response messages, you must check this option. In order to encrypt a response, the incoming SOAP request must contain the client's signing certificate. Therefore, only responses to signed messages may be encrypted.
- 5 Click **Next**. The **Encrypt Soap XML** setup screen appears. See [Setting up SOAP Message Encrypting](#) on page 142.

## Setting up SOAP Message Encrypting

The **Encrypt SOAP XML** setup screen, shown in [Figure 8](#), allows you to encrypt outgoing SOAP responses using the certificate included in a signed request. Encrypting response messages makes them more difficult to decipher, and therefore more difficult to tamper with.

- ▶ This screen only appears if you are configuring the WSE Enforcer plugin.




**Figure 8 Encrypt Soap XML Setup Screen**


## To set up SOAP message encrypting

- 1 Check **Encrypt outgoing SOAP response messages** if you want the responses to signed messages to be encrypted.

When this option is checked, the WSE Enforcer plugin will attempt to encrypt the message using the certificate that was used to sign the incoming SOAP request. The private key is not required to encrypt the message, but is needed to decrypt it.

 In order to encrypt a response, the incoming SOAP request must contain the client's signing certificate. Therefore, only responses to signed messages may be encrypted. If you want all response messages to be encrypted, you must check **Require all incoming messages** to be signed on the **Sign SOAP XML** setup screen.

If the incoming request is not signed, the response is sent unencrypted.

 The WSE Enforcer plugin can only encrypt messages using an X509 certificate key. If the incoming request is signed using a UsernameToken or some other token, the message is sent unencrypted

- 2 Click **Next**. The **Pass-through Domains** setup screen appears. See [Setting up a list of pass-through domains](#) on page 145.

## Setting up a List of Ignored Filenames

The **Ignored Filenames** setup screen, shown in [Figure 9](#), allows you to list security-insensitive files or file types that do not always require policy checking (for example, graphics on an HTML page) by the Enforcer plugin. Consequently, the Enforcer plugin bypasses the Policy Validator authorization step and automatically gives the identity access to the resource. This direct response to the identity's access request:

- Reduces the number of network-based transactions.
- Frees the Policy Validator to react to queries of a more security-sensitive nature.



This screen only appears if you are configuring one of the following Enforcers: Sun/Netscape/iPlanet Enforcer plugin, Apache 2 Enforcer plugin, IIS Enforcer plugin, or Generic Enforcer plugin.



If you are configuring the IIS Enforcer plugin and are also installing the WSE Enforcer plugin to protect web services, the IIS Enforcer plugin must be configured to ignore HTTP SOAP requests, or it will incorrectly attempt to validate the request using the information in the HTTP headers.

To allow SOAP requests to bypass IIS Enforcer plugin security, add the web services' relative URLs to the **Ignored Filenames** list for your IIS Enforcer plugin.

For example, if the URL to your web service is `https://localhost/web/service/web/service.asmx`, you could add any of the following to the list of Ignored filenames:

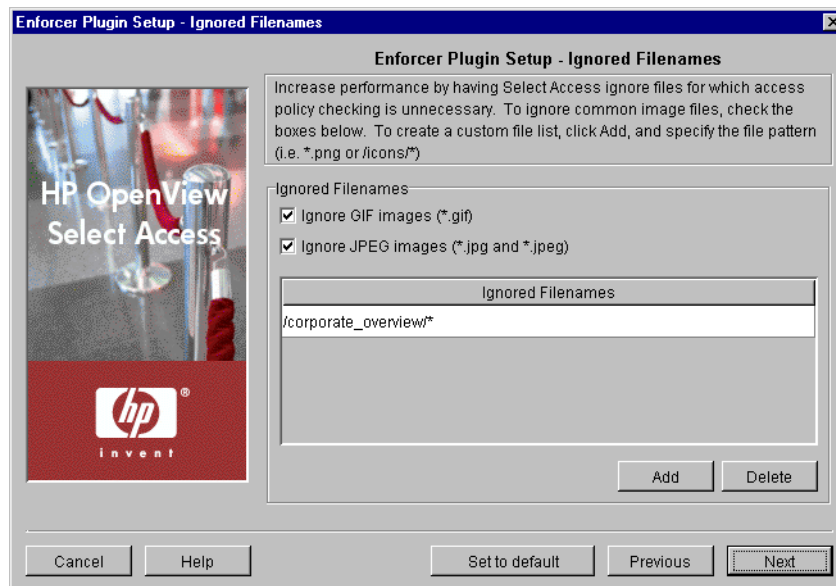
```
/web/service/web/service.asmx
/web/service/*.asmx
*.asmx
```



If you are configuring the servlet Enforcer plugin and are also installing the Axis Enforcer plugin to protect web services, the servlet Enforcer plugin must be configured to ignore Axis requests, or it will incorrectly attempt to validate the request using the information in the HTTP headers.

To allow Axis requests to bypass servlet Enforcer plugin security, add the following URL to the **Ignored Filenames** list:

```
/Axis/*
```



**Figure 9 Ignored Filenames Setup Screen**

## To create a list of ignored filenames

- 1 To ignore common graphic file types, click one of the following boxes to perform pattern matching with the following suffixes only:

- **Ignore GIF images**
- **Ignore JPEG images**

By checking these boxes, the Enforcer plugin does not perform a policy check for any files of these graphic types.

- 2 To create a custom ignored filename list, click **Add** and supply a list of filenames. Repeat this step as needed to create a complete list. Each row you add can only contain one filename or file type definition.

You can define entries that use the following types of pattern matching:

- Match by suffix (for example, \*.jpeg or \*.jpg).
- Match by prefix (for example, /images/\*).
- Match by prefix and suffix (for example, /apps/\*.gif)
- Use exact matching (for example, /welcome.txt)

➤ The ignored file list performs case-insensitive matching, and only supports wildcard (\*) expressions. You can only have one wildcard per expression.

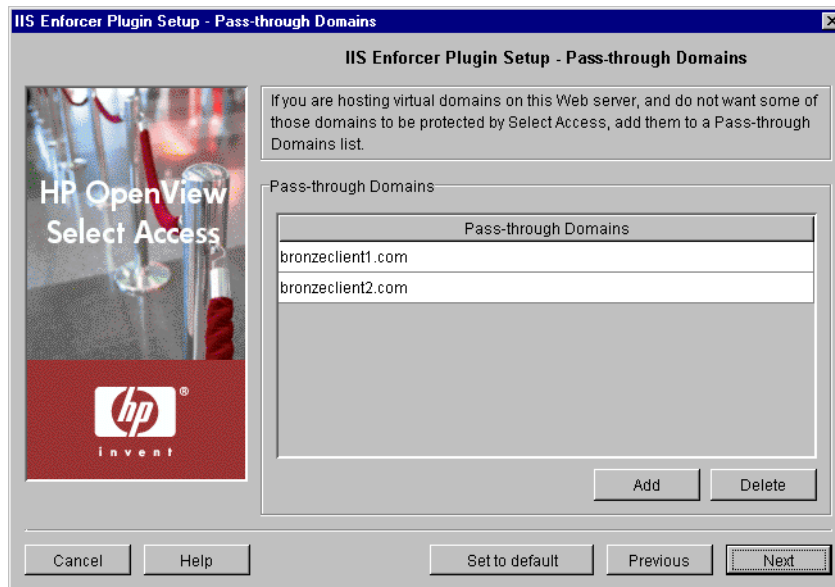
- 3 If you are configuring the IIS Enforcer plugin and are also using the WSE Enforcer plugin to protect web services, click **Add** and supply the relative URLs for each of the web services you want to protect.
- 4 To delete a row in the ignored filenames list, select the offending entry and click **Delete**.
- 5 Click **Next**. The **Pass-through Domains** setup screen appears. See [Setting up a list of pass-through domains](#) on page 145.

## Setting up a list of pass-through domains

The **Pass-through Domains** setup screen, shown in [Figure 10](#), enables you to define a list of virtual Web sites that the Enforcer plugin “passes through” without validating them with the Policy Validator.

- This screen only appears if you are configuring one of the following Enforcers: Sun/Netscape/iPlanet Enforcer plugin, Apache 2 Enforcer plugin, IIS Enforcer plugin, or Generic Enforcer plugin.
- In addition to using IP addresses or host domain names, you can also use host header-based virtual host names on Apache, IIS, and Netscape/iPlanet/Sun ONE servers.

For additional details on virtual Web hosting, see [Securing Virtual Domains](#) on page 55 in the *HP OpenView Select Access 6.1 Network Integration Guide*.



**Figure 10 Pass-through Domains Setup Screen**

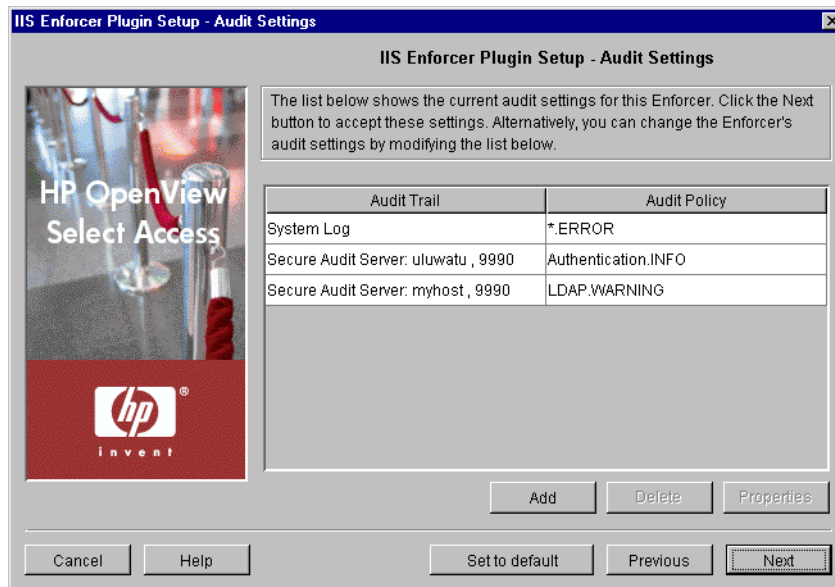
### To set up a list of pass-through domains

- 1 Click **Add** and enter a domain that needs to be part of the **Pass-through Domains** list. Repeat this step as needed to create a complete list.
- 2 Click **Next**. The **Audit Settings** setup screen appears. See [Configuring Enforcer-Specific Audit Settings](#) on page 146.

## Configuring Enforcer-Specific Audit Settings

By default, all Select Access components use the audit settings you configured for the Administration server. The **Audit Settings** setup screen, shown in [Figure 11](#), allows you to create custom audit settings for a specific Enforcer plugin.

- ▶ If you log events to the Secure Audit server, the Enforcer plugin becomes a client of it. Ensure that you have configured the Secure Audit server before continuing. For details, see [Chapter 6, Configuring the Secure Audit Server](#).
- ▶ On Windows platforms, when starting a Web server with an Enforcer plugin logging DEBUG messages to a Secure Audit server that is offline, you may see the following message: “The service did not respond to the start or control request in a timely fashion.” Do not be alarmed by this message; the Web server does eventually start after a delay.
- ⚠ When an Enforcer plugin cannot log to a Secure Audit server because it is offline, the plugin logs two messages to the Windows Event Log. If this occurs, ensure you modify the Enforcer plugin’s audit settings to not log to the Secure Audit server. Otherwise, your Web server’s performance is degraded as a result of this connection delay.



**Figure 11 Audit Settings Setup Screen**

### To set enforcer-specific audit settings

- 1 Review the audit settings that appear. To create custom audit settings for this specific Enforcer plugin only, change the settings as required.
- 2 To create or modify audit settings rows, click **Add** or **Properties** respectively. The **New Audit Entry** dialog box appears displaying two tabs, **Audit Trail** and **Audit Policy**. These tabs correspond to the columns of the **Default Audit Settings** setup screen.

When you configure the tabs of the **New Audit Entry** dialog box, then click **OK**, the Setup Tool adds a new row below the one you have selected and the cells are populated automatically. For details, see [Configuring an Audit Policy](#) on page 110.

- 3 To remove an empty or populated row, select the entry in question and click **Delete**.
  - Ensure you have write permissions for the file that you have configured your Enforcer plugin to log events to. Otherwise, logging does not occur. Starting your Web server as root on Unix systems or administrator on Windows systems does not guarantee that the Web server process has write permissions across the system.
  - You can create reports from the runtime messages that the Enforcer plugin has logged—preferably from a non-refutable administrative log that you have digitally signed and output in XML. You create this report with a tool known as the Audit Report Viewer, which is available from the **Audit** menu in the Policy Builder. For details, see [Chapter 14, Creating Reports from Secure Audit Server Output](#), in the *HP OpenView Select Access 6.1 Policy Builder Guide*.
- 4 Click **Next**. The **Validators** setup screen appears. See [Configuring Policy Validator Settings](#) on page 148.

## Configuring Policy Validator Settings

The **Validators** setup screen, shown in [Figure 12](#), allows you to determine which Policy Validators the Enforcer plugin uses to authenticate identities and authorize access.

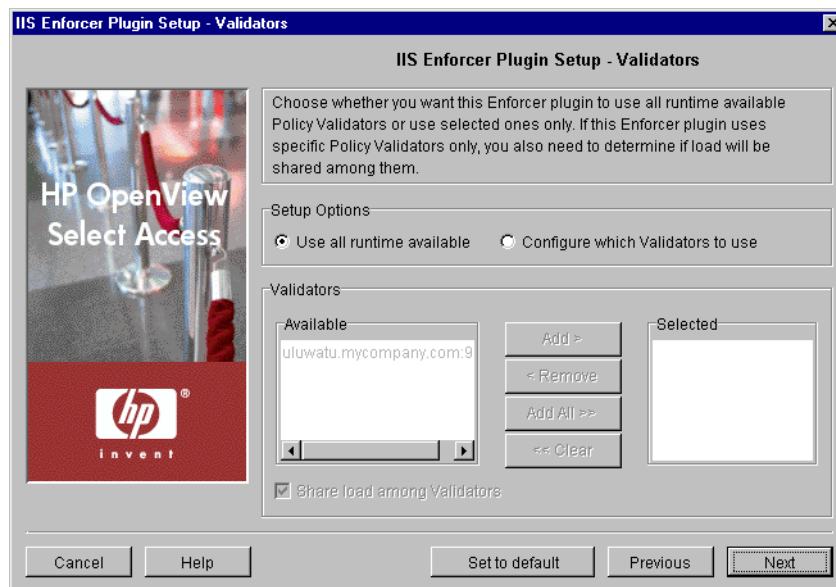
It also allows you to configure:

- **Round-robin support:** Provides load-balancing by distributing queries among a list of Policy Validators.
- **Failover support:** Ensures that the Enforcer plugin redirects a query to an available Policy Validator if the current Policy Validator is unable to process the query.



If you do not configure all your Policy Validators before configuring Enforcer plugins, the Enforcer plugin's bootstrap XML configuration file only includes the names of Policy Validators that were available at that time.

This can be problematic if you create a test or pilot deployment that initially includes only one Policy Validator, but add multiple new Policy Validators during a full Select Access deployment. Potentially any test Enforcer plugins (as well as your delegated administration Enforcer plugin), cannot failover and/or round robin to the new Policy Validators if the test Policy Validator fails. If you must stagger your deployment, re-run the Setup Tool for your existing Enforcer plugin to ensure all new Policy Validators are written to its `enforcer_<type>.xml` file.



**Figure 12** Validators Setup Screen

### To set Policy Validator settings

- 1 Review HP's recommended values. To customize these values, modify fields in the **Setup Options** and **Validators** groups as needed.
  - **Use all runtime available:** Optional. The Enforcer plugin uses all Policy Validators available at runtime for round-robin and failover support.



- **Configure which Validators to use:** Optional. The Enforcer plugin uses only the specific Policy Validators that you select for round-robin and failover support. If you select this option, you must move registered Policy Validators between the corresponding lists.



If you have not yet installed or configured a particular instance of the Policy Validator, it does not appear in the list of available Policy Validators. However, if you rerun the Setup Tool, any new Policy Validators subsequently appear in the list.

- **Validators:** Optional. If you enable the previous option, displays all registered Policy Validators in the **Available** list.

To move one or more Policy Validators to the **Selected** list, select them and click either the **Add** or **Add all** buttons. This creates a Validator list that the Enforcer plugin uses for failover and round-robinning (if you check the box described below).

To remove one or more Policy Validators from the Validator list, select them in the **Selected** list and click either the **Remove** or **Clear all** buttons.

- **Share load among Validators:** Optional. Check this box to balance query loads among Policy Validators in the Validator list and to randomly pick which Policy Validator the Enforcer plugin contacts first. If you do not check this box, the Enforcer plugin sends queries to the first Policy Validator in the selected list unless it cannot establish a connection. In this case, it then sends queries to the next Policy Validator in the list and gradually moves down the list until it can contact one of them.

To order the Policy Validators in the **Selected** list, select a Policy Validator and use the **Up** and **Down** arrows to sort them correctly.

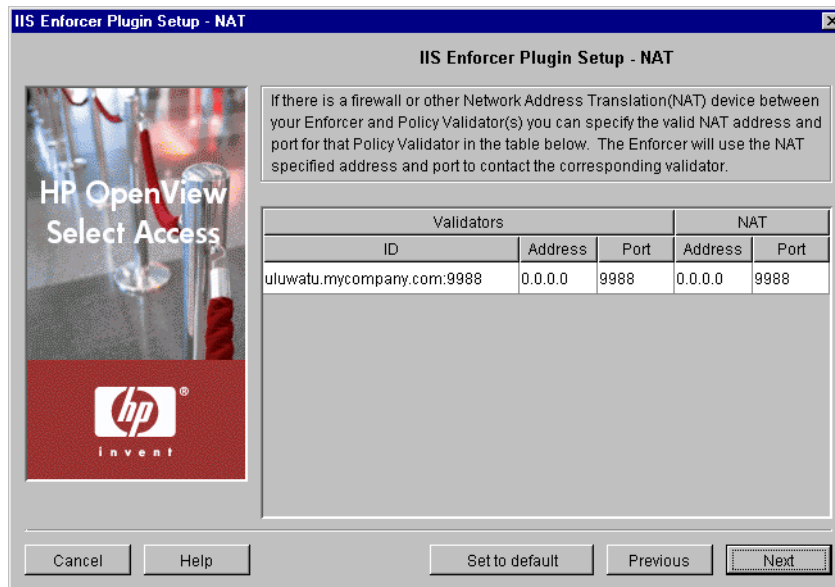
- 2 Click **Next**. The **NAT** setup screen appears. See [Mapping Policy Validators to NAT Addresses](#) on page 149.

## Mapping Policy Validators to NAT Addresses

The **NAT** setup screen, shown in [Figure 13](#), allows you to map a Policy Validator to a specific Network Address Translation (NAT) address or hostname. This allows the Enforcer plugin to communicate with the Policy Validator—even when there is a firewall and/or NAT device on your network between these components.



Only the Policy Validators this Enforcer plugin is configured to use appear in this table. The **Address** and **Port** cells in the **Policy Validator** column are automatically configured for you. Most Policy Validator addresses are automatically configured as 0.0.0.0, which means the Policy Validator is listening on all IP addresses configured for the Policy Validator's host computer. To configure more Policy Validators for this Enforcer plugin, click **Previous** and configure the **Validators** setup screen. See [Configuring Policy Validator Settings](#) on page 148 for details.



**Figure 13 NAT Setup Screen**

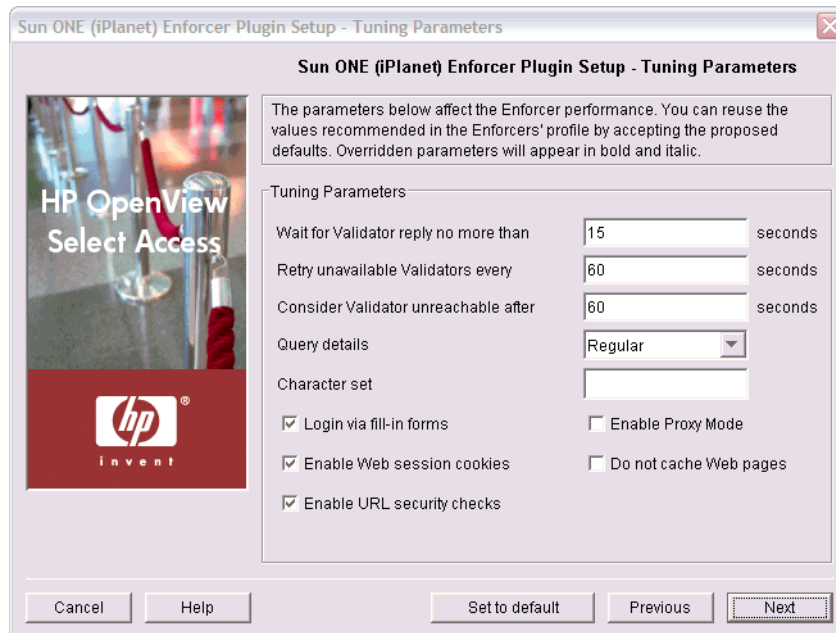
### To map a Policy Validator to a NAT address

- 1 For the corresponding Policy Validator ID, click the **Address** cell below the **NAT** column. If the **Address** appears as 0.0.0.0, it indicates that no firewall or NAT device exists between this Enforcer plugin and the corresponding Policy Validator. Otherwise, type the **NAT Address** for that Policy Validator.
- 2 If the NAT port number is different, click the **Port** cell and type the alternate Policy Validator port number.
- 3 Click **Next**. The **Tuning Parameters** setup screen appears. See [Tuning your Enforcer plugin](#) on page 150.

## Tuning your Enforcer plugin




The **Tuning Parameters** setup screen, shown in [Figure 14](#), allows you to adjust how the Enforcer plugin behaves at runtime. You can enhance the Enforcer plugin's performance depending on how you define the following settings.

- ▶ Text on the **Tuning Parameters** setup screen appear in bold and italics if the Enforcer plugin has any override values set for it. The remaining parameters are those that are shared by all Enforcer plugins.



**Figure 14 Tuning Parameters Setup Screen**

## To tune your Enforcer plugin

- Review HP's recommended values and modify fields in the **Tuning Parameters** group as needed.
  - Wait for Validator reply:** Defines the length of time the Enforcer plugin waits for a Policy Validator reply. If the reply is not received in this time, the connection is declared broken. The request is retried on the next available Policy Validator connection.
    -  You can use a value of 0 to disable this parameter; however, the Enforcer plugin does not stop waiting for a reply and the connection is never declared broken, which frees the plugin to try alternate connections.
    -  If this value is less than OCSP or the directory server timeout used by the Policy Validator, it can appear as if the Policy Validator and Enforcer plugin have entered into a query loop. In reality, the Enforcer plugin is actually resending queries to the Policy Validator before the Policy Validator returns a response for the original query. However, to correct this problem, increase the value of the Enforcer plugin's **Wait for Validator Reply** setting parameter.
  - Retry unavailable Validators:** If the Enforcer plugin declares a Policy Validator connection broken, it does not try to reopen a new connection until the configured number of seconds have passed. Reasons a connection is considered broken include:
    - The Enforcer plugin reached the timeout limit (configured by the **Consider Validator unreachable** parameter below).
    - A network communication error was detected on the connection.
    -  Good practice dictates that you configure the Enforcer plugin to forward all queries to other Policy Validators in a pool if they are available.

- **Consider Validator unreachable:** Defines the timeout interval for each individual connection attempt, after which time the Enforcer plugin declares the connection failed if the connection is not established within that time. The Enforcer plugin tries to re-connect only after the retry delay (described above) has been reached.



You can use a value of 0 to disable this parameter; however, you will break failover as a result.



Carefully consider the settings you make for **Wait for Validator reply**, **Retry unavailable Validators**, and **Consider Validator unreachable** parameters. If you are still unsure of the implications among these parameters, consider reading an example scenario described in [A Tuning Parameters Walk-through](#) on page 153.

- **Query details:** Determines the number of fields the Enforcer plugin adds to the XML query. The more query fields the Enforcer plugin adds (even when it does not use them in the decision process), the more it slows the communication process with Policy Validator. [Table 3](#) outlines the levels you can choose and describes the differences among them.

**Table 3 Query Details Overview**

Level...	Description...
minimal	Sends a small amount of data to the Policy Validator: <ul style="list-style-type: none"> <li>• site_data</li> <li>• service</li> <li>• path</li> <li>• All related authentication elements</li> </ul>
regular	Sends standard query data: <ul style="list-style-type: none"> <li>• All of the minimal elements</li> <li>• http_query</li> <li>• method</li> <li>• dstIP and srcIP</li> <li>• dstPort and srcPort</li> <li>• dstHost</li> <li>• protocol</li> </ul>
maximal	Sends all available data: <ul style="list-style-type: none"> <li>• All of the minimal and regular elements</li> <li>• http_query_list</li> <li>• http_header_list</li> <li>• server</li> <li>• srcHost</li> </ul>

- **Character set:** Enter the name of the character set the Enforcer plugin uses to convert data to UTF-8 from the set you specify when a Web browser POSTs data to a Web server. The default character set is iso8859-1. You can change this value to any valid character set name for the system on which the you installed Enforcer plugin.

For details on a list of possible character sets you can use, see [Appendix B, Character Set Listing](#).

- **Login via fill-in forms:** Check this box to enable form-based login.



Check this box if you intend to use SecurID or RADIUS authentication.

- **Enable Web session cookies:** Check this box to use Web session cookies.



Check this box if Select Access needs to support form-based login.

- **Enable URL security checks:** Check this box if you want to perform security checks on URLs to determine whether they contain characters that could be unsafe.

- **Enable Proxy Mode:** If you have installed your Enforcer plugin on a proxy or reverse proxy server, check this box to allow URLs of the form:

```
<protocol>://:<proxy_server>/<path>/<protocol>://:
<web_server>/<path>
```

For example, `http://proxy.mycompany.com/portal/http://content_server.com/stories`

Typically, URLs of this and other forms are disallowed because they are considered to be suspicious. For details, see *Documented Enforcer plugin issues* in the *HP OpenView Select Access 6.1 Release Notes*.

- **Do not cache Web pages:** Check this box to prevent Web pages from being cached.



Check this box if you are using multidomain SSO with Apache, Netscape/iPlanet/Sun ONE Web servers.

- 2 Click **Next**. The **Finish** setup screen appears informing you that you have completed all setup tasks for the Enforcer plugin. See [Completing the Enforcer Plugin Setup Process](#) on page 154.

### A Tuning Parameters Walk-through

Consider the impact of the following settings when an Enforcer plugin connection attempt fails with a particular Policy Validator:

- **Wait for validator reply:** 15 seconds
- **Retry unavailable validator after:** 60 seconds
- **Consider validator unreachable after:** 15 seconds (default is 60)

The exchange between the Policy Validator and the Enforcer plugin are summarized as follows:

- 1 The Policy Validator receives and begins processing the Enforcer plugin's query.
- 2 The connections fails.
- 3 The Enforcer plugin waits for 15 seconds before declaring that connection broken.
- 4 The Enforcer plugin re-sends the same query to the next Policy Validator in the pool.
- 5 After 60 seconds, the Enforcer plugin attempts to reconnect to the original Policy Validator so subsequent queries are processed there.
- 6 If the original Policy Validator is still unavailable, the Enforcer plugin gives up on the connection attempt after retrying it for 15 seconds.
- 7 It again forwards the new query to the next available Policy Validator in the pool.

## Completing the Enforcer Plugin Setup Process

The **Finish/Update Configuration** screen allows you to commit the component's configuration to the Policy Store.

Depending on which enforcer you are configuring, the procedure varies:

- If you are configuring a Generic Enforcer plugin, click **Finish** to commit your configuration to the Policy Store you defined at the beginning of the Administration server's setup and the bootstrap XML file (`enforcer_<type>.xml`).



These bootstrap files contain startup and general configuration information for their respective Enforcer plugin. Modifying or moving these files could result in the Enforcer plugins being unable to start correctly. You should ensure that you protect these files using both logical and physical controls.

- If you are configuring the WSE Enforcer plugin, see [To complete the WSE Enforcer plugin setup](#) on page 154 to complete the setup process.
- If you are configuring any other Enforcer plugin, see [To complete the Netscape/iPlanet/Sun ONE, Apache 2, IIS or Axis Enforcer plugin setup](#) on page 155 to complete the setup process.

### To complete the WSE Enforcer plugin setup

- 1 Check **Update configuration files** if you want to ensure that the plugin is started each time you start your Web server. Checking this box causes Select Access to automatically modify the `web.config` configuration of one or more web services.
- 2 If you check **Update configuration files**, choose one of the following options:
  - **All Web Services:** Optional. Check this box to update the configuration files of all available web services.
  - **Select Specific Web Services:** Optional. Check this box to select specifically which web services you want to modify with your configuration changes.  
  
When you check this option, you must click **Select** to display the **Select Web Services** dialog box. From this dialog box, select which web services you want to update.
- 3 Check **Restart IIS Web Server** if you want to restart the IIS Web server after you have changed the WSE Enforcer plugin's configuration and/or updated the configuration file of one or more web services.
- 4 Click **Finish** to commit your configuration to both the Policy Store you defined at the beginning of the Administration server's setup and the bootstrap XML file (`enforcer_wse.xml`).



This bootstrap file contains startup and general configuration information for the WSE Enforcer plugin. Modifying or moving this file could result in this plugin being unable to start correctly. You should ensure that you protect this file using both logical and physical controls.

- 5 If you chose the **Update Web server configuration** option, the **IIS Web Server** dialog box appears. This dialog box allows you to provide the Start and Stop commands so that the Setup Tool can update the configuration file.



After configuring the WSE Enforcer plugin to protect the selected Web services, create the protected Web resource service and resources on the Resources Tree of the Policy Builder. .NET web service resources can be protected with following Select Access authentication services:

- Password
- Certificate
- SecurID (next pin scenario is not supported)
- Windows Kerberos (the domain name must be prepended to the login name)
- Windows NTLM (the domain name must be prepended to the login name)

For more information, see [The IIS Web Server Dialog Box](#) on page 158.

### To complete the Netscape/iPlanet/Sun ONE, Apache 2, IIS or Axis Enforcer plugin setup

- 1 Check **Update configuration files** if you want to ensure that the plugin is started each time you start your Web server. Checking this box causes Select Access to automatically modify the Web server's configuration.
- 2 Check **Restart Web server** if you want to restart your Web/Application server after you have changed the Enforcer plugin's configuration and updated the Web server's configuration file.
- 3 Click **Finish** to commit your configuration to the Policy Store you defined at the beginning of the Administration server's setup and the bootstrap XML file (`enforcer_<type>.xml`).



This bootstrap file contains startup and general configuration information for the WSE Enforcer plugin. Modifying or moving this file could result in this plugin being unable to start correctly. You should ensure that you protect this file using both logical and physical controls.

- 4 If you chose the **Update the configuration option**, one of the following dialog boxes appears. These dialog boxes request the information required to integrate the Enforcer plugin with its respective Web or Application server.
  - The **Netscape/iPlanet/Sun ONE Web Server** dialog box. For more information, see [The Netscape/iPlanet/Sun ONE Web Server Dialog Box](#) on page 156.
  - The **Apache Web Server** dialog box. For more information, see [The Apache Web Server Dialog Box](#) on page 157.
  - The **IIS Web Server** dialog box. For more information, see [The IIS Web Server Dialog Box](#) on page 158.
  - The **Axis Host Application** dialog box. For more information, see [The Axis Host Application Dialog Box](#) on page 159.

# Starting Your Enforcer Plugin

Because the Enforcer is a plugin, you need to configure your server to load the plugin on startup. Typically, you check the **Update Web server configuration to load the Enforcer plugin** box on the **Finish** setup screen. By checking this box, you cause the Setup Tool to display one of three dialog boxes that correspond to each type of Web server, as shown in [Table 4](#).

**Table 4 Dialog Boxes Displayed After Configuration**

<b>This server</b>	<b>For details, see...</b>
Netscape/iPlanet/ Sun ONE	<a href="#">The Netscape/iPlanet/Sun ONE Web Server Dialog Box on page 156</a>
Apache	<a href="#">The Apache Web Server Dialog Box on page 157</a>
IIS	<a href="#">The IIS Web Server Dialog Box on page 158</a>
Axis	<a href="#">The Axis Host Application Dialog Box on page 159</a>
TCP	<a href="#">Manually Configuring inetd to Start the TCP Enforcer Plugin on page 159</a>

However, you can also manually modify your Web server's configuration if you want to have more control over the process. For details, see [Preparing your Web Server for Integration](#) on page 45 in the *HP OpenView Select Access 6.1 Network Integration Guide*.

## The Netscape/iPlanet/Sun ONE Web Server Dialog Box

This dialog box allows you to select the version of your Web server as well as identify which configuration files it uses. The Setup Tool requires this information so it can integrate the Sun/Netscape/iPlanet Enforcer plugin with the Web server. Otherwise, it cannot automatically load with the Web server.



If you are running your Netscape/iPlanet/Sun ONE Web server over HTTPS, do not restart the server with the Setup Tool. HTTPS requires a password to start the Web server. Use the iPlanet or Sun ONE console to restart the server.



When using the iPlanet or Sun ONE console, do not use the **Save and Apply Configuration Files** option. It overwrites changes the Setup Tool automatically made to the server's configuration file. Instead, choose either **Load Configuration Files** or **Apply**.

### Server version

Required. Choose the server version. You can choose from 4.x., 6.0, or 6.1

### Path of obj.conf

Required. Click **Browse** and locate your Web server's `obj.conf` file. The Setup Tool modifies this file to include Select Access-specific changes.



### Path of magnus.conf

Required for version 6.x. Click **Browse** and locate your Web server's `magnus.conf` file. The Setup Tool modifies this file to include Select Access-specific changes.



The Setup Tool update changes the value of the `StackSize` parameter to 393216 in the `magnus.conf` file. It does this to prevent fatal errors from occurring in the Sun/Netscape/iPlanet Enforcer plugin. If it uses the default value, the Sun/Netscape/iPlanet Enforcer plugin runs out of stack—especially when logging to a Secure Audit server.

For more information on what lines are added, see [Chapter 3, Transparently Supported Web Server Integrations](#), in the *HP OpenView Select Access 6.1 Network Integration Guide*.

### Command to start/stop

Required for Windows systems. Click **Browse** and locate the specific batch file used to start and stop the Web Server. By default, the start and stop files are `startsvr.bat` and `stopsvr.bat` respectively.

## The Apache Web Server Dialog Box

The Apache Web Server dialog box appears if you checked **Restart Web Server** in the **Finish** setup screen of the Apache 2 Enforcer plugin setup wizard.

This dialog box allows you to integrate the Apache 2 Enforcer plugin with the Apache web server so it automatically loads with the web server.

### Path to httpd.conf

Optional. Click **Browse** and locate your Web server's `httpd.conf` file. The Setup Tool modifies this file to include Select Access-specific changes.

For more information on what lines are added, see [Chapter 3, Transparently Supported Web Server Integrations](#), in the *HP OpenView Select Access 6.1 Network Integration Guide*.

### Command to start/stop

Required. Click **Browse** and locate the specific batch file used to start and stop the Apache Web Server. By default, the start and stop files are `net start` and `net stop` respectively.



If you are running the Apache Web server on HP-UX, you need to start the Web server manually. For details, see [To start the Apache Web server on HP-UX manually](#) on page 157.

Or, if you want the Setup Tool to be able to start the Apache Web server, you need to export the corresponding environment variable for it. For details, see [To allow the Setup Tool to start the Apache Web server](#) on page 158.

## To start the Apache Web server on HP-UX manually

Depending on whether or not you have built Apache to run with `mod_ssl`, do one of the following:

- Without `mod_ssl`, run this command:

```
LD_PRELOAD=/usr/lib/libc1.2 apachectl start
```

- With `mod_ssl`, run this command:

```
LD_PRELOAD=/usr/lib/libc1.2 apachectl startssl
```



This technique can interfere with other software on HP-UX. HP recommends that, when possible, you set `LD_PRELOAD` in the environment. For details, see [To allow the Setup Tool to start the Apache Web server](#) on page 158.

## To allow the Setup Tool to start the Apache Web server

- 1 Exit the Setup Tool.
- 2 Set `LD_PRELOAD` in the environment with one of the following commands:  

```
export LD_PRELOAD=/usr/lib/libc1.2 /<install_path>/shared/setuptools
```

OR  

```
LD_PRELOAD=/usr/lib/libc1.2 /<install_path>/shared/setuptools
```
- 3 Restart the Setup Tool, configure the Apache 2 Enforcer plugin as needed, and use the **Apache Web Server** dialog box to start Apache.

## The IIS Web Server Dialog Box

The IIS Web Server dialog box appears if you checked **Restart Web Server** in the **Finish** setup screen of the IIS Enforcer plugin or WSE Enforcer plugin setup wizards.

This dialog box allows you to select the version of your Web server as well as identify which configuration files it uses. The Setup Tool requires this information so it can integrate the IIS Enforcer plugin with the Web server. Otherwise, it is unable to automatically load with the Web server.



The IIS Enforcer plugin requires that you assign an IP address to it. For details, see [Manually Integrating the IIS Enforcer plugin](#) on page 50, in the *HP OpenView Select Access 6.1 Network Integration Guide*.



You must stop the World Wide Web Publishing Service before configuring the settings in this dialog box. Otherwise, the Setup Tool cannot commit configuration changes that allow the IIS Web server to load the IIS Enforcer plugin. Use the following command to stop the World Wide Web Publishing service:

```
net stop iisadmin /y
```

**Note:** If you have other IIS dependency services like FTP Publishing Service, Simple Mail Transport Protocol (SMTP), and Network News Transport Protocol (NNTP) running from the same host machine, the previous command also stops these services. You will need to restart these services manually.

### Command to start/stop

Required. Click **Browse** and locate the specific batch file used to start and stop the IIS Web Server. By default, the start and stop files are `net start "World Wide Web Publishing Service"` and `net stop iisadmin /y` respectively.

## The Axis Host Application Dialog Box

The Axis Host Application dialog box appears if you checked **Restart Host Application** in the **Finish** setup screen of the Axis Enforcer plugin setup wizard.

This dialog box allows you to integrate the Axis Enforcer plugin with the Axis Engine so it automatically loads with the servlet container which hosts the Axis Engine.

### Path to server-config.wsdd

Required. Click **Browse** and locate the Axis Engine's configuration file. By default, this file is located at:

```
<AXIS_Home>/WEB-INF/server-config.wsdd
```

where `AXIS_HOME` is the installation directory of the Axis web application in the servlet container in which the Axis Engine runs.

The Setup Tool modifies this file to include Select Access-specific changes.

### Command to start/stop

Required. Click **Browse** and locate the specific batch file used to start and stop the Axis engine's host application. These commands will vary depending on what application is hosting your Axis engine.

For example, if your Axis engine is running in a Tomcat servlet container, the default start and stop files are `net start Tomcat` and `net stop Tomcat` respectively.



These commands are not restricted to Tomcat application servers nor to Windows 32-bit operating systems. Simply type appropriate values in the fields provided, so that they suit your operating system and your server type.

## Manually Configuring inetd to Start the TCP Enforcer Plugin

The TCP Enforcer plugin secures services configured in `/etc/inetd.conf`. For example, you can use this plugin with services such as FTP, finger, telnet, and rlogin.

You can configure `inetd` to invoke the TCP Enforcer plugin when starting a service. The TCP Enforcer plugin sends a query to the Policy Validator to determine if it can start the service. The plugin then starts or terminates the service, depending on the reply received from the Policy Validator.

### To configure inetd to start the TCP Enforcer plugin

- 1 Create an XML configuration file for the TCP Enforcer plugin by running the Setup Tool. For details, see [Connecting to the Administration Server](#) on page 135.

- 2 Open the following file:

```
/etc/inetd.conf
```

- 3 Modify your existing entries to use the following:

```
/opt/OV/SelectAccess/bin/tcp_enforcer tcp_enforcer [-r] [-c  
config_filename] [-p protocol_name]
```



All parameters are optional.

These parameters are described in [Table 5](#).

**Table 5 Optional Configuration Parameters Available**

Parameter	Usage
-c filename	Specifies an enforcer configuration file. <code>filename</code> is the name and location of the enforcer configuration file. If you do not provide a <code>filename</code> , the Enforcer plugin uses its default one.
-d	Enables internal debugging. You can increment the debug level by one for each parameter you use. For example, <code>-dd</code> increments the level of debugging to level two (which enables tracing).
-p protocol_name	Enter the protocol name used in Policy Builder if it is different than the program name used by the server. If you do not enter this parameter, the Enforcer plugin uses the last string in the program as the protocol name.
-r	Enables reverse name lookup. This option is necessary to verify host names (such as <code>www.mycompany.com</code> ) used in your security policy rules with an IP domains decision point.
-v	Returns the version number of the TCP Enforcer plugin and exits.

For example, suppose your `inetd.conf` file contains the following line:

```
ftp stream tcp nowait root /usr/sbin/tcpd in.ftpd -l -a
```

You then modify the line as follows:

```
ftp stream tcp nowait root /opt/OV/SelectAccess/bin/tcp_enforcer  
tcp_enforcer -p ftp /usr/sbin/in.ftpd -l -a
```

➤ Although the line in this example spans several lines, the line in your `inetd.conf` file must be a single line.

- 4 Restart your server so the old file does not remain cached.

## Uninstalling the Enforcer plugins

You can uninstall the Enforcer plugin using the uninstaller shipped with Select Access. For details, see [Uninstalling Select Access](#) on page 194.

➤ For Unix administrators, run the uninstaller as root to ensure all files are completely removed.

# 9 Configuring Custom Settings

While the Select Access Setup Tool provides a setup wizard for each Select Access component, it also includes an extra Custom Settings setup wizard designed to handle those rare instances when necessary parameters are not available in a component's own setup wizard. This chapter documents how to configure these settings.

## Chapter Overview

This chapter outlines how to configure custom settings. Topics in this chapter include:

- [Understanding Custom Settings](#) on page 161
- [When is it Necessary to Configure Custom Settings?](#) on page 161
- [Configuring the Custom Settings Flags](#) on page 162

## Understanding Custom Settings

As you upgrade Select Access, you may have a mixed environment of older and newer components. Tags used by older components may no longer match those used by newer ones. In order for these components to communicate with each other, they must use the same tags.

The Custom Settings setup component provides a central location where you can set a flag which instructs the newer components to use the old tags, so that backwards compatibility is maintained. Because these flags are set in the Setup Tool, the changes are global.



In most cases, the Custom Settings setup component can be ignored; it is intended for use primarily by HP's integration teams.

## When is it Necessary to Configure Custom Settings?

With the release of Select Access 5.2, three flags—each of which enables backwards compatibility between old and new components—are predefined and can be enabled as needed. However, the Custom Settings component is extensible, allowing you to add additional settings should the need arise.

Custom settings very rarely need to be configured. Typically, the average Select Access administrator will not need to access these settings. It is intended for use primarily by HP's integration staff, who may on occasion need to define a special parameter in order to ensure

that Select Access components can communicate and are behaving as they should. It is available to all administrators, however, since more sophisticated Select Access administrators may also find it useful.

- ▶ While adding new settings is documented in this chapter, the steps required to configure Select Access components so that they can use these settings are not.

## Configuring the Custom Settings Flags

The Custom Settings are initially configured via the Select Access Setup Tool. Because the Setup Tool is installed with the Select Access components, you can modify your settings at any time.

- ▶ You can also modify certain parameters that the Administration server writes to the Policy Store via the **Tools**→**Configure Components** command in the Policy Builder. For details, see [Chapter 16, Modifying Components' Central Configuration Parameters](#), in the *HP OpenView Select Access 6.1 Policy Builder Guide*.

## About Select Access Predefined Flags

HP has identified some common situations in which custom settings may be needed. By setting these flags, they become global settings for all Enforcer plugins.

Depending on the Enforcer plugin, the behavior of these flags vary. [Table 1](#) summarizes these behaviors.

**Table 1 Behaviors of Select Access Predefined Flags**

Flag Name	Description	Enforcer plugin Behavior
USE_OLD_P13N	Controls whether or not to prefix personalization headers added to resource request.	Adds prefixes according to what you configure in the USE_BSA_PREFIX flag. <sup>a</sup>
USE_BSA_PREFIX	Controls which prefix (BSA or SA) is added if you configured the previous flag. You can use this flag if you are upgrading from a Select Access version prior to version 5.2 and do not want to re-write HTTP headers.	If you configure Enforcer plugin to use this prefix, the header syntax for this header is HTTP_BSA <VARIABLE>. If you do not configure Enforcer plugins to use this flag, then the syntax is HTTP_SA<VARIABLE>.

- a. Sun/Netscape/iPlanet Enforcer plugin also check requests for suspicious headers, even if you also do not configure this flag name. For details, see [Denying Access to Suspicious URLs](#) on page 59 of the *HP OpenView Select Access 6.0 Network Integration Guide*.

- ▶ For information on how extract the attributes from these variables, see [Chapter 6, Implementing Select Access Personalization With Your Web Server](#) in the *HP OpenView Select Access 6.1 Concepts Guide*.

For details on how to enable personalization, see [To enable personalization](#) on page 88 of the *HP OpenView Select Access 6.1 Policy Builder Guide*

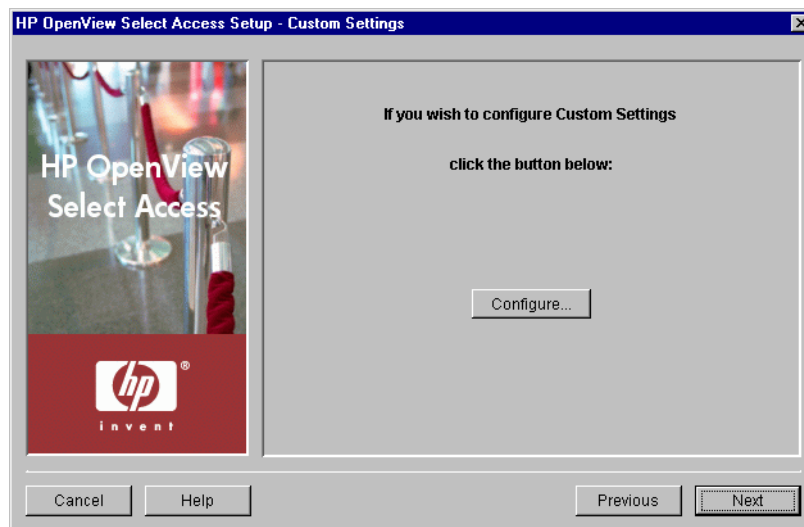
## Using the Setup Tool to Configure the Custom Settings Flags

If you choose to configure your Select Access components directly from the installer, the Setup Tool will be started for you automatically.

If you choose to configure your Select Access components at a later time, or want to modify your configuration settings, you can run the Setup Tool and access the Custom Settings configuration settings at any time.

### To set the custom settings flags

- 1 If the Setup tool is not already started, click **Start**→**Programs**→**HP OpenView**→**Select Access**→**Setup Tool**. The **Component Setup Tool** window appears.
- 2 Click **Next** until you reach the Setup Tool's **Custom Settings** setup screen.



**Figure 1 Custom Settings Setup Screen**

- 3 Click the **Configure** button. The **Custom Settings** setup process starts and the **Contact the Administration server** setup screen appears.
  - ▶ This screen does *not* appear if you have previously connected to the Administration server during your Setup Tool session, as the Setup tool already has the information needed to connect to it. In this case, the **Custom Settings Flags** setup screen appears instead.

- 4 Complete the setup screens of the Custom Settings setup process, listed in [Table 2](#), as necessary.

**Table 2 Overview of Custom Settings Setup Screens**

Setup Screen	Description	Default value(s)
<b>Contact the Administration Server</b> setup screen	Allows the Setup Tool to connect to the Administration server, so it can manage the custom settings flags. See <a href="#">Connecting to the Administration Server</a> on page 164.	auto-defined
<b>Custom Settings Flags</b> setup screen	Allows you to enable flags which override the typical behavior of the components to which they apply. You can enable one of the predefined backwards compatibility flags or add your own custom settings. See <a href="#">Enabling Custom Settings Flags</a> on page 165.	not defined
<b>Finish</b> setup screen	The <b>Finish</b> setup screen allows you to commit your configuration settings to the Policy Store, and to automatically start the Policy Validator. See <a href="#">Completing the Custom Settings Setup Process</a> on page 166.	enable Enforcer plugin restart

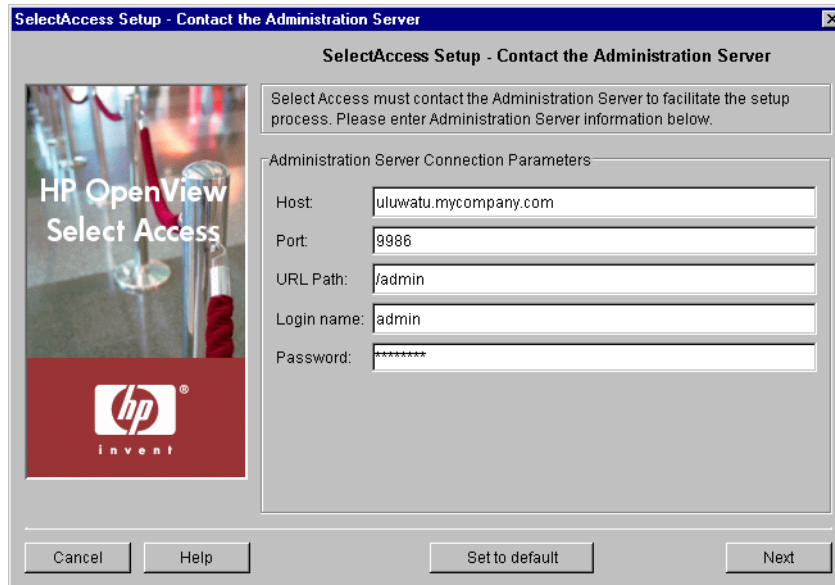
## Connecting to the Administration Server

In order to configure the custom settings, the Setup wizard must be able to connect to the Administration server. The Administration server stores and manages the custom settings flags. The **Contact the Administration server** setup screen, shown in [Figure 2](#), allows you to provide the connection parameters.



This screen does *not* appear if you have previously configured the Administration server settings during your Setup Tool session, since the Setup tool already has the information needed to connect to it. In this case, the **Custom Settings Flags** setup screen appears





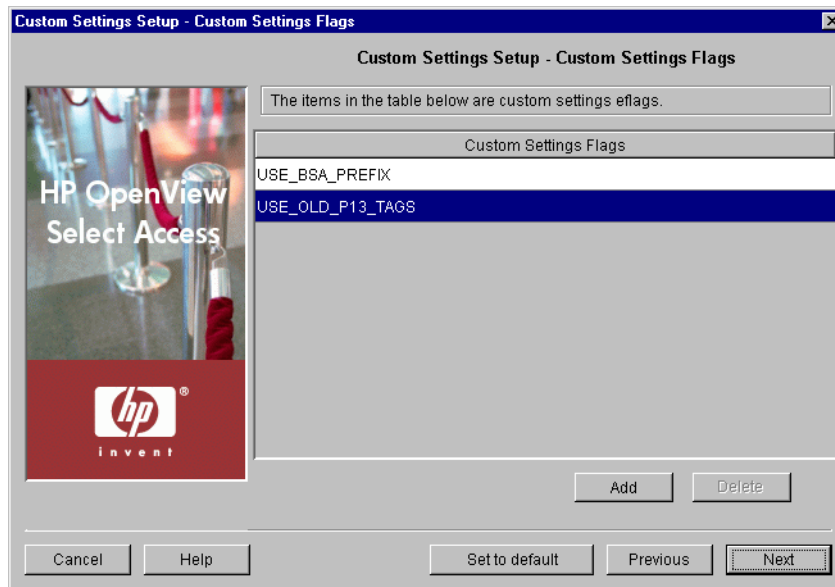
**Figure 2 Contact the Administration Server Setup Screen**

### To connect to the Administration server

- 1 Define values for the connection parameters in the **Administration Server Connection Parameters** group.
  - **Host:** Required. Enter the name or IP address of the host computer on which you have installed the Administration Server.
  - **Port:** Required. Enter the port the administration server is running on. By default, the port is 9986.
  - **URL Path:** Required. Enter the path to the Select Access Administration login page. By default, the path is /admin.
  - **Login name:** Required. Enter the Select Access root administrator's login name.
  - **Password:** Required. Enter the Select Access root administrator's password.
- 2 Click **Next**. At this point, the Setup Tool tries to connect to the Administration server. If it connects successfully, the **Custom Settings Flags** setup screen appears. Proceed to [Enabling Custom Settings Flags](#).

## Enabling Custom Settings Flags

The **Custom Settings Flags** setup screen, shown in [Figure 3](#), allows you to enable flags which override the typical behavior of the components to which they apply. You can enable one of the predefined backwards compatibility flags, described in [About Select Access Predefined Flags](#) on page 162, or add your own custom settings. Flags set in this screen are applied globally to all applicable components.



**Figure 3 Custom Settings Flags Setup Screen**

### To enable custom settings flags

- 1 Add flags to the **Custom Settings Flags** table to enable a setting:
  - a Click **Add**. A new row is added to the table.
  - b To select a predefined flag, right-click the row and choose the appropriate flag. For more information, see [About Select Access Predefined Flags](#) on page 162
  - c To add a new custom flag, select the row and type the flag name.

➤ Administrators are responsible for ensuring that the necessary Select Access components can read and understand any custom settings added through this setup screen. HP strongly recommends that only HP integration staff or sophisticated Select Access administrators add new custom settings.

- 2 Remove flags to disable a setting. Select the entry in question and click **Delete**.
- 3 Click **Next**. The **Finish** setup screen appears informing you that you have completed all setup tasks required. Proceed to [Completing the Custom Settings Setup Process](#).

### Completing the Custom Settings Setup Process

The **Finish** setup screen informs you that you have completed all setup tasks and allows you to automatically restart the Enforcer plugin.

### To complete the custom settings setup

- 1 If you want to start the Policy Validator immediately after the Setup Tool records your configuration parameters, click the **Restart now** box.
- 2 Click **Finish** to commit your configuration to the Policy Store.





# 10 Maintaining Select Access: Failovers, Repairs, and Updates

From time to time, changes on your network may require that you modify your current deployment of Select Access. From failures to new third-party technologies, you may find that you need to re-distribute components you have installed. This chapter explains how to perform these tasks.

## Chapter Overview

This chapter outlines how to maintain Select Access when system-wide modifications are required. Topics in this chapter include:

- [Failing Over to Another Administration Server](#) on page 169
- [Maintaining Select Access](#) on page 171

## Failing Over to Another Administration Server

Currently, you can only have one Administration server running on a Select Access-protected network at a time. However, if your current Administration server fails—especially in a large, decentralized network deployment—you need to install a new Administration server.



Be sure to regularly back up your Policy Store. For details, see the documentation provided by your directory server vendor.

Typically, you want to fail over to a new Administration server when the computer hosting the existing server fails. In this case, you want to recover the existing Administration server's configuration so that your distributed deployment can continue without any interruptions or setbacks.

## Tips for Ensuring a Smooth Recovery

To ensure a seamless recovery, always keep the following guidelines in mind:

- Because a decentralized deployment of Select Access typically involves a single host computer for each Select Access component, you can fail over to the same or a different host computer—depending on the severity of the incident that caused the computer to fail. In most cases, however, always consider installing the Administration server on its own host to simplify the process of recovering the failed computer.

- Back up the files listed in the following procedure to an archive format like TAR or ZIP. This keeps all files in a single location and makes it easier to recover the files needed to make your transition seamless.



Always remember to update your archives each time you reconfigure your current Administration server. Otherwise, other components on your network may behave unpredictably.

## To recover to an Administration server from a failed host

- 1 Back up the following files each time you reconfigure your Administration server.
  - From the `<install_path>\bin\` folder:
    - `adminserver.xml`: The local bootstrap configuration file that holds parameters needed to start the Administration server
  - From the `<install_path>\bin\` folder:
    - `rsa.*.key`: Your Select Access component key pairs.
    - `ca_cert.pem`: The CA certificate used by Select Access.
    - `*.pem`: Other certificates used in your deployment.
  - From the `<install_path>\shared\jetty\protected` folder: all certificate files.
  - If you are using database reporting, you also need all JDBC-compliant database driver files from `<install_path>\shared\`.
- 2 Run the Select Access installer on the computer that hosts the new Administration server. Do not run the Setup Tool to configure the server. Instead, finish the installation and exit the installer.
- 3 Copy the archived files listed in step 1 to their corresponding locations on the host computer.
- 4 Run the Setup Tool. Notice that the Setup Tool populates fields on the setup screens with values from your previous instance of the Administration server. You can accept or modify these values as needed.



If you accept the previous policy data location, the Setup Tool warns you that you are overwriting an existing installation. This warning appears because the Administration server records the identity of the computer on which it is running in the Policy Store on the directory server. When you run the Setup Tool on a different computer, it notices the difference in computer names, which triggers a warning. However, none of your pre-existing policy data is lost during configuration on the second computer; the only effect is to change the computer name recorded in the Policy Store.



Modifying certain parameters requires that you reconfigure existing Select Access components as well. See [Chapter 5, Configuring the Administration Server](#), for details.

## Maintaining Select Access

You can modify your existing installation of Select Access 6.1 at any time by running the maintenance program from either the Select Access installer or the Control Panel's **Add/Remove Programs** application on Windows, or the uninstaller program on Unix. The maintenance program allows you to perform the following actions:

- **Repair:** Reinstalls files for specific components only. For details, see [Repairing Select Access](#) on page 171.
- **Modify:** Installs a new component to the existing set of components already installed. For details, see [Modifying Select Access](#) on page 184.
- **Uninstall:** Uninstalls some or all of Select Access components on the current host machine. For details, see [Uninstalling Select Access](#) on page 194.

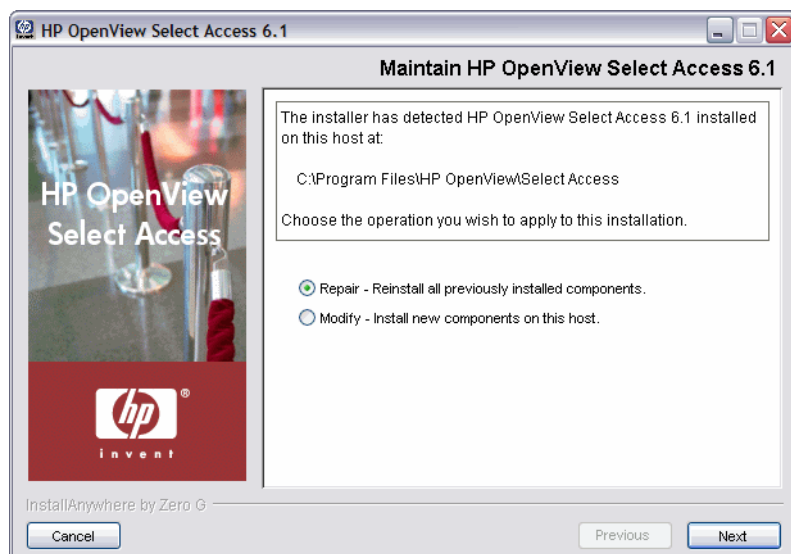
### Repairing Select Access

Select Access allows you to repair detected components on a given host computer. Typically, you want to repair a component when:

- It is under the advisement of HP's Identity Management Support team.
- One or more files have been overwritten or are missing.

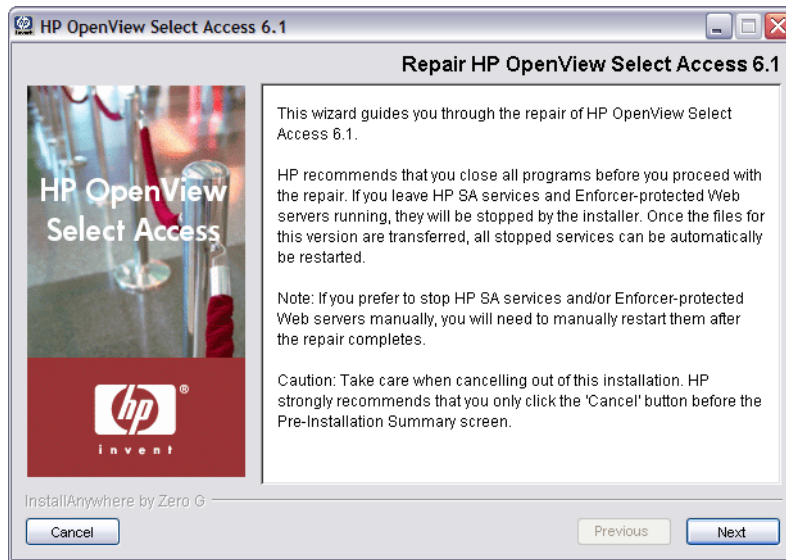
#### To repair detected components with Select Access's installer

- 1 Run the Select Access installer. The **Maintain HP OpenView Select Access 6.1** screen appears.



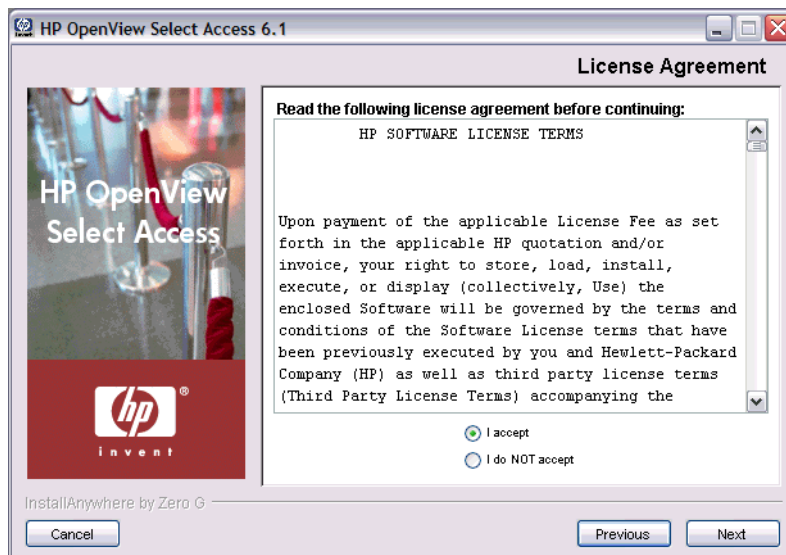
**Figure 1** Maintain HP OpenView Select Access 6.1 Screen

- 2 Click the **Repair** option. The **Repair HP OpenView Select Access 6.1** screen appears.



**Figure 2 Repair HP OpenView Select Access 6.1 Screen**

- 3 Click **Next**. The **License Agreement** screen appears.



**Figure 3 The License Agreement Screen**

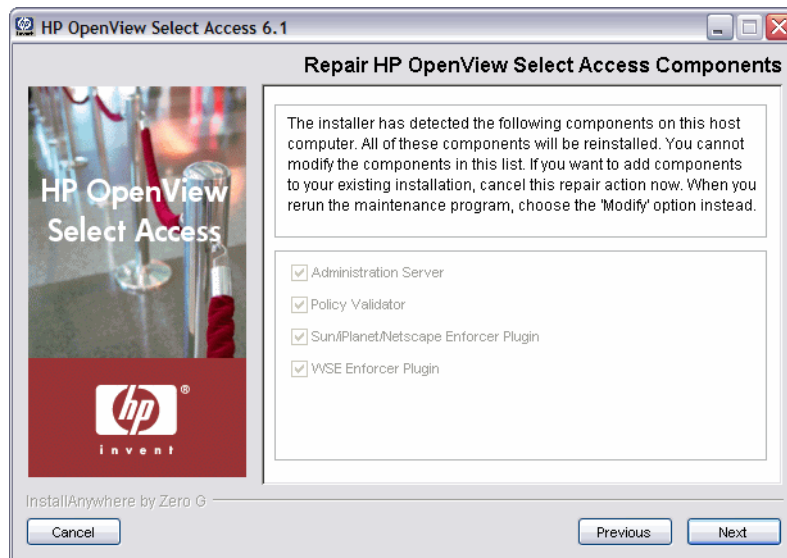
- 4 Read the license agreement. When you understand and agree to the terms, click the **I accept** option and click **Next**.

➤ You cannot proceed to the next screen until you accept the terms of the License agreement.



The **Repair HP OpenView Select Access Components** screen appears. This screen lists all components that are detected on this host computer. The maintenance program reinstalls the corresponding files for these components.

- ▶ You cannot modify the list of repairable components. Due to the cross-component dependencies that can exist, the maintenance program repairs all components. If you want to install new components in addition to reinstalling the components listed, run the installer in modify mode. For details, see [Modifying Select Access](#) on page 184.



**Figure 4 Repair HP OpenView Select Access Components Screen**

- 5 Click **Next**. If any HP services are running, the installer displays a warning message. Click **OK** to let the installer automatically stop the services for you. Otherwise, stop them manually now.

- ▶ On Windows, if you have any Enforcer-protected Web servers like Apache 2, Sun/Netscape/iPlanet, or IIS running, the installer also stops these servers. For the IIS Admin Service, all its dependent services are also stopped.

On Unix, the installer detects whether an Enforcer-protected Web server is running. However, you must manually stop the Web servers. The installer cannot do this automatically on these hosts.

The **Pre-Installation Summary** screen appears.



**Figure 5 Pre-Installation Summary Screen**

The **Pre-Installation Summary** screen creates a digest of the following installation information you provided to this point:

- The name and version of the product (that is, HP OpenView Select Access 6.1)
- The install path of Select Access.

On Windows, the default install path is:

```
C:\Program Files\HP OpenView\Select Access
```

On Unix, the default install path is:

```
/opt/OV/SelectAccess
```

- The folder that holds the program shortcuts for the Select Access administration tools.
  - The Select Access components you selected to install on this computer.
  - The installation location of the Java Virtual Machine that the Select Access Install Wizard has automatically installed. The Java Virtual Machine is required to run both the maintenance program as well as Select Access components—with the exception of the Policy Validator and the Enforcer plugins.
  - The amount of disk space required for the components you selected to install. If the disk space required exceeds what is available on this computer, free up space or adjust what you are currently intending to install.
- 6 Review this information. If your installation details are acceptable, click **Install** to begin the installation.



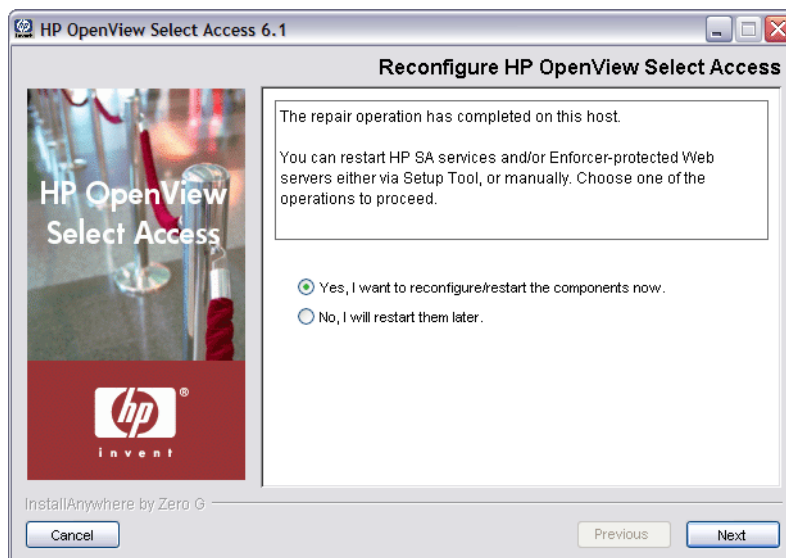
If you want to make changes, click **Previous** to change the install settings as required.

The **Installing HP OpenView Select Access 6.1** screen appears and outlines the installation progress of the components you selected to install.



**Figure 6 Installing HP OpenView Select Access 6.1 Screen**

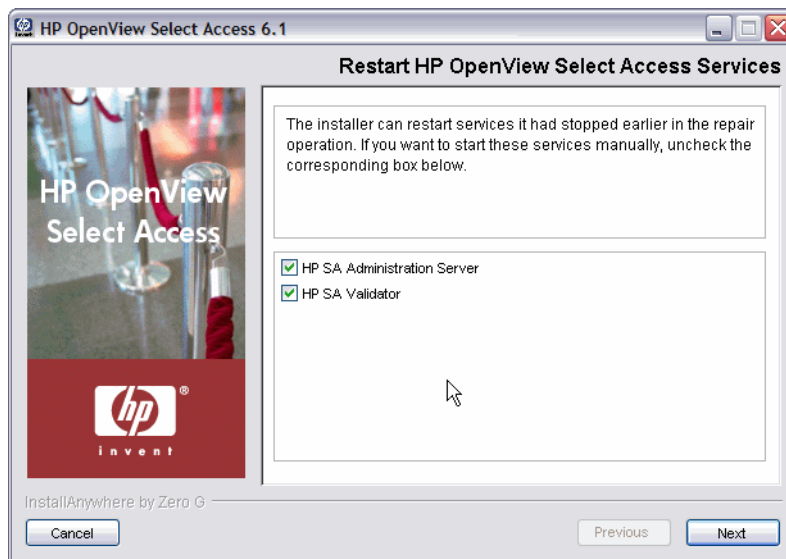
- 7 On completion, one of two things will happen:
- If you had installed and configured components that were running and stopped by the installer, you can complete the repair process. Skip to [step 10](#).
  - If you have:
    - Installed but unconfigured components.
- OR
- Installed and configured components but they were not running *before* you started repairing Select Access by running the installer, the **Reconfigure HP Select Access** screen appears. Skip to [step 8](#).



**Figure 7 Reconfigure HP OpenView Select Access Screen**

- 8 Click the corresponding option that determines whether or not you want to restart the host machine now:

- **Yes, I want to reconfigure/restart the components now.**
  - **No, I will restart them later.**
- 9 If you selected **Yes** in the previous step, a **Please Wait** screen appears while the maintenance program loads the Setup Tool. When the Setup Tool has loaded, the **Welcome to HP OpenView Select Access Setup** screen appears. Use the Setup Tool to configure the components you just installed as needed. For details, see [Chapter 4, Configuring Select Access](#). On completion, the Setup Tool will start those newly-configured components for you. You can now skip to [step 13](#).
- 10 For those existing deployments with running components that the installer automatically stopped during the repair, the **Restart HP OpenView Select Access Services** screen appears. If you stopped your own services before repairing Select Access, continue on to [step 11](#). Ensure that you restart the services that you had stopped manually after you exit this wizard.



**Figure 8 Restart HP OpenView Select Access Services Screen**

- 11 This screen prompts you to restart the components it had automatically stopped. To start a component, check the corresponding box beside the component's name.

➤ If you let the installer stop the IIS Admin Service, you are also prompted to restart it as well as any IIS-dependent services that the installer also stopped. Depending on whether or not you installed these dependencies on the same host computer as the IIS Admin service, the IIS-dependent services include: the World Wide Web Publishing service, the FTP Publishing service, the Simple Mail Transport Protocol (SMTP), and the Network News Transport Protocol (NNTP).

If you selected **No** in the previous step, you have finished the modification procedure.

➤ You must configure your components before you can start them. The Administration server must be configured before all other Select Access components.

When the installer is finished repairing and reconfiguring Select Access (if applicable), the **Installation Complete** screen appears.

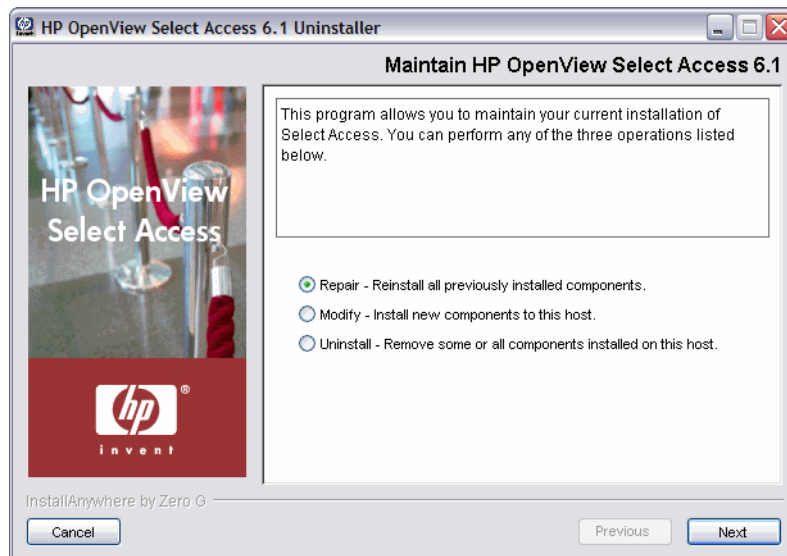
- 12 If errors were generated, click the **View install log** box to review the messages for those errors.
- 13 Click **Finish** to complete the installation of the product. The installer then:
  - Creates/modifies a global configuration file called `selectaccess.conf` in your installation directory root.
  - Cleans up all temporary installation files.

## To repair detected Select Access components from the Control Panel

- 1 Run the Select Access maintenance program.
  - *On Windows:*
    - From the **Start** menu, click **Settings**→**Control Panel**→**Add/Remove Programs**. The **Add/Remove Program Properties** dialog box appears.
    - Locate the **HP OpenView Select Access** entry from the list of installed programs and then click the **Add/Remove** button.
  - *On Unix:*
    - From the command line, enter the following: `<install_path>/UninstallerData/uninstaller`

The **Maintain HP OpenView Select Access 6.1** screen appears.

➤ If you are uninstalling, installing, or configuring Select Access components on a Windows host computer, ensure that you do not have the Services window—or any other Control Panel application open. This open Control Panel application triggers conflicts that cause the installer and Setup Tool to behave abnormally.



**Figure 9** Maintain HP OpenView Select Access 6.1 Screen

- 2 To reinstall all of Select Access 6.1, click the **Repair** option, and then click the **Next** button. The **Run Installer in Repair Mode** screen appears.

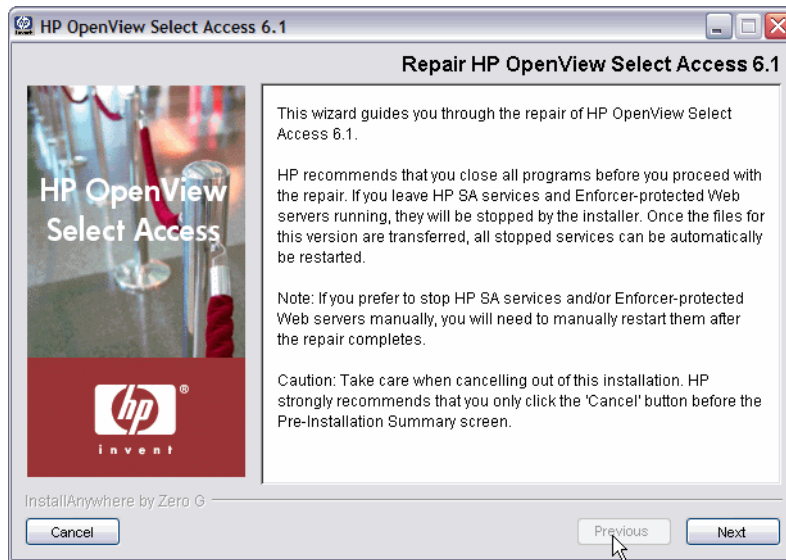


**Figure 10 Run Installer in Repair Mode Screen**

- 3 Configure the location of the installer:
  - If the default location is acceptable, proceed to step 4.
  - If you have moved your installer, click the **Choose** button, select the folder, and then click **OK**. The new folder appears in the **Installer** field.
  - If you choose the wrong folder, click the **Restore Default** button to restore Select Access defaults. If this is your first time running the maintenance program, the default installation folder is the location you originally ran the installer from. Otherwise, the path is the one you defined during the previous execution of this program.
    - The maintenance program does not support UNC network mapping conventions that define file locations using this format:
 

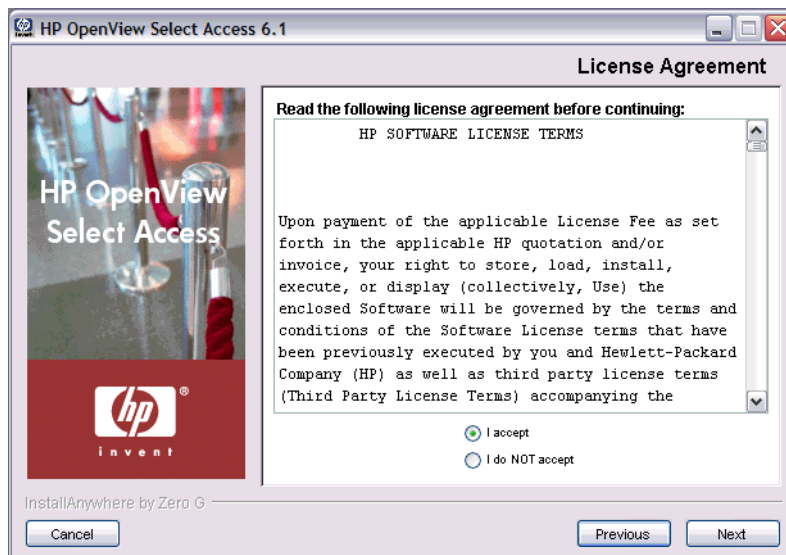
```
\\<server_name>\<path_name>
```

 Instead, either map the network folder to a specific letter drive and then browse to this network location, or run the executable locally.
- 4 Click **Next**. The maintenance program extracts the installer from this location. When it is finished, the **Repair HP OpenView Select Access 6.1** screen appears.



**Figure 11 The Repair HP OpenView Select Access 6.1 Screen**

- 5 Click **Next**. The **License Agreement** screen appears.



**Figure 12 The License Agreement Screen**

- 6 Read the license agreement. When you understand and agree to the terms, click the **I accept** option and click **Next**.

➤ You cannot proceed to the next screen until you accept the terms of the License agreement.

The **Repair HP Select Access Components** screen appears. This screen lists all components that are detected on this host computer. The maintenance program reinstalls the corresponding files for these components.

- ▶ You cannot modify the repair options on this screen. Due to the cross-component dependencies that can exist, the maintenance program repairs all components. If you want to install new components in addition to reinstalling the components listed in the screen shot that follows, run the maintenance program in modify mode. For details, see [To modify the current installation of Select Access from the Control Panel](#) on page 188.



**Figure 13 Repair HP OpenView Select Access Components Screen**

- 7 Click **Next**. If any HP services are running, the maintenance program displays a warning message. Click **OK** to let the installer automatically stop the services for you. Otherwise, stop them manually now.
  - ▶ On Windows, if you have any Enforcer-protected Web servers like Apache 2, Sun/Netscape/iPlanet, or IIS running, the maintenance program also stops these servers. For the IIS Admin Service, all its dependent services are also stopped.

On Unix, the installer detects whether an Enforcer-protected Web server is running. However, you must manually stop the Web servers. The installer cannot do this automatically on these hosts.

The **Pre-Installation Summary** screen appears.





**Figure 14 Pre-Installation Summary Screen**

The **Pre-Installation Summary** screen creates a digest of the following installation information you provided to this point:

- The name and version of the product (that is, HP OpenView Select Access 6.1)
- The install path of Select Access.

On Windows, the default install path is:

```
C:\Program Files\HP OpenView\Select Access
```

On Unix, the default install path is:

```
/opt/OV/SelectAccess
```

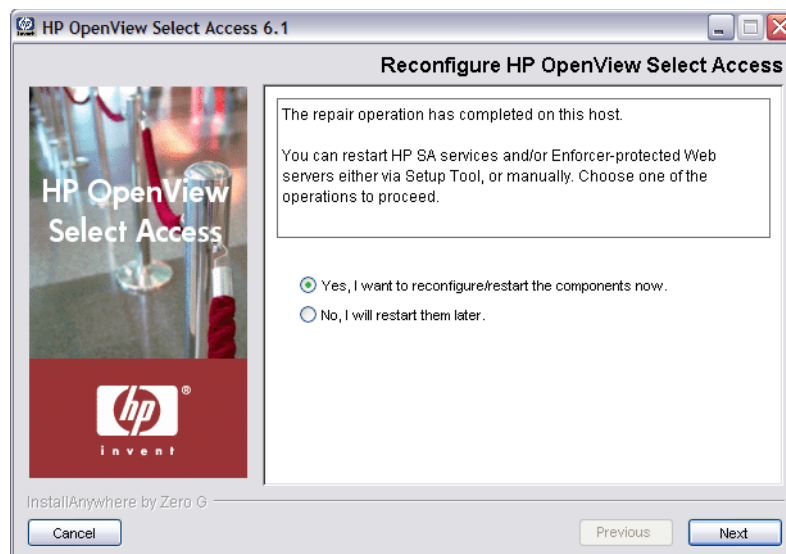
- The folder that holds the program shortcuts for the Select Access administration tools.
  - The Select Access components you selected to install on this computer.
  - The installation location of the Java Virtual Machine that the Select Access Install Wizard has automatically installed. The Java Virtual Machine is required to run both the maintenance program as well as Select Access components—with the exception of the Policy Validator and the Enforcer plugins.
  - The amount of disk space required for the components you selected to install. If the disk space required exceeds what is available on this computer, free up space or adjust what you are currently intending to install.
- 8 Review this information. If your installation details are acceptable, click **Install** to begin the installation.

The **Installing HP Select Access 6.1** screen appears and outlines the installation progress of the components you selected to install.



**Figure 15 Installing HP Select Access 6.1 Screen**

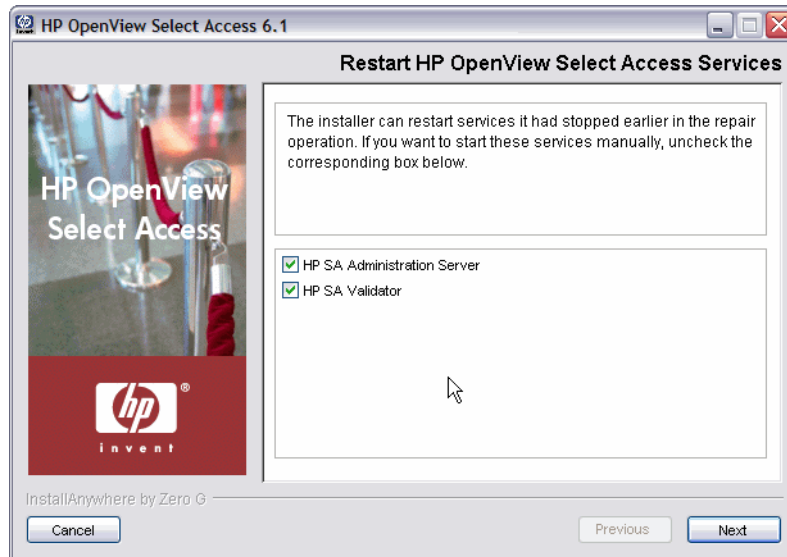
- 9 On completion, one of two things will happen:
- If you had installed and configured components that were running and stopped by the installer, you can complete the repair process. Skip to [step 12](#).
  - If you have:
    - Installed but unconfigured components.
- OR
- Installed and configured components but they were not running *before* you started repairing Select Access by running the installer, the **Reconfigure HP Select Access** screen appears. Continue to [step 10](#).



**Figure 16 Reconfigure HP OpenView Select Access Screen**

- 10 Click the corresponding option that determines whether or not you want to restart the host machine now:

- **Yes, I want to reconfigure/restart the components now.**
  - **No, I will restart them later.**
- 11 If you selected **Yes** in the previous step, a **Please Wait** screen appears while the maintenance program loads the Setup Tool. When the Setup Tool has loaded, the **Welcome to HP OpenView Select Access Setup** screen appears. Use the Setup Tool to configure the components you just installed as needed. For details, see [Chapter 4, Configuring Select Access](#). On completion, the Setup Tool will start those newly-configured components for you. You can now skip to [step 14](#).
  - 12 For those existing deployments with running components that the installer automatically stopped during the repair, the **Restart HP OpenView Select Access Services** screen appears.



**Figure 17 Restart HP OpenView Select Access Services Screen**

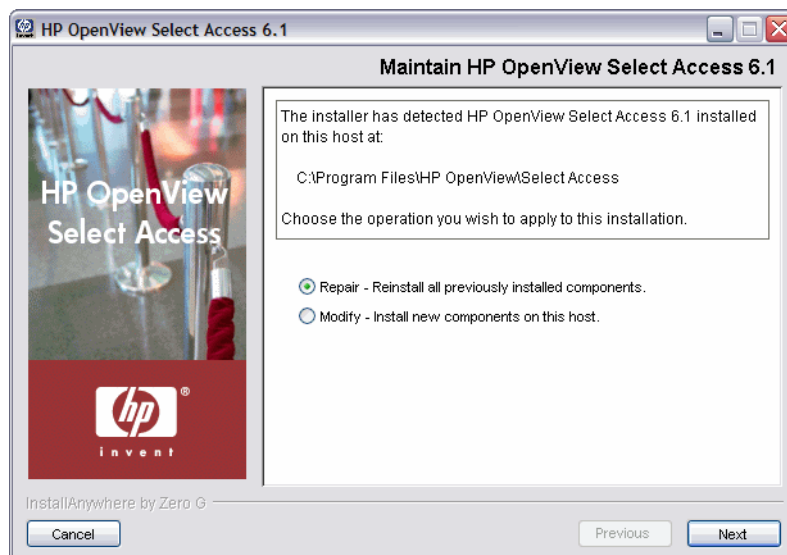
- 13 This screen prompts you to restart the components it had automatically stopped. To start a component, check the corresponding box beside the component's name.
  - ▶ If you let the installer stop the IIS Admin Service, you are also prompted to restart it as well as any IIS-dependent services that the installer also stopped. Depending on whether or not you installed these dependencies on the same host computer as the IIS Admin service, the IIS-dependent services include: the World Wide Web Publishing service, the FTP Publishing service, the Simple Mail Transport Protocol (SMTP), and the Network News Transport Protocol (NNTP).
- 14 When the installer is finished repairing and reconfiguring Select Access (if applicable), the **Installation Complete** screen appears.
- 15 If errors were generated, click the **View install log** box to review the messages for those errors.
- 16 Click **Finish** to complete the installation of the product. The installer then:
  - Creates a global configuration file called `selectaccess.conf` in your installation directory root.
  - Cleans up all temporary installation files.

## Modifying Select Access

Select Access allows you to modify your current installation by installing new components on this host computer.

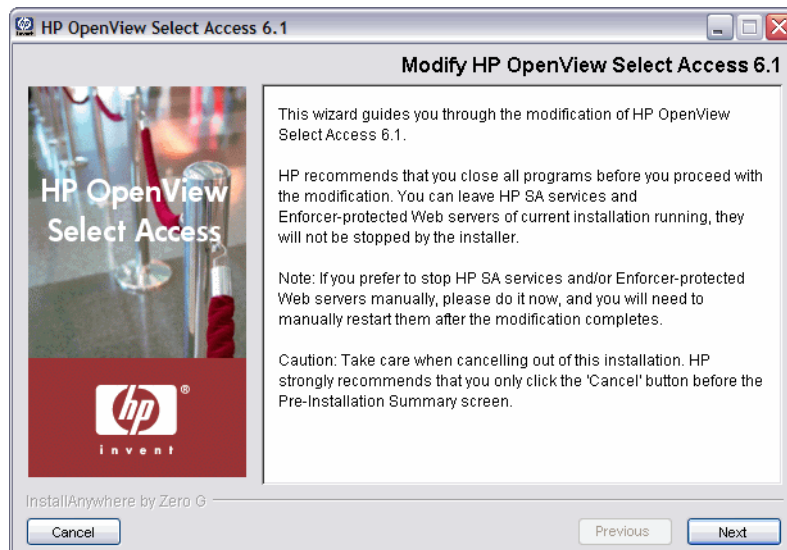
### To modify current installations of Select Access with the installer

- 1 Run the Select Access installer. The **Maintain HP OpenView Select Access 6.1** screen appears.



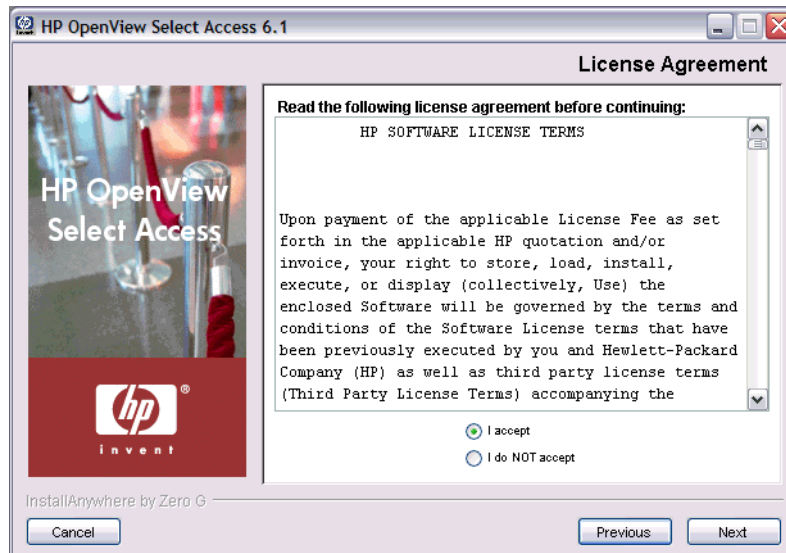
**Figure 18 Maintain HP OpenView Select Access 6.1 Screen**

- 2 Click the **Modify** option. The **Modify HP OpenView Select Access 6.1** screen appears.



**Figure 19 Modify HP OpenView Select Access 6.1 Screen**

- 3 Click **Next**. The **License Agreement** screen appears.

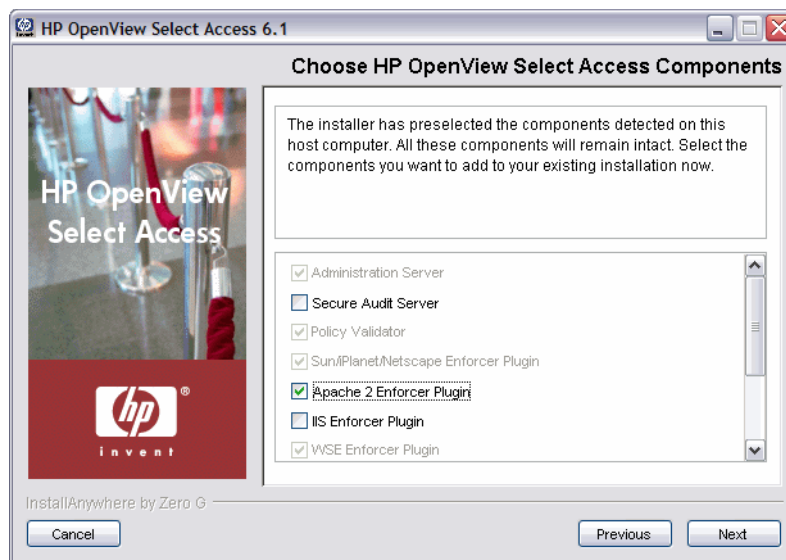


**Figure 20 The License Agreement Screen**

- 4 Read the license agreement. When you understand and agree to the terms, click the **I accept** option and click **Next**.

➤ You cannot proceed to the next screen until you accept the terms of the License agreement.

The **Choose HP OpenView Select Access Components** screen appears.



**Figure 21 Choose HP OpenView Select Access Components Screen**

- 5 Review the list displayed to you:
  - The greyed out but checked components are those that have been previously installed on this host and will not be upgraded. You cannot modify these components.
  - Any additional components available to be added are listed but are unchecked. You can check these boxes if you would like an additional component installed.

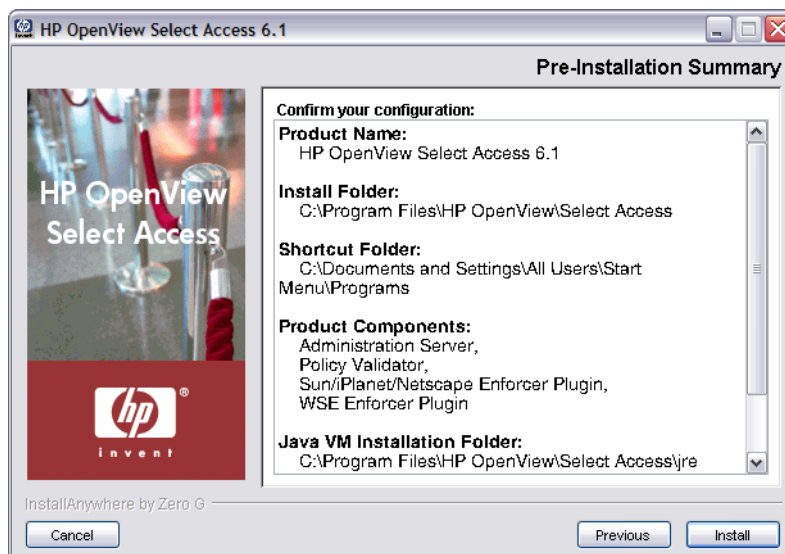
The maintenance program installs only the newly-checked components.

- ▶ On Windows, if you have any Enforcer-protected Web servers like Apache 2, Sun/Netscape/iPlanet, or IIS running, the maintenance program also stops these servers. For the IIS Admin Service, all its dependent services are also stopped.

On Unix, the installer detects whether an Enforcer-protected Web server is running. However, you must manually stop the Web servers. The installer cannot do this automatically on these hosts.

- 6 Click **Next**. Because the maintenance program will not touch any currently installed components, it does not detect or stop running Select Access services or Enforcer-protected Web servers. If your business environment allows you to stop these services/servers, HP recommends that you do so.

The **Pre-Installation Summary** screen appears.



**Figure 22 Pre-Installation Summary Screen**

The **Pre-Installation Summary** screen creates a digest of the following installation information you provided to this point:

- The name and version of the product (that is, HP OpenView Select Access 6.1)
- The install path of Select Access.

On Windows, the default install path is:

```
C:\Program Files\HP OpenView\Select Access
```

On Unix, the default install path is:

```
/opt/OV/SelectAccess
```

- The folder that holds the program shortcuts for the Select Access administration tools.
- The Select Access components you selected to install on this computer.
- The installation location of the Java Virtual Machine that the Select Access Install Wizard has automatically installed. The Java Virtual Machine is required to run both the maintenance program as well as Select Access components—with the exception of the Policy Validator and the Enforcer plugins.

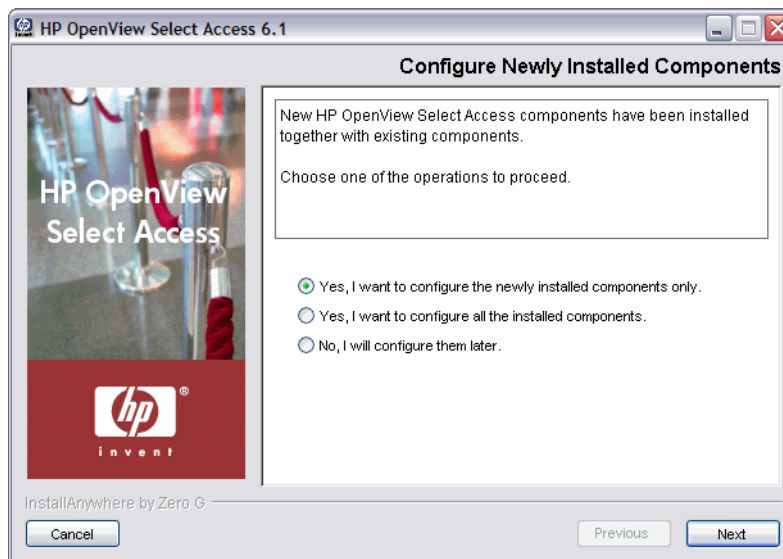
- The amount of disk space required for the components you selected to install. If the disk space required exceeds what is available on this computer, free up space or adjust what you are currently intending to install.
- 7 Review this information. If your installation details are acceptable, click **Install** to begin the installation.
    - ▶ If you want to make changes, click **Previous** to change the install settings as required.

The **Installing HP OpenView Select Access 6.1** screen appears and outlines the installation progress of the components you selected to install.



**Figure 23 Installing HP OpenView Select Access 6.1 Screen**


- 8 On completion, the **Configure Newly Installed Components** screen appears.



**Figure 24 Configure Newly Installed Components Screen**

- 9 Click the corresponding option that determines whether or not you want to configure the newly installed components on the host machine now:

- **Yes, I want to configure the newly installed components only.**
- **Yes, I want to configure all installed components.**
- **No, I will configure them later.**

 If you stopped your own services before modifying Select Access, ensure that you restart the services that you had stopped manually after you exit this wizard.

- 10 When the installer is finished repairing and reconfiguring Select Access (if applicable), the **Installation Complete** screen appears.
- 11 If errors were generated, click the **View install log** box to review the messages for those errors.
- 12 Click **Finish** to complete the installation of the product. The installer then:
  - Creates a global configuration file called `selectaccess.conf` in your installation directory root.
  - Cleans up all temporary installation files.

## To modify the current installation of Select Access from the Control Panel

- 1 Run the Select Access maintenance program.


*On Windows:*

- From the **Start** menu, click **Settings**→**Control Panel**→**Add/Remove Programs**. The **Add/Remove Program Properties** dialog box appears.
- Locate the **HP OpenView Select Access** entry from the list of installed programs and then click the **Add/Remove** button.

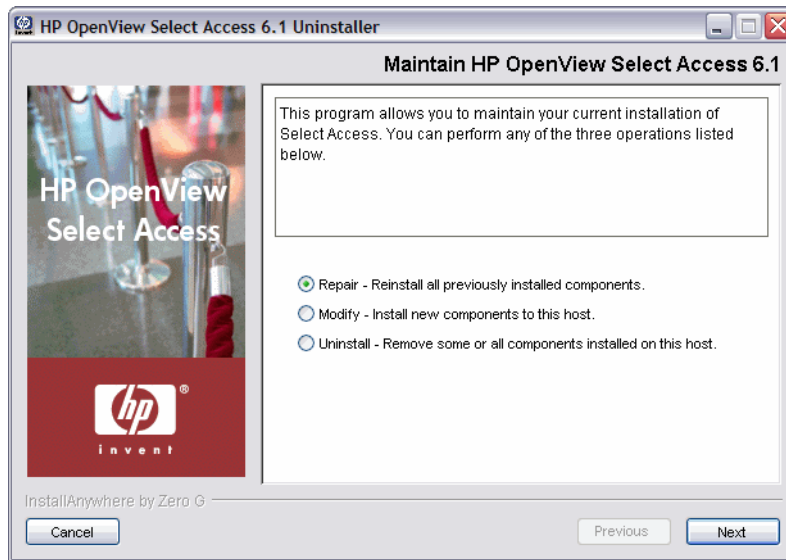
*On Unix:*

From the command line, enter the following: `<install_path>/UninstallerData/Uninstaller`

The **Maintain HP OpenView Select Access 6.1** screen appears.

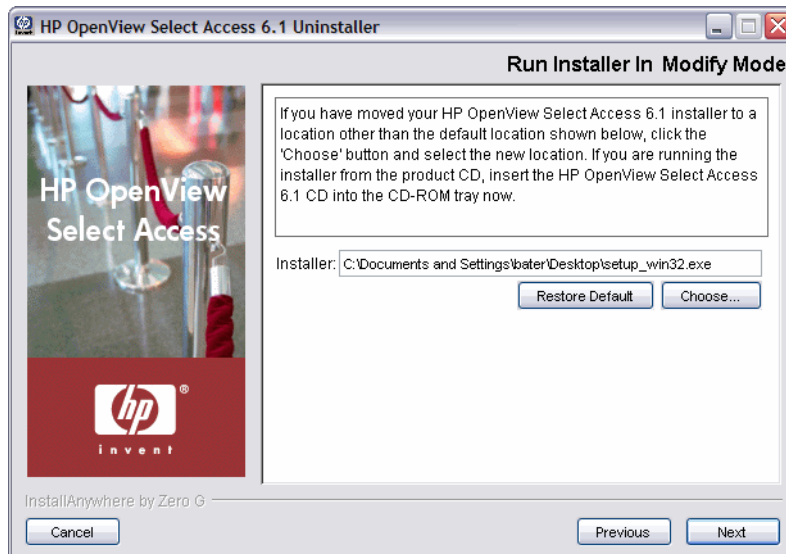
 If you are uninstalling and/or installing or configuring Select Access components on a Windows host computer, ensure that you do not have the Services window—or any other Control Panel application open. This open Control Panel application triggers conflicts that cause the installer and Setup Tool to behave abnormally.





**Figure 25 Maintain HP OpenView Select Access 6.1 Screen**

- 2 To uninstall all or part of Select Access 6.1, click the **Modify** option, and then click the **Next** button. The **Run Installer in Modify Mode** screen appears.



**Figure 26 Run Installer in Modify Mode Screen**

- 3 Select from one of the following configuration options:
  - If the default location is acceptable, proceed to step 4.
  - If you want to select a different installation folder, click the **Choose** button, select a folder, and then click **OK**. The new folder appears in the **Installer** field.

- If you choose the wrong folder, click the **Restore Default** button to restore Select Access defaults. If this is your first time running the maintenance program, the default installation folder is the location you originally ran the installer from. Otherwise, the path is the one you defined during the previous execution of this program.

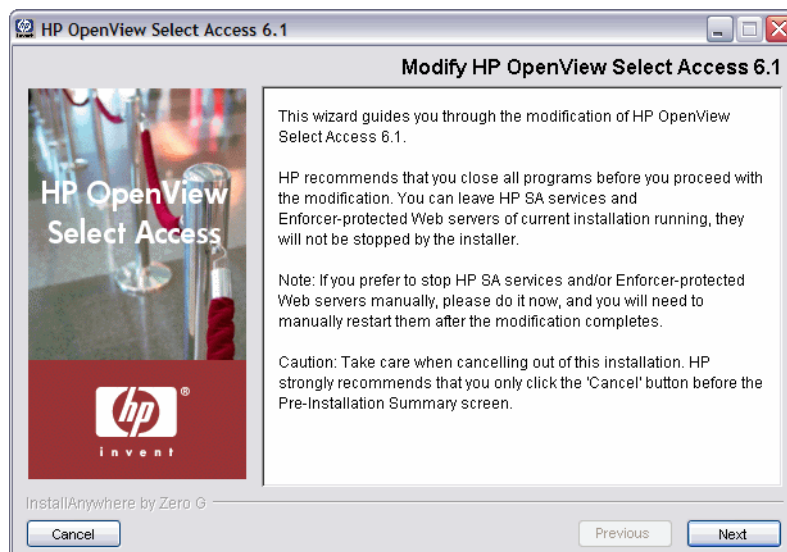
- The maintenance program does not support UNC network mapping conventions that define file locations using this format:

```
\\<server_name>\<path_name>
```

Instead, either map the network folder to a specific letter drive and then browse to this network location, or run the executable locally.

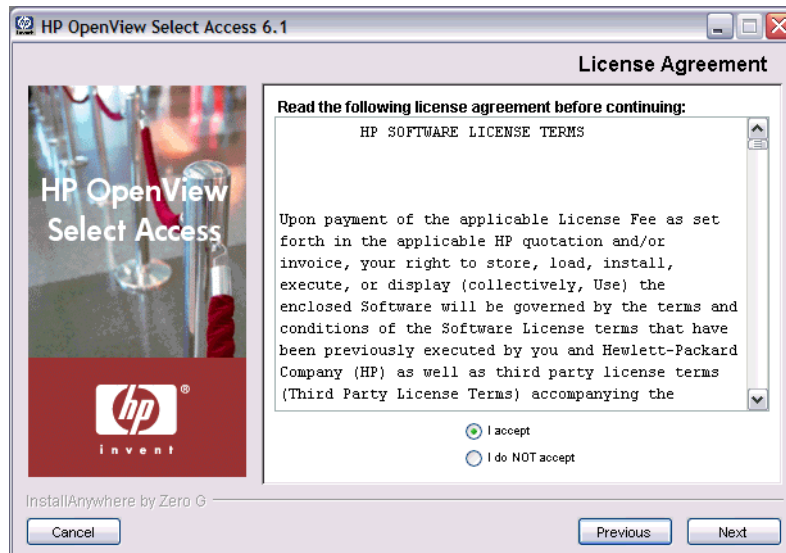
- To make sure the *HP OpenView Select Access 6.1 Release Notes* are installed to the installation directory, ensure the installer resides in the same path as the Select Access `docs` folder. To ensure this, HP recommends that you always run the installer from the product CD.

- 4 Click **Next**. The maintenance program extracts the installer from this location. When it is finished, the **Modify HP OpenView Select Access 6.1** screen appears.



**Figure 27 The Modify HP OpenView Select Access 6.1 Screen**

- 5 Click **Next**. The **License Agreement** screen appears.

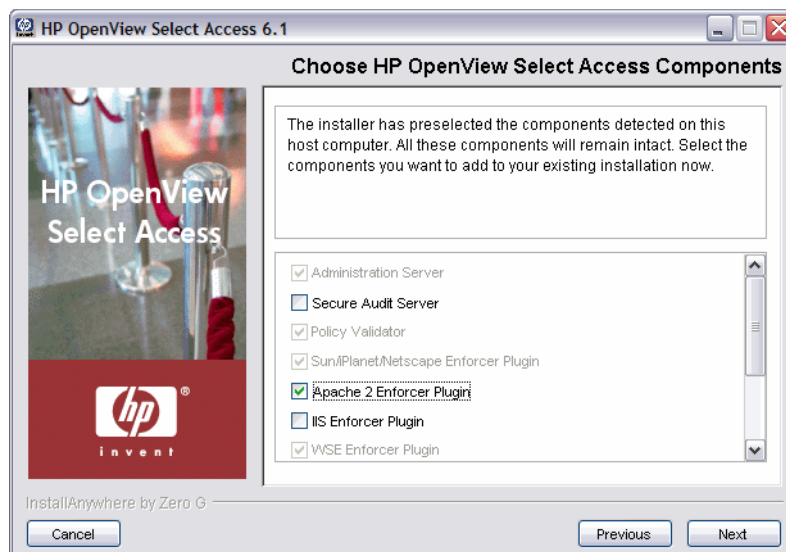


**Figure 28 The License Agreement Screen**

- 6 Read the license agreement. When you understand and agree to the terms, click the **I accept** option and click **Next**.

➤ You cannot proceed to the next screen until you accept the terms of the License agreement.

The **Choose HP OpenView Select Access Components** screen appears.



**Figure 29 Choose HP OpenView Select Access Components Screen**

- 7 Review the list displayed to you:
  - The greyed out but checked components are those that have been previously installed on this host and will not be upgraded. You cannot modify these components.
  - Any additional components available to be added are listed but are unchecked. You can check these boxes if you would like an additional component installed.

The maintenance program installs only the newly-checked components.

- 8 Click **Next**. Because the maintenance program will not touch any currently installed components, it does not detect or stop running Select Access services or Enforcer-protected Web servers. If your business environment allows you to stop these services/servers, HP recommends that you do so.

The **Pre-Installation Summary** screen appears.



**Figure 30 Pre-Installation Summary Screen**

The **Pre-Installation Summary** screen creates a digest of the following installation information you provided to this point:

- The name and version of the product (that is, HP OpenView Select Access 6.1)
- The install path of Select Access.

On Windows, the default install path is:

```
C:\Program Files\HP OpenView\Select Access
```

On Unix, the default install path is:

```
/opt/OV/SelectAccess
```

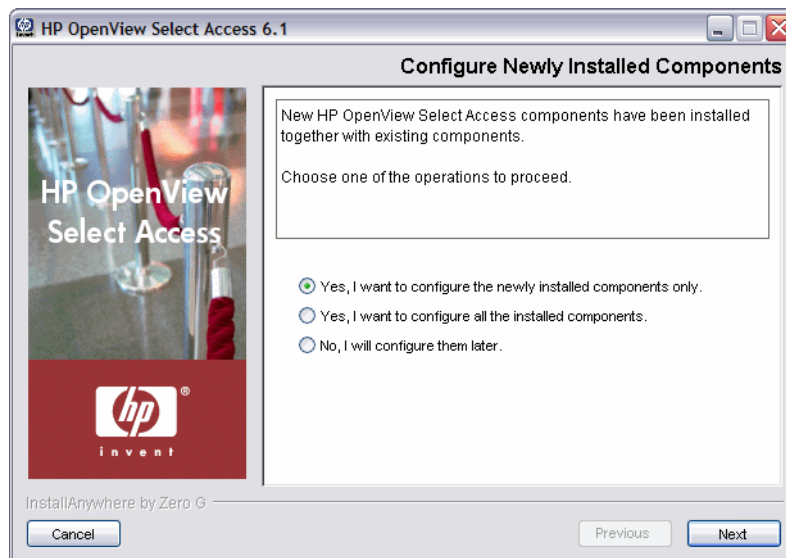
- The folder that holds the program shortcuts for the Select Access administration tools.
  - The Select Access components you selected to install on this computer.
  - The installation location of the Java Virtual Machine that the Select Access Install Wizard has automatically installed. The Java Virtual Machine is required to run both the maintenance program as well as Select Access components—with the exception of the Policy Validator and the Enforcer plugins.
  - The amount of disk space required for the components you selected to install. If the disk space required exceeds what is available on this computer, free up space or adjust what you are currently intending to install.
- 9 Review this information. If your installation details are acceptable, click **Install** to begin the installation.

The **Installing HP OpenView Select Access 6.1** screen appears and outlines the installation progress of the components you selected to install.



**Figure 31 Installing HP OpenView Select Access 6.1 Screen**

10 On completion, the **Configure Newly Installed Components** screen appears.



**Figure 32 Configure Newly Install Components Screen**

11 Click the corresponding option that determines whether or not you want to configure the newly installed components on the host machine now:

- **Yes, I want to configure the newly installed components only.**
- **Yes, I want to configure all installed components.**
- **No, I will configure them later.**

When the installer is finished repairing and reconfiguring Select Access (if applicable), the **Installation Complete** screen appears.

12 If errors were generated, click the **View install log** box to review the messages for those errors.

13 Click **Finish** to complete the installation of the product. The installer then:

- Creates a global configuration file called `selectaccess.conf` in your installation directory root.
- Cleans up all temporary installation files.

## Uninstalling Select Access

Select Access allows you to uninstall detected components on a given host computer, as well as unregister them from the Policy Store.

- ▶ If you are uninstalling and/or installing or configuring Select Access components on a Windows host computer, ensure that you do not have the Services window—or any other Control Panel application—open. This open Control Panel application triggers conflicts that cause the installer and Setup Tool to behave abnormally.

### To uninstall detected components of Select Access

- 1 Run the Select Access uninstaller.

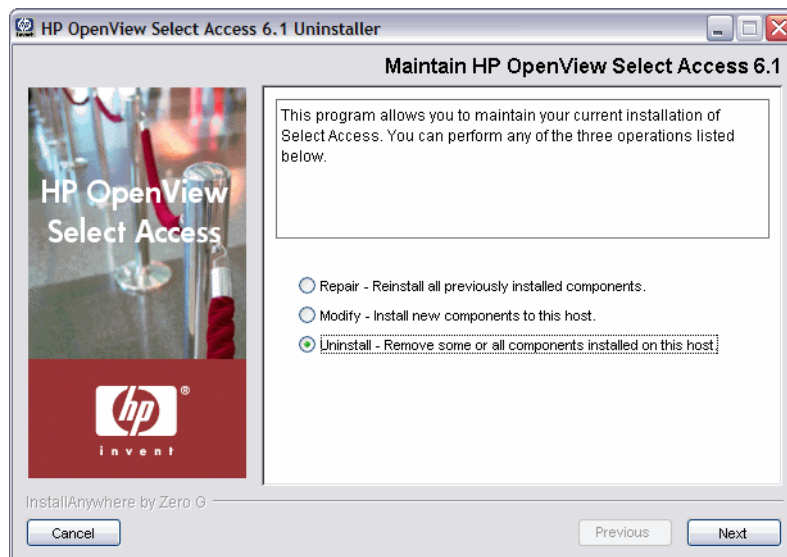
*On Windows:*

- From the **Start** menu, click **Settings**→**Control Panel**→**Add/Remove Programs**. The **Add/Remove Program Properties** dialog box appears.
- Locate the **HP OpenView Select Access** entry from the list of installed programs and then click the **Add/Remove** button.

*On Unix:*

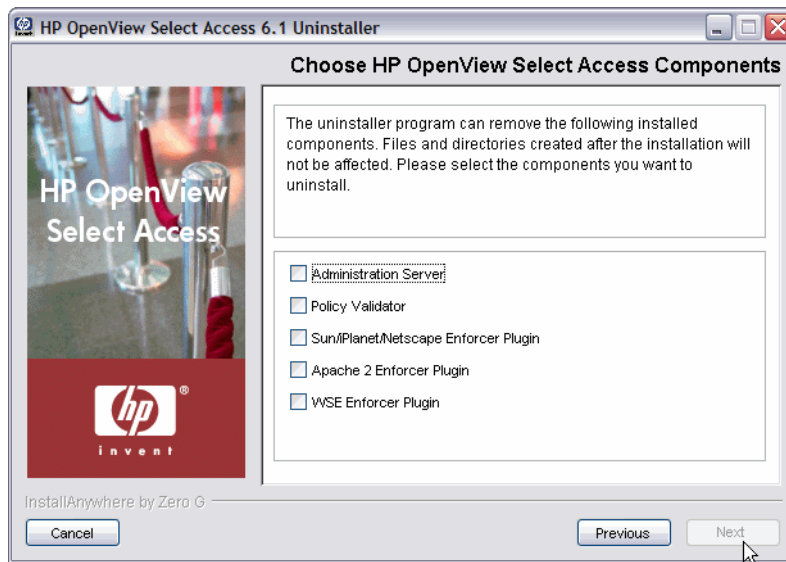
From the command line, enter the following: `<install_path>/UninstallerData/Uninstaller`

The **Maintain HP OpenView Select Access 6.1** screen appears.



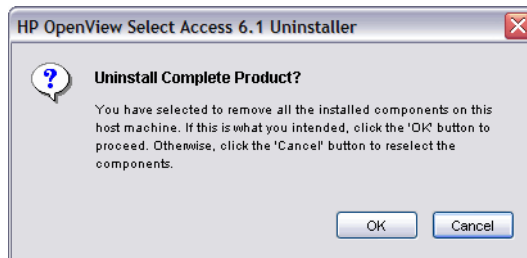
**Figure 33 Maintain HP OpenView Select Access 6.1 Screen**

- 2 To uninstall all or part of Select Access 6.1, click the **Uninstall** option, and then click the **Next** button. The **Choose HP OpenView Select Access Components** screen appears.



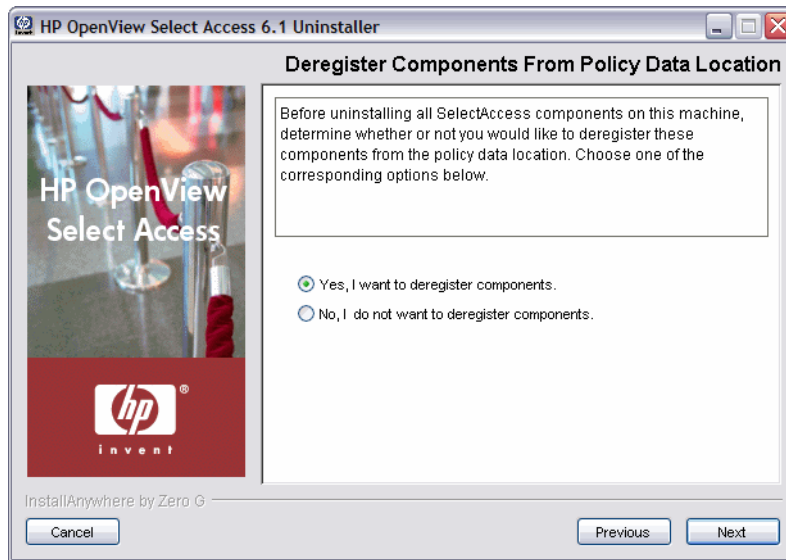
**Figure 34 Choose HP OpenView Select Access Components Screen**

- 3 Select each component you want to uninstall from this host computer by checking the box beside the corresponding component's name.
- 4 Click **Next**. If you are uninstalling all components, the **Uninstall Complete Product** confirmation dialog box appears. If you are only uninstalling some components, skip to step 6.



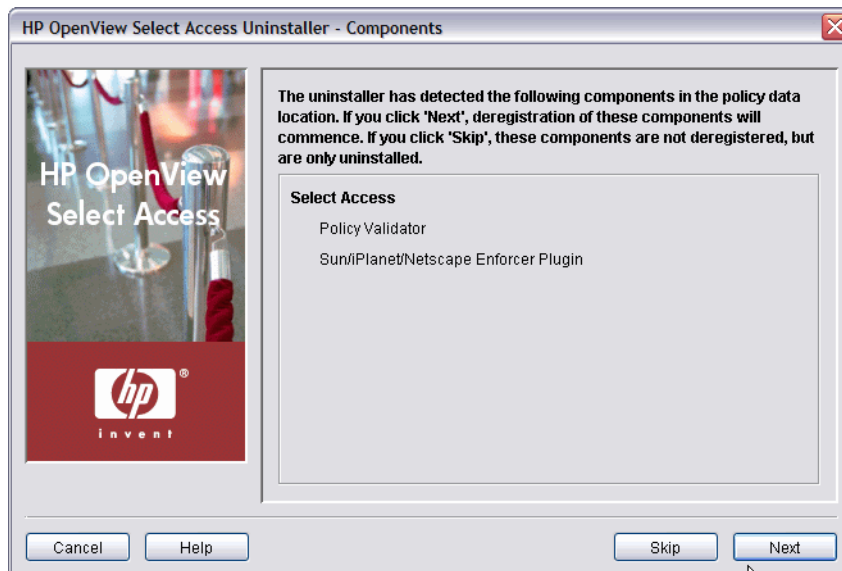
**Figure 35 Uninstall Complete Product Dialog Box**

- 5 Confirm the uninstallation of the components you selected by clicking **OK**. Otherwise, if you need to make changes, click **Cancel** and reselect the new set of components you wish to uninstall.
- 6 The **Deregister Components From Policy Data Location** screen appears.



**Figure 36 Deregister Components From Policy Data Location Screen**

- 7 Do one of the following:
  - Click the **Yes** option if you want to deregister some or all of the Select Access components on this machine. Deregistration removes all records and configuration details from the Policy Store.
  - Click the **No** option if you only want to uninstall the components but not deregister them. The Uninstaller does not remove any record of the component nor any of its configuration details. Skip to [step 12](#).
- 8 Click **Next**. The **Deregistration** screen appears, displaying all detected components in the Policy Store.

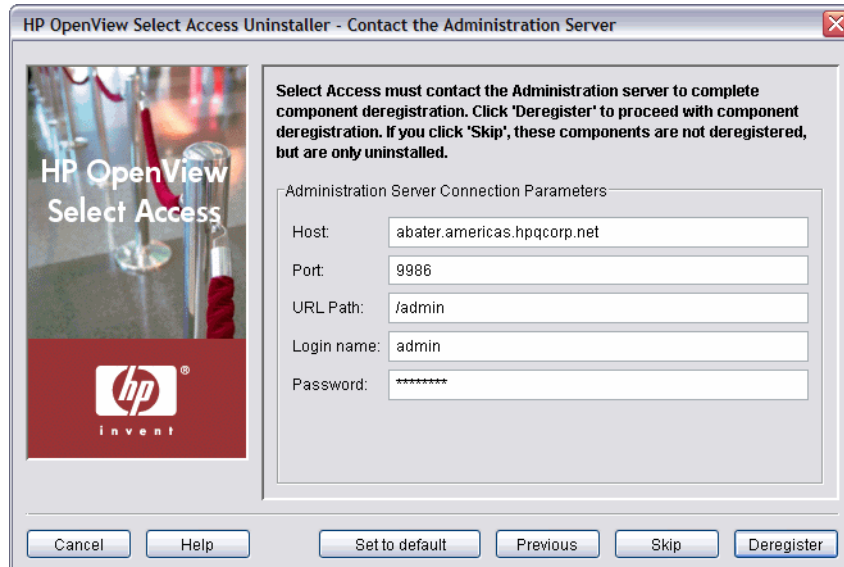


**Figure 37 Deregistration Screen**

- 9 Do one of the following:



- Click **Skip** if you want to keep registration information for components on this host computer in the existing policy data location, but want to continue uninstalling Select Access. The **Choose HP OpenView Select Access Components** screen appears. Go to [step 12](#).
- Click **Next** if you want to deregister components from your system before Select Access gets uninstalled from your system. The **HP OpenView Select Access Uninstaller - Contact the Administration Server** screen appears, as shown in [Figure 38](#).



**Figure 38 Contact the Administration Server Screen**

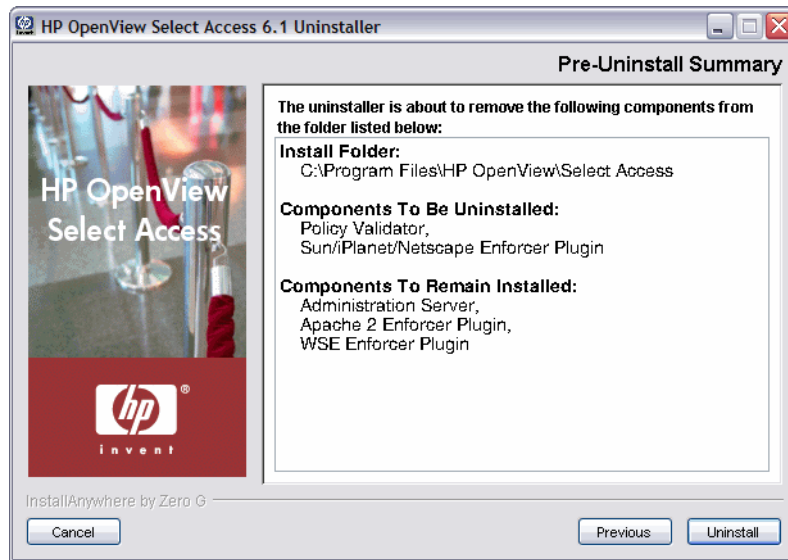
- 10 To connect to the Administration server, define values for the connection parameters in the **Administration Server Connection Parameters** group.
  - **Host:** Required. Enter the name or IP address of the host computer on which the Administration Server is installed.
  - **Port:** Required. Enter the port the administration server is running on. By default, the port is 9986.
  - **Login name:** Required. Enter the Select Access root administrator's login name.
  - **Password:** Required. Enter the Select Access root administrator's password.
- 11 Do one of the following:
  - Click **Skip** if you want to keep registration information for components on this host computer in the existing policy data location, but want to continue uninstalling Select Access.
  - Click the **Deregister** button to proceed with deregistration.

- 12 If any Select Access services are running, the maintenance program displays a warning message. Click **OK** to let the uninstaller automatically stop them for you. Otherwise, stop them manually now.

▶ On Windows, if you have any Enforcer-protected Web servers running, the uninstaller also stops these servers. For the IIS Admin Service, all its dependent services are also stopped.

On Unix, the installer detects whether an Enforcer-protected Web server is running. However, you must manually stop the Web servers. The uninstaller cannot do this automatically on these hosts.

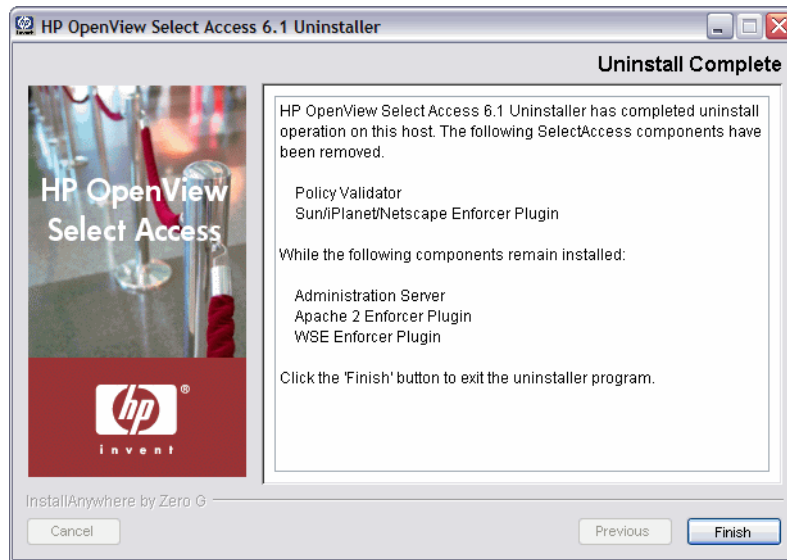
- 13 When the uninstaller is ready, the **Pre-Uninstall Summary** screen appears.



**Figure 39 Pre-Uninstall Summary Screen**

- 14 Click **Uninstall** to proceed with the uninstallation of these Select Access components. Otherwise, if you need to make changes, click **Previous** and reselect the new set of components you wish to uninstall.

At this point, the **Uninstalling Select Access** screen appears, outlining the progress of the uninstallation. When the uninstallation is finished, the **Uninstall Complete** screen appears.



**Figure 40 Uninstall Complete Screen**

15 Click **Finish** to exit the uninstaller. This removes the local files for the uninstalled components, as well as the following:

- Registry entries on Windows hosts.
- `/etc/selectaccess.conf` and the Select Access-installed libraries under `/usr/lib/` on Unix hosts.

- To uninstall other components on different computers, rerun the uninstaller on those machines.
- A number of files are not removed during an uninstallation. The uninstaller only removes those files that were installed by the Select Access installer. Because configuration, log, and initialization files are Select Access administrator-created files that were not installed by the installer, they are left behind.

If you want to remove these files, you must do so manually after the uninstaller has completed the removal of Select Access.



# 11 Starting and Stopping Components

Once you have installed and configured your Select Access components, you can start and stop them as required. Different components support different start and stop methods. This chapter documents those methods.

**Table 1** lists the methods you can try. If the method is supported for a given component, a page number references the section in which the method for that component has been documented.



You do not need to start Enforcer plugins. They are programmed to start when the service they are protecting starts.

**Table 1 Start and Stop Methods**

Components	Start Method Details				Stop Method Details	
	Windows Shortcut	Windows Control Panel	Windows Command Line	Unix Script	Windows Control Panel	Unix Script
<b>Front-end (GUI) components</b>						
Setup Tool	page 202	N/A	N/A	page 202	N/A	N/A
Policy Builder	page 203	N/A	N/A	N/A	N/A	N/A
<b>Back-end components</b>						
Administration server	N/A	page 204	page 204	page 205	page 204	page 205
Policy Validators	N/A	page 205	page 206	page 207	page 205	page 207
Secure Audit server	N/A	page 208	page 208	page 209	page 208	page 209

# Starting the Setup Tool

If you have X-Windows or VNC running on a Unix host computer, the Setup Tool runs in GUI mode. HP recommends that you run the Setup Tool in this mode if it is at all possible. It is preferable to even run the Setup Tool on another host and then copy the corresponding configuration file to the local host that runs the component—except in the case of the Administration server. For this component, HP requires that you run the Setup Tool locally.

## Starting the Setup Tool from the Installer

You can always run the Setup Tool after each Select Access component installation. Depending on the components you have installed, the Setup Tool automatically runs the corresponding setup wizards for those components.

### To run the Setup Tool from the installer

- 1 Answer **Yes** to the question, “Would you like to configure Select Access components now?”
- 2 Click **Next** until you reach the configuration wizard for the component you require. The wizard asks whether or not you want to configure that component now.
  - To configure that component, click **Configure**.
  - To skip a component and configure the next one, click **Next**.

## Starting the Setup Tool Any Time

You are not restricted to only running the Setup Tool from the installer. As your deployment requirements change over time, you will likely need to reconfigure your components to suit your new requirements. Depending on the components you have installed, the Setup Tool automatically detects those already installed on the local host and runs the corresponding setup wizards for those components.



The Setup Tool exits once your configuration session ends. No special command is required to stop or exit the Setup Tool.

### To run the Setup Tool with the Windows desktop icon

- 1 Locate the shortcut for the Setup Tool. By default, you can run the Setup Tool by clicking **Start**→**Programs**→**HP OpenView**→**Select Access**→**Setup Tool**.
- 2 Click **Next** until you reach the configuration wizard for the component you require. The wizard asks whether or not you want to configure that component now.
  - To configure that component, click **Configure**.
  - To skip a component and configure the next one, click **Next**.
  - To return to a previous screen, click **Previous**.

### To run the Setup Tool with the Unix startup script

- 1 cd to the `<install_path>/shared/setuptool` folder.
- 2 Enter the following command:

./setuptool



HP recommends that you set up the corresponding component on Windows or a Unix computer that has X-Windows or VNC.



Select Access requires that you configure the Administration server on the local host computer. Do not run the Setup Tool on another host and copy the configuration file to the host computer, as you might do for other Select Access components. This is because specific settings for the Administration server require that the Setup Tool be run locally so the correct parameters are populated accordingly.

- 3 Click **Next** until you reach the configuration wizard for the component you require. The wizard asks whether or not you want to configure that component now.
  - To configure that component, click **Configure**.
  - To skip a component and configure the next one, click **Next**.
  - To return to a previous screen, click **Previous**.

## Starting the Policy Builder

If you are the super administrator and want to run the Policy Builder in full administration mode, you can run the Policy Builder in two ways:

- Locate the shortcut for the Policy Builder. By default, you can run the Setup Tool by clicking **Start**→**Programs**→**HP OpenView**→**Select Access**→**Policy Builder**.
- Type the appropriate URL and port for this mode in a Web browser's Address field. The syntax used by the Setup Tool to configure the URL and port for full is:

```
https://<admin_server_host>.<domain>:9986/admin
```



You can initialize the Policy Builder in other modes. For details, see [Table 1](#) on page 19 of the *HP OpenView Select Access 6.1 Policy Builder Guide*.

## Starting and Stopping the Administration Server

The Setup Tool's configuration wizard allows you to start the Administration server by checking the **Start now** box on its **Finish** setup screen. If you do not start the Administration server immediately after you configure it, you need to use an alternate method to get it running.

### When to Restart the Administration server

You must stop and restart the Administration server if:

- You change the Administration server's configuration.
- You change the date or time on the computer where the Administration server is running.

## To start and stop the Administration server from the Windows Control Panel

- 1 Click **Start**→**Control Panel**→**Administrative Tools**→**Services**.  
The **Services** window appears.
- 2 Right-click **HP SA Administration Service**.
- 3 From the shortcut menu, choose the appropriate command: **Start**, **Stop**, **Pause**.

## To start the Administration server from the command line

- 1 Change to the `<install_path>\bin` directory.
- 2 At the command prompt, enter the startup command. The startup command uses the following syntax:

```
adminserver [options]
```

Where *[options]* are the command line parameters available to you. [Table 2](#) describes these options.



If you use any of these options, they override any other logging configuration settings.

**Table 2** Command Line Options

Options	Usage
-c	Enables tracing of the cache cleanup code.
-d	Enables internal debugging, which the Administration server outputs to the terminal window. This option overrides all audit settings you configured. Use this option twice to increase the debugging level. <b>Note:</b> The XML queries and responses that get logged can contain sensitive information—particularly when logging the registration process. Take the appropriate precautions so that the Administration server restricts log files to individuals with an appropriate trust hierarchy.
-I	Installs Administration server as a Windows service. <b>Note:</b> This parameter does not tell it to run it.
-L logClient.xml	The XML file that stores logging configuration information. This configuration file uses exactly the same XML format that the log server uses. It overrides any other logging configuration settings stored there.



**Table 2 Command Line Options (cont'd)**

Options	Usage
-N	Returns the Windows service name and exits.
-t	Enables the tracing of requests.
-U	Uninstalls Administration server as a Windows service. <i>Note:</i> To confirm that the uninstaller has removed the service, close and reopen the Control Panel <b>Services</b> dialog box.
-V	Returns the version number of Administration server and exits.

### To start and stop the Administration server with a Unix script

You can use the `adminserver` script to start and stop the Administration server:

- 1 To start the Administration server, enter the following:  
`<install_path>/adminserver start`
- 2 To stop the Administration server, enter the following:  
`<install_path>/adminserver stop`

## Starting and Stopping the Policy Validator

The Setup Tool's configuration wizard allows you to start the Policy Validator by checking the **Start now** box on its **Finish** setup screen. If you do not start the Policy Validator immediately after you configure it, you need to use an alternate method to get it running.

### When to Restart the Policy Validator

You must stop and restart the Policy Validator if:

- The Policy Validator fails. Because the Policy Validator is a service that is not part of a cluster group, it does not automatically restart after a failure.
- You change the Policy Validator's configuration.
- You change the date or time on the computer where the Policy Validator is running.
- You change configuration details for the Secure Audit server.

### To start and stop the Policy Validator from the Control Panel

- 1 Do one of the following:
  - If you are running Windows XP, click **Start**→**Control Panel**→**Administrative Tools**→**Services**.
  - If you are running Windows NT, click **Start**→**Control Panel**→**Services**.


- The **Services** window appears.
- 2 Right-click **HP SA Validator**.
  - 3 From the shortcut menu, choose the appropriate command: **Start, Stop, Pause**.

### To start the Policy Validator from the Windows command line

- 1 Change to the `<install_path>\bin` directory.
- 2 At the command prompt, enter the startup command. The startup command uses the following syntax:

```
validator [options]
```

Where *[options]* are the command line parameters available to you. [Table 3](#) describes these options.

 If you use any of the logging options, they override any other logging configuration settings.

**Table 3 Command Line Options**

Options	Usage
-c	Enables tracing of the cache cleanup code.
-d	Enables internal debugging, which the Policy Validator outputs to the terminal window. This option overrides all audit settings you configured. Use this option twice to increase the debugging level. <b>Note:</b> The XML queries and responses that get logged can contain sensitive information—particularly when logging the registration process. Take the appropriate precautions so that the Policy Validator restricts log files to individuals with an appropriate trust hierarchy.
-I	Installs Policy Validator as a Windows service. <b>Note:</b> This parameter does not tell the installer to start and run the Policy Validator.
-L logClient.xml	The XML file that stores logging configuration information. This configuration file uses exactly the same XML format that the log server uses. It overrides any other logging configuration settings stored there.
-N	Returns the Windows service name and exits.
-n <server_threads>	Specifies the number of server threads

**Table 3 Command Line Options (cont'd)**

Options	Usage
-p <server_port>	Specifies the server port.
-t	Enables the tracing of requests.
-U	Uninstalls Policy Validator as a Windows service. <b>Note:</b> To confirm that the uninstaller has removed the service, close and reopen the <b>Services</b> dialog box.
-V	Returns the version number of Policy Validator and exits.

### To start and stop the Policy Validator with a Unix script

- 1 Change to the <install\_path> directory.
- 2 At the command prompt, enter the startup command. The startup command uses the following syntax:

```
validator [options]
```

Where *[options]* are the command line parameters available to you. [Table 4](#) describes these options.

**Table 4 Startup Script Options**

Options	Usage
debug	Enables and starts internal debugging, which the Policy Validator outputs to the terminal window. This option overrides all audit settings you configured. Use this option twice to increase the debugging level. <b>Note:</b> The XML queries and responses that get logged can contain sensitive information—particularly when logging the registration process. Take the appropriate precautions so that the Policy Validator restricts log files to individuals with an appropriate trust hierarchy.
restart	Acts as a wrapper for stop and start commands so both are performed sequentially.
start	Starts the Policy Validator in the background.
start nohup	Starts the Policy Validator so that it ignores the SIGHUP signal, which allows its processes to continue running.

**Table 4 Startup Script Options (cont'd)**

Options	Usage
stop	Stops the Policy Validator.
status	Returns the current operational status of the Policy Validator.
version	Returns the version number of Policy Validator and exits.

## Starting and Stopping the Secure Audit Server

The Setup Tool's configuration wizard allows you to start the Secure Audit server by checking the **Start now** box on its **Finish** setup screen. If you do not start the Secure Audit server immediately after you configure it, you need to use an alternate method to get it running.

### When to Restart the Secure Audit server

You must stop and restart the Administration server if:

- You change the Secure Audit server's configuration.
- You change the Administration server's configuration.
- You change the date and/or time on the computers where the Secure Audit server clients are running.

### To start and stop the Secure Audit Server from the Windows Control Panel

- 1 Click **Start**→**Control Panel**→**Administrative Tools**→**Services**.  
The **Services** window appears.
- 2 Right-click **HP SA Audit Server**.
- 3 From the shortcut menu, choose the appropriate command: **Start**, **Stop**, **Pause**.

### To start the Secure Audit server from the Windows command line

- 1 Change to the `<install_path>\policy_builder` directory.
- 2 At the command prompt, enter the startup command. The startup command uses the following syntax:

```
auditserver <options>
```

Where `<options>` are the command line parameters available to you. [Table 5](#) describes these options.



If you use any of the logging options, they override any other logging configuration settings.

**Table 5 Command Line Options**

Options	Usage
<code>-f filename.xml</code>	Specifies the path and filename for the Secure Audit server configuration file. This argument is only necessary if the file you did not save the file the default location ( <code>&lt;install_path&gt;\policy_builder</code> ) or uses a filename other than <code>logserver.xml</code> .
<code>-v</code>	Returns the version number of Secure Audit server and exits.

### To start or stop the Secure Audit server with a Unix script

- 1 To start the Secure Audit server, enter the following:  
`<install_path>/auditserver start`
- 2 To stop the Secure Audit server, enter the following:  
`<install_path>/auditserver stop`

# 11 Chapter:Title

# A Policy Validator Stability: Setting File Descriptor Limits

Over the course of several releases, the Policy Validator's stability has been improved by allowing it to handle a greater number of open connections (which includes Enforcer plugin connections). However, each platform has a limit on the number of simultaneous connections it allows.

Table 1 summarizes these differences by platform.

**Table 1 Simultaneous connection limitations by platform**

<b>Platform</b>	<b>Connection limit</b>
HP-UX	60,000
All other platforms	8192

If you need to increase the number of simultaneous connections on your platform, you must do so manually.

## Appendix Overview

This appendix describes how to increase Unix connection limits for the Policy Validator.

Topics in this appendix include:

- [Increasing Unix Connection Limits for the Policy Validator](#) on page 212

## Increasing Unix Connection Limits for the Policy Validator

In order to achieve a high number of connections, you need root privileges to run the script that starts the Policy Validator on Unix platforms with the `ulimit` parameter. Currently, the scripts used to start the Policy Validator on these platforms set the limit of simultaneous connections to 4096.



The initial `nfile` value is calculated by the system. Therefore, you may have a different value than the one specified in this chapter.

### Configuring the Limit on Linux and Solaris

This is performed with the `ulimit -SHn 4096` command. For most deployments of Select Access, this limit is sufficient. However, if your deployment requires a higher or lower number, you can modify the number by editing this command in the startup script.

#### To change the limit in Policy Validator's startup script

- 1 Open the `<install_path>/validator` script.
- 2 Change the value of the `ulimit -SHn 4096` command.
- 3 Save the file and run this script to restart the Policy Validator with this new connection limit.

### Configuring the Limit on HP-UX

The default HP-UX kernel can only open about 920 files at once. This is a system-wide limit, shared between all processes on the system. Since the number of maximum connection can exceed the maximum limit on HP-UX, you need to set HP-UX's descriptor limit to a number that is a much larger value than the maximum number of connections required for the Policy Validator.

#### To find the current number of open files vs. the current limit

You can find the current number of open files, as well as HP-UX's current file descriptor limit, with the System Activity Reporter. Using the command `#sar -v 300` does the following:

- Monitors the system for five minutes.
- Reports the results; look under the `file-sz` column for the values.



## To increase the file descriptor limit

- 1 Run the System Administration Manager (sam).
- 2 Click the **Kernel Configuration** link.
- 3 In the window that appears, click the **Configurable Parameters** link.
- 4 Click on **nfile** and change the value of the kernel's `nfile` parameter to a more suitable number.

For details, see the following documents on HP's Web site:

- <http://forums.itrc.hp.com/cm/QuestionAnswer/1,,0x4f6b402f24d5d61190050090279cd0f9,00.html>
- <http://docs.hp.com/hpux/onlinedocs/939/KCParms/KCparam.Nfile.html>



## B Character Set Listing

This appendix lists the character sets supported by Select Access. [Table 1](#) lists the specific sets you can define when configuring the Enforcer plugin's tuning parameters—either with the Setup Tool or the Policy Builder.

If you select a specific character set, the Enforcer plugin uses it when data is POSTed from a Web browser to a Web server. This ensures that transferred data the Enforcer plugin converts the set you specify to UTF-8 format.



The default character set is iso8859-1.

**Table 1 Supported Character Sets**

37	273	277	278	280
284	285	297	420	424
437	500	646	813	819
850	851	852	855	856
857	860	861	862	863
865	866	868	869	871
874	875	912	913	914
915	916	920	921	922
923	930	933	935	937
939	943	949	950	1089
1112	1122	1123	1383	2022
25546	33722	8859-1	8859-15	8859-2
8859-3	8859-4	8859-5	8859-6	8859-7
8859-8	8859-9	Adobe-Latin1- Encoding	Adobe-Standard- Encoding	ANSI_X3.110- 1983
ANSI_X3.4-1968	ANSI_X3.4-1986	arabic	ascii	ascii-7
asmo-708	Big5	chinese	cns11643	cp037
cp1004	cp1008	cp1025	CP1026	cp1027
cp1046	cp1089	cp1112	cp1114	cp1122
cp1123	cp1125	cp1130	cp1131	cp1200
cp1208	cp1250	cp1251	cp1252	cp1253

**Table 1 Supported Character Sets (cont'd)**

cp1254	cp1255	cp1256	cp1257	cp1258
cp1363	cp1364	cp1383	cp2022	cp273
cp277	cp278	cp280	cp284	cp285
cp28709	cp290	cp297	cp300	cp33722
cp367	cp37	cp420	cp424	cp437
cp500	cp803	cp813	cp819	cp834
cp835	cp850	cp851	cp852	cp855
cp856	cp857	cp858	cp859	cp860
cp861	cp862	cp863	cp864	cp865
cp866	cp867	cp868	cp869	CP870
cp871	cp874	cp875	cp878	cp9030
cp9066	cp912	cp913	cp914	cp915
cp916	CP918	cp920	cp921	cp922
cp923	cp930	cp932	cp933	cp935
cp936	cp937	cp939	cp943	cp947
cp949	cp950	cp-ar	cp-gr	cpibm1047
cpibm1123	cpibm1140	cpibm1141	cpibm1142	cpibm1143
cpibm1144	cpibm1145	cpibm1146	cpibm1147	cpibm1148
cpibm1149	cpibm1153	cpibm1154	cpibm1155	cpibm1156
cpibm1157	cpibm1158	cpibm1160	cpibm1164	cpibm12712
cpibm1371	cpibm1390	cpibm16804	cpibm273	cpibm277
cpibm278	cpibm280	cpibm284	cpibm285	cpibm297
cpibm37	cpibm4899	cpibm4971	cpibm500	cpibm871
cpibm930	cpibm933	cpibm935	cpibm937	cp-is
csAdobeStandard Encoding	csASCII	csBig5	csEUCKR	cseucpkdfmt japanese
csGB2312	csHPRoman8	csIBM037	csIBM1026	csIBM273
csIBM277	csIBM278	csIBM280	csIBM284	csIBM285
csIBM290	csIBM297	csIBM420	csIBM424	csIBM500
csIBM855	csIBM857	csIBM860	csIBM861	csIBM863
csIBM864	csIBM865	csIBM866	csIBM868	csIBM869
csIBM870	csIBM871	csIBM918	csISO2022CN	csISO2022JP
csISO2022JP2	csISO2022KR	csISO58GB231280	csisolatin0	csisolatin1

**Table 1 Supported Character Sets (cont'd)**

csisolatin2	csisolatin3	csisolatin4	csisolatin5	csisolatin9
csisolatin arabic	csisolatin cyrillic	csisolatingreek	csisolatin hebrew	csJISEncoding
cskoi8r	csKSC56011987	csMacintosh	csPC850Multilin gual	csPC851
cspc862latin hebrew	csPC8CodePage 437	csPCp852	csPCp855	csshiftjis
csUCS4	csUnicode	csWindows31J	cyrillic	ebcdic-ar
ebcdic-cp-ar1	ebcdic-cp-ar2	ebcdic-cp-be	ebcdic-cp-ca	ebcdic-cp-ch
EBCDIC-CP-DK	ebcdic-cp-es	ebcdic-cp-fi	ebcdic-cp-fr	ebcdic-cp-gb
ebcdic-cp-he	ebcdic-cp-is	ebcdic-cp-it	ebcdic-cp-nl	EBCDIC-CP-NO
ebcdic-cp-roece	ebcdic-cp-se	ebcdic-cp-us	ebcdic-cp-wt	ebcdic-cp-yu
ebcdic-de	ebcdic-dk	ebcdic-gb	ebcdic-he	ebcdic-is
EBCDIC-JP-kana	ebcdic-sv	ebcdic-xml-us	ecma-114	ecma-118
ECMA-128	elot_928	EUC-CN	eucjis	EUC-JP
EUC-KR	EUC-TW	extended_unix_ code_packed_ format_for_ japanese	gb	GB_2312-80
gb18030	GB2312	gb2312-1980	gbk	greek
greek8	hebrew	hp-roman8	HZ	HZ-GB-2312
IBM00858	IBM01140	IBM01141	IBM01142	IBM01143
IBM037	ibm-037	ibm037-s390	ibm-1004	ibm-1006
ibm-1006_P100- 2000	ibm-1006_STD	ibm-1006_VPUA	ibm-1006_X100- 2000	ibm-1025
ibm-1025_P100- 2000	ibm-1025_STD	IBM1026	ibm-1026	ibm-1026_P100- 2000
ibm-1026_STD	ibm-1047	ibm-1047-s390	ibm-1051	ibm-1089
ibm-1097	ibm-1097_P100- 2000	ibm-1097_STD	ibm-1097_VPUA	ibm-1097_X100- 2000
ibm-1098	ibm-1098_P100- 2000	ibm-1098_VSUB	ibm-1098_VSUB_V PUA	ibm-1098_X100- 2000
ibm-1112	ibm-1112_P100- 2000	ibm-1112_STD	ibm-1122	ibm-1122_P100- 2000
ibm-1122_STD	ibm-1123	ibm-1124	ibm-1124_P100- 2000	ibm-1124_STD

**Table 1 Supported Character Sets (cont'd)**

ibm-1125	ibm-1125_P100-2000	ibm-1125_VSUB	ibm-1129	ibm-1129_P100-2000
ibm-1129_STD	ibm-1130	ibm-1130_P100-2000	ibm-1130_STD	ibm-1131
ibm-1131_P100-2000	ibm-1131_VSUB	ibm-1132	ibm-1132_P100-2000	ibm-1132_STD
ibm-1133	ibm-1133_P100-2000	ibm-1133_STD	ibm-1137	ibm-1137_P100-2000
ibm-1137_STD	ibm-1140	ibm-1140-s390	ibm-1141	ibm-1142
ibm-1142-s390	ibm-1143	ibm-1143-s390	ibm-1144	ibm-1144-s390
ibm-1145	ibm-1145-s390	ibm-1146	ibm-1146-s390	ibm-1147
ibm-1147-s390	ibm-1148	ibm-1148-s390	ibm-1149	ibm-1149-s390
ibm-1153	ibm-1153-s390	ibm-1154	ibm-1155	ibm-1156
ibm-1157	ibm-1158	ibm-1159	ibm-1160	ibm-1161
ibm-1162	ibm-1164	ibm-1200	ibm-1208	ibm-1232
ibm-1250	ibm-1251	ibm-1252	ibm-1253	ibm-1254
ibm-1255	ibm-1256	ibm-1257	ibm-1258	ibm-12712
ibm-12712-s390	ibm-1275	ibm-1276	ibm-1277	ibm-1280
ibm-1281	ibm-1282	ibm-1283	ibm-13488	ibm-1362
ibm-1363	ibm-1363_P110-2000	ibm-1363_P11B-2000	ibm-1363_VASCII_VSUB_VPUA	ibm-1363_VSUB_VPUA
ibm-1364	ibm-1364_P110-2000	ibm-1364_VPUA	ibm-1370	ibm-1371
ibm-1381	ibm-1381_P110-2000	ibm-1381_VSUB_VPUA	ibm-1383	ibm-1386
ibm-1388	ibm-1390	ibm-1392	ibm-1399	ibm-16684
ibm-16804	ibm-16804-s390	ibm-17248	ibm-17584	ibm-21427
ibm-25546	ibm-25546_P100	IBM273	ibm-273	IBM277
ibm-277	IBM278	ibm-278	IBM280	ibm-280
IBM284	ibm-284	IBM285	ibm-285	IBM290
ibm-290	IBM297	ibm-297	ibm-33722	ibm-367
ibm-37	ibm-37-s390	IBM420	ibm-420	IBM424
ibm-424	ibm-437	ibm-4899	ibm-4909	ibm-4971
IBM500	ibm-500	ibm-5050	ibm-5104	ibm-5123
ibm-5210	ibm-5346	ibm-5347	ibm-5348	ibm-5349

**Table 1 Supported Character Sets (cont'd)**

ibm-5350	ibm-5351	ibm-5352	ibm-5353	ibm-5354
ibm-803	ibm-806	ibm-806_P100-2000	ibm-806_VSUB	ibm-808
ibm-813	ibm-819	ibm-834	ibm-835	ibm-848
ibm-8482	ibm-849	IBM850	ibm-850	IBM851
ibm-851	IBM852	ibm-852	IBM855	ibm-855
ibm-856	IBM857	ibm-857	ibm-858	ibm-859
IBM860	ibm-860	IBM861	ibm-861	IBM862
ibm-862	IBM863	ibm-863	IBM864	ibm-864
IBM865	ibm-865	ibm-866	ibm-867	IBM868
ibm-868	IBM869	ibm-869	IBM870	ibm-870
ibm-870_P100-2000	ibm-870_STD	IBM871	ibm-871	ibm-872
ibm-874	ibm-875	ibm-875_P100-2000	ibm-875_STD	ibm-878
ibm-901	ibm-902	ibm-9027	ibm-9030	ibm-9030_P100-2000
ibm-9030_STD	ibm-9044	ibm-9049	ibm-9061	ibm-9066
ibm-9066_P100-2000	ibm-9066_VSUB	ibm-912	ibm-913	ibm-914
ibm-915	ibm-916	IBM918	ibm-918	ibm-918_P100-2000
ibm-918_STD	ibm-918_VPUA	ibm-918_X100-2000	ibm-920	ibm-921
ibm-922	ibm-923	ibm-9238	ibm-930	ibm-932
ibm-932_VASCII_VSUB_VPUA	ibm-932_VSUB_VPUA	ibm-933	ibm-935	ibm-937
ibm-939	ibm-942	ibm-942_P120-2000	ibm-942_P12A-2000	ibm-942_VASCII_VSUB_VPUA
ibm-942_VSUB_VPUA	ibm-943	ibm-943_P130-2000	ibm-943_P14A-2000	ibm-943_VASCII_VSUB_VPUA
ibm-943_VSUB_VPUA	ibm-949	ibm-949_P110-2000	ibm-949_P11A-2000	ibm-949_VASCII_VSUB_VPUA
ibm-949_VSUB_VPUA	ibm-950	ibm-964	ibm-970	ibm-eucCN
ibm-eucJP	ibm-eucKR	ibm-eucTW	ISCII,version=0	ISCII,version=1
ISCII,version=2	ISCII,version=3	ISCII,version=4	ISCII,version=5	ISCII,version=6

**Table 1 Supported Character Sets (cont'd)**

ISCII,version=7	ISCII,version=8	iscii-bng	iscii-dev	iscii-guj
iscii-gur	iscii-knd	iscii-mlm	iscii-ori	iscii-tlg
iscii-tml	ISO_2022	ISO_2022,locale=ja,version=0	ISO_2022,locale=ja,version=1	ISO_2022,locale=ja,version=2
ISO_2022,locale=ja,version=3	ISO_2022,locale=ja,version=4	ISO_2022,locale=ko,version=0	ISO_2022,locale=ko,version=1	ISO_2022,locale=zh,version=0
ISO_2022,locale=zh,version=1	ISO_646.irv:1991	ISO_8859-1:1987	ISO_8859-2:1987	ISO_8859-3:1988
ISO_8859-4:1988	ISO_8859-5:1988	ISO_8859-6:1987	ISO_8859-7:1987	ISO_8859-8:1988
ISO_8859-9:1989	ISO-10646-UCS-2	ISO-10646-UCS-4	ISO-2022	ISO-2022-CN
ISO-2022-CN-EXT	ISO-2022-JP	ISO-2022-JP-1	ISO-2022-JP-2	ISO-2022-KR
iso646-us	iso8859_15_fdis	ISO-8859-1	iso-8859-15	iso-8859-2
iso-8859-3	iso-8859-4	iso-8859-5	iso-8859-6	iso-8859-7
iso-8859-8	iso-8859-9	iso-ir-100	iso-ir-101	iso-ir-109
iso-ir-110	iso-ir-126	iso-ir-127	iso-ir-138	iso-ir-144
iso-ir-148	iso-ir-149	iso-ir-58	iso-ir-6	JIS
JIS_Encoding	JIS7	JIS8	johab	koi8
KOI8-R	korean	KS_C_5601-1987	KS_C_5601-1989	ks_x_1001:1992
ksc	KSC_5601	ksc5601_1987	ksc5601_1992	l1
l2	l3	l4	l5	LATIN_1
latin0	latin1	latin2	latin3	latin4
latin5	latin9	lmbcs	LMBCS-1	LMBCS-11
LMBCS-16	LMBCS-17	LMBCS-18	LMBCS-19	LMBCS-2
LMBCS-3	LMBCS-4	LMBCS-5	LMBCS-6	LMBCS-8
mac	macce	maccy	macgr	macintosh
mactr	ms_kanji	ms874	pck	r8
roman8	SCSU	Shift_JIS	shift_jis78	sjis
sjis78	tis-620	ucs-2	ucs-4	us
US-ASCII	UTF-16	UTF16_BigEndian	UTF16_LittleEndian	UTF16_OppositeEndian
UTF16_PlatformEndian	UTF-16BE	UTF-16LE	UTF-32	UTF32_BigEndian
UTF32_LittleEndian	UTF32_OppositeEndian	UTF32_PlatformEndian	UTF-32BE	UTF-32LE
UTF-7	UTF-8	windows-1250	windows-1251	windows-1252



**Table 1 Supported Character Sets (cont'd)**

windows-1253	windows-1254	windows-1255	windows-1256	windows-1257
windows-1258	windows-31j	windows-874	windows-949	x-big5
X-EUC-JP	x-iscii-as	x-iscii-be	x-iscii-de	x-iscii-gu
x-iscii-ka	x-iscii-ma	x-iscii-or	x-iscii-pa	x-iscii-ta
x-iscii-te	x-sjis	x-utf-16be	x-utf-16le	zh_cn



# C Troubleshooting

This appendix provides solutions to possible problems you may be experiencing.

## Appendix Overview

This appendix includes topics that troubleshoot the following areas of a Select Access-protected system:

- [Installer Errors](#) on page 223
- [Policy Builder Errors](#) on page 224
- [Policy Validator Errors](#) on page 226
- [Web server/Application Server Errors](#) on page 228
- [Denied Access Errors](#) on page 231
- [Directory Server Errors](#) on page 232
- [Certificate Errors](#) on page 233
- [Browser Errors](#) on page 235
- [Logging Errors](#) on page 236
- [Personalization Problems](#) on page 236
- [Password Management Problems](#) on page 237

## Installer Errors

HP has documented the following error:

- [Out of Memory Error when Installing on HP-UX](#) on page 223

### Out of Memory Error when Installing on HP-UX

**Q--->Why am I generating an out of memory error when I try to install Select Access on HP-UX?**

**A--->**When installing Select Access on HP-UX, an out of memory error may sometimes be generated. If this occurs, you will need to adjust the `maxdsiz` parameter in the kernel configuration in the HP-UX System Administration Manager (SAM) to increase the size of the kernel. To adjust this parameter, follow these steps:

- a Start the System Administration Manager.

- b Double-click **Kernel Configuration**.
- c Double click **Configurable Parameters**.
- d Double click on the `maxdsiz` parameter.
- e Change the value of `maxdsiz`. HP recommends a value of 2 063 835 136 to ensure that the installer does not run out of memory.
- f Exit the SAM and create a new kernel, then reboot.

## Policy Builder Errors

HP has documented the following errors:

- [Network Discovery Not Detecting Redirects](#) on page 224
- [Policy Builder and Critical Path Index Node Values](#) on page 224
- [Running Policy Builder in Delegated Administration Mode](#) on page 225
- [Running Two Sessions on the Same Machine](#) on page 225

### Network Discovery Not Detecting Redirects

**Q-->Why is network discovery not detecting redirects?**

**A-->**The HTTP network resource plugin only detects a redirect if the HTTP tag contains a relative URL to the resource:

```
<META HTTP-EQUIV="Refresh" CONTENT="0;URL=allow.html">
```

It does not detect a redirect if the HTTP tag contains a fully qualified URL to the resource:

```
<META HTTP-EQUIV="Refresh" CONTENT="0;URL=http://www.mycompany.com/allow.html">
```

### Policy Builder and Critical Path Index Node Values

**Q-->My Policy Builder keeps generating an error. What is causing this?**

**A-->**A misconfigured CP property can cause the Policy Builder to generate an error because the index node value is too low. If you encounter a lot of unusual Policy Builder errors, try to reconfigure this setting.

To set the correct maximum CP index node value:

- a Open the following file in a text editor of your choice:

```
<CP_install_path>/ds.properties
```

- b Locate the following parameter and ensure that it has the corresponding value:

```
directory.indexNodeMax=524288
```



If this parameter does not exist, you can always include it in your file.

- c Restart your directory server to ensure it uses the new parameter value.

## Running Policy Builder in Delegated Administration Mode

**Q--->I tried to run Policy Builder in delegated administration mode and my browser displays a “404 Not Found” message. What is causing this?**

**A--->**This usually occurs if you:

- Enable delegated administration
- Regenerate the Administration server’s and Policy Validator certificates

This delegated administration Enforcer plugin consequently fails to connect to both components because its certificate hasn’t been updated.

To solve this problem:

- a Disable delegated administration mode.
- b Immediately re-enable delegated administration mode.

## Running Two Sessions on the Same Machine

**Q--->I want to run the Policy Builder in two modes: super administrator and delegated. But an error results as a consequence. Can I work around this problem?**

**A--->**An issue exists which prevents administrators from running Policy Builder in both the full administration mode and delegated administration mode on the same machine. You can work around this issue in one of the following ways:

- By opening each mode in a different browser (that is, one in Netscape, one in Internet Explorer).
- In Internet Explorer, by disabling the **Reuse windows for launching shortcuts** option.

To disable this option:

- a In Internet Explorer, select **Tools**→**Internet Options**.
- b In the **Internet Options** dialog, select the **Advanced** tab.
- c In the **Advanced** tab, under the Browsing category, locate the **Reuse windows for launching shortcuts** option and disable it.

## X11 Display Error with Delegated Mode on Solaris

**Q--->If I reboot my machine without closing down the Policy Builder in delegated mode on Solaris, I get the following error the next time I start the Policy Builder:**

```
Can't connect to X11 window server using ':0.0' as the value of the
DISPLAY variable.
```

**A--->**The workaround for this issue involves exporting the display variable via a shell script before restarting the Administration server:

```
DISPLAY=<host_name>:0.0; export DISPLAY
```

# Policy Validator Errors

HP has documented the following errors:

- [Policy Validator Registers with Wrong Address on Linux](#) on page 226
- [Policy Validator Generates Error When Installing](#) on page 226
- [Policy Validator Failing at Startup](#) on page 227
- [iPlanet 4.0 and Sun ONE 6.0: Cookies Not Refreshed on IE](#) on page 227
- [Policy Validator Looping](#) on page 228
- [Policy Validator Short Circuits](#) on page 228

## Policy Validator Registers with Wrong Address on Linux

**Q--->I just installed the Policy Validator on Linux. However, it incorrectly registered itself as local host only, not it's correct IP address. It seems this is causing the "Clear Validator Cache" issue that keeps appearing in the Policy Builder.**

**A--->**On a RedHat Linux installation, the Select Access installer adds the full hostname of the Policy Validator to the localhost line in the `/etc/hosts` file.

For example, if the full hostname is `dev03.can.hp.com`, the line would appear similar to the one shown below:

```
127.0.0.1          localhost.localdomain localhost dev03.can.hp.com
```

Ensure that you remove your full hostname from the localhost entry so it looks like this:

```
127.0.0.1          localhost.localdomain localhost
```

## Policy Validator Generates Error When Installing

**Q--->I just tried installing the Policy Validator, however it keeps displaying an error message and I cannot complete the installation process. Why is this happening and what can I do?**

**A--->**It is likely that your version of the `mscVRT.dll` is very old (that is, older than 6.00.8397.0). Typically, when this file becomes outdated, it may cause Policy Validator to report an error when you install the it as a service. To get around this issue, HP recommends that you follow the steps outlined below:

- a When the Policy Validator generates an error, click the **OK** button on the popup message to continue with the installation.
- b Click **OK** until the **Configure HP Select Access** screen appears.
- c Check the **No** box to skip the configuration of Policy Validator (as well as other components).
- d At the prompt that asks you to restart your machine, check the **Yes, I want to restart now** box. This causes your machine to reboot when the installation is complete, and consequently replace the offending file with a newer version of it.
- e Open a command prompt and `cd` to the following directory:
- f `<install_path>\bin`

- g Run the following command to install the Policy Validator as a service:  

```
validator -I
```
- h When the installer installs the Policy Validator as a service, click **Start>Programs>HP Select Access v5.0>Setup Tool** to configure the Policy Validator and any other components installed on this host machine.

## Policy Validator Failing at Startup

### Q--->Why is my Validator service failing at startup?

A--->The most likely cause is that the service cannot find the Policy Validator configuration file. Make sure the configuration file is in the following location:

```
<install_path> \bin\validator.xml
```

## Policy Validator and Hostnames

Q--->**I am trying to flush the Policy Validator cache, but my Administration server host cannot contact my Policy Validator even though my Policy Validator is running. Both components are running on different hosts and I have only used my machine name as host.**

A--->Because the Administration server's host is not on the same network as the Policy Validator, contact by machine name fails. If, however, the Policy Validator's hostname returns the fully-qualified domain name, the Administration server would know to look on another network for the Policy Validator host. HP recommends you run the Setup Tool and ensure all hostnames are fully-qualified.

Also, since the certificate generated for the Administration server's connection also uses the hostname returned, you may get a warning regarding the machine name if administrator does not have it configured to return the fully-qualified domain name.

## iPlanet 4.0 and Sun ONE 6.0: Cookies Not Refreshed on IE

Q--->**Why is the Policy Validator not refreshing my cookies?**

A--->It is. However, session cookies for identities that the Policy Validator allows to access network resources are not refreshing properly. This issue is limited to iPlanet and Sun ONE Web servers using Microsoft Internet Explorer. The Internet Explorer only refreshes cookie data from iPlanet and Sun ONE servers when:

- You have recently modified the page.
- A page is not in its cache.

Therefore, the cookie is timing out despite the fact that Policy Validator has refreshed it. To solve this problem, disallow caching of any content:

- a Point to `http://<hostname>:<port>/` to launch the iPlanet or Sun ONE Web server administration tool and enter your login information. The **Manage Servers** page appears.
- b From the drop listbox, select a server and click the **Manage** button. The **Server on/off** page appears.
- c Click the **Content Mgmt** tab. The **Primary Document Directory** page appears.

- d Click the **Cache Control Directives** link in the left navigation bar. The **Cache Control Directives** page appears.
- e Under **Cache Control Response Directives**, enable **No Cache** and click **OK**. The **Save and Apply Changes** page appears.
- f Click the **Save and Apply** button.

## Policy Validator Looping

**Q--->Why does the Policy Validator sometimes loop when it processes certificates—especially now that I've enabled OCSP?**

**A--->**Certificate evaluation, which can involve LDAP lookups and OCSP, can take some time, so the Enforcer plugin is timing out before the Policy Validator evaluates the certificate. To prevent the Policy Validator from looping when validating certificates, increase your Enforcer plugin **Wait for Validator Reply** parameter (in the **Tuning** setup screen) from its default of 15 seconds. For details on configuring the Enforcer plugins, see [Chapter 8, Configuring the Enforcer Plugins](#), in the *HP OpenView Select Access 6.1 Installation Guide*.

## Policy Validator Short Circuits

**Q--->The Policy Validator displays a message stating that it is “short circuiting” when it does certificate authentication for transient identities.**

**A--->**Certificate chain verification is a very expensive operation in term of the network traffic it creates, which involves the following operations: LDAP lookups, RSA signature verifications, and possible CRL and OCSP lookups. As a result, it is timing-out before verification is complete. To prevent this from happening, decrease your **Certificate Verify Interval** value by reconfiguring your Administration server.

## Policy Validator Missing SSL session Information

**Q--->I've noticed that the Policy Validator is dropping session information from queries originating from Apache plugins under SSL mode. How can I correct this?**

**A--->**It is important to get the complete SSL session back into your queries, because without it, any encryption decision points in your existing rules fail. To correct this problem you need to open your `httpd.conf` file on your Web server and add the following line to the enforcer plugin section:

```
SSLOptions +ExportCertData +CompatEnvVars +StdEnvVars
```

## Web server/Application Server Errors

HP has documented the following errors:

- [HTTP Basic Authentication Problematic](#) on page 229
- [Restricted IBM HTTP Server Resources](#) on page 229
- [Virtual Web Server Support Problems with IIS](#) on page 229



- [Caching Problems with IIS](#) on page 230
- [Integrated Windows authentication issues on IIS](#) on page 230

## HTTP Basic Authentication Problematic

**Q--->I have created an HTML form with at least two text boxes named “user” and “password”. I am using HTML basic authentication, and have applied a deny policy to Unknown Identities and an allow policy to Known Identities. However, when an identity enters their credentials with the Password server I configured, they are denied access. The Policy Validator then prompts the end-user for credentials again using HTTP basic authentication. Why is this happening?**

**A--->**It appears that the Policy Validator is authenticating with the credential data from the form instead of the credential data from the HTTP basic authentication prompt. If you were to log the Policy Validator’s output, you would notice two user and password XML elements: one from the form and one from the HTTP basic authentication. To get form-based logins to work on a Select Access-protected system, ensure that you both check the **Enable Web Session Cookies** box and uncheck the **Login using Forms** box when setting up the Enforcer plugin’s **Tuning Parameters**.

## Restricted IBM HTTP Server Resources

**Q--->I have restricted access to confidential resources on the IBM HTTP server that was bundled with WebSphere. However, it appears that irrespective of the policy I set, identities can still access these resources via Telnet. How do I prevent this from happening?**

**A--->**Due to the way in which IBM has implemented security on their IBM HTTP server, identities are able to access restricted resources via Telnet. HP has reported this issue with IBM. In the meantime, HP recommends that you check the **Fast cache response** configuration parameter. If you enable this option, it negatively impacts Select Access’s access control mechanisms. Therefore, you must disable this feature. You can disable fast caching of response by either:

- Running the IBM HTTP Server Administration tool and ensuring that **Enable fast response caching** is set to **No**
- Removing the `AfpaEnable` directive from the server's `httpd.conf` file

## Virtual Web Server Support Problems with IIS

**Q--->I am having trouble configuring virtual Web server support on IIS. I am running on Windows 2000 with Service Pack 2.**

**A--->**Microsoft states this is a known issue with DNS on Windows 2000 Service Pack 2. When faced with this problem, you have three options:

- Add `hostname` to IP address resolution to the `HOSTS` system file. The Web server must have IP addresses assigned to each virtual Web server.
- Contact Microsoft Product Support Services for a hotfix to this issue.
- Install Service Pack 3.

## Caching Problems with IIS

### Q--->Why are my PDFs not downloading with IIS?

A--->When you enable caching with the IIS Enforcer plugin, PDFs do not get downloaded over HTTPS as a result of a known Internet Explorer bug. HP enables caching in all Enforcer plugins by default. To get the desired browser behavior with this bug, disable caching on your IIS Enforcer plugin. You can do this by:

- a Doing one of the following:
  - Running the Setup Tool
  - Displaying the Component Configuration tool from the Policy Builder
- b Modifying the Enforcer plugin's existing **Tuning Parameters** by checking the **Do not cache Web pages** box. For details on the Setup Tool, see [Chapter 8, Configuring the Enforcer Plugins](#) in the *HP OpenView Select Access 6.1 Installation Guide*. For details on the Component Configuration tool, see [Chapter 16, Modifying Components' Central Configuration Parameters](#) in the *HP OpenView Select Access 6.1 Policy Builder Guide*.

## Integrated Windows authentication issues on IIS

### Q--->I am having problems with my Integrated Windows authentication service which runs on an IIS Web server over Windows 2000. How can I authenticate using NTLM?

A--->You can authenticate using NTLM by doing the following:

- a Open an MS-DOS command prompt session.
- b Navigate to the `Inetpub\AdminScripts` folder.
- c At the command prompt, run the following utility with the following command:
- d `adsutil get w3svc/NTAuthenticationProviders`
- e This command tests your Integrated Windows authentication system. If your deployment is problematic, you receive an error message.
- f If you receive an error message, enter the following command from the same location:
- g `cscript adsutil.vbs get w3svc/NTAuthenticationProviders`
- h To set the value to use NTLM authentication, enter one of the following commands:  
`adsutil set w3svc/NTAuthenticationProviders "NTLM"`  
-OR-  
`cscript adsutil.vbs set w3svc/NTAuthenticationProviders "NTLM"`



For more details, visit the following Microsoft support page:

**(<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q215383>)**

## Denied Access Errors

HP has documented the following errors:

- [Denied Access to Service](#) on page 231
- [Denied Access on Default Page](#) on page 231
- [Browser Gets Deny yet Policy Validator Returns Allow](#) on page 231

### Denied Access to Service

**Q--->I manually added a new service to the Resources Tree, but I am always denied access to the service regardless of the rule I have set in Policy Builder.**

**A--->**Make sure the name you entered for the service is the same as the name passed to Policy Validator. All Enforcer plugins send a name to identify the network service with every XML query they send to Policy Validator. In order for rule evaluations to work correctly, the Policy Matrix must have a matching service name. When they do not match, you typically get a DENY from Policy Validator and it logs a message such as:

```
No LDAP record for service
http://www.mycompany.com:8000 (query '(&
(objectclass=nxResourceEntry) (nxURL=http://
demo.mycompany.com:8000))')
```

To fix this:

- a In the Policy Matrix, right-click the network service and select **Properties**. The **Editing Service Properties** dialog box appears.
- b Enter a new **Name** that matches the service name that the Enforcer plugin is sending.

### Denied Access on Default Page

**Q--->I have allowed access at the service level for my Web server, but the Policy Validator denies my identities are access when they go to the default page.**

**A--->**You have manually added the default page as a resource under the Web server and created a security policy for the resource. Delete the resource from the Resources Tree; it is not needed because the policies created for the service apply to the Web server's default page.

### Browser Gets Deny yet Policy Validator Returns Allow

**Q--->Why is my Web browser displaying a deny error message, even though Policy Validator is returning an allow decision?**

**A--->**Web servers can have their own mechanism for checking access entitlements. So, while you may have configured the Policy Builder with an allow for this resource, you may have set up your server's mechanism with a deny. If you are using server-specific access controls, make sure they are consistent with your Policy Builder policies.

# Directory Server Errors

HP has documented the following errors:

- [Active Directory 2003 and Profile Password Setup Problems](#) on page 232
- [iPlanet and iPlanet Unicode Problems](#) on page 232
- [Critical Path and Siemens Over SSL Problems](#) on page 233
- [Policy Builder and Critical Path Index Node Values](#) on page 224
- [Browsing for OCSP certificates on Critical Path](#) on page 233

## Active Directory 2003 and Profile Password Setup Problems

**Q--->I've tried creating a profile with the Policy Builder, but when I try to create a password, an error message tells me that password I set does not meet the password policy for ADS.**

**A--->**You must always try to meet the password policy of your directory server. ADS requires that passwords be equal to or greater than seven characters. However, you can work around this limitation by disabling ADS' policy by modifying the Password properties and Lockout properties for both the Default Domain Security Policy and Default Domain Controller Security Policy on the server as follows:

### Password Policy Properties

- reverse encryption: disabled
- complexity rules: disabled
- minimum length: 0
- minimum age: 0
- maximum age: 0
- password history: 0

### Lockout Policy Properties

- reset: not defined
- lockout threshold: 0

**A--->** lockout duration: not defined

## iPlanet and iPlanet Unicode Problems

**Q--->How do I fix Unicode character set errors on iPlanet?**

**A--->**Locate the plugin that enforces 7-bit (ASCII) character storage. When you disable this plugin, you will be able to store your Unicode characters correctly.

## Critical Path and Siemens Over SSL Problems

**Q--->I am having trouble connecting to Critical Path or Siemens over SSL. Why is this happening?**

**A--->**The directory server certificate is probably not compliant with Transport Layer Security (TLS) version 1.0. Both Critical Path and Siemens DirX do not verify the server certificate, which means the end user has to make sure that the server certificate is in TLS compliance. When a key usage extension is present, you must set:

- the `digitalSignature` bit to enable signing
- the `keyEncipherment` bit to enable encryption.
- the `keyAgreement` bit if you are using a Diffie-Hellman certificate.

## Certificate Errors

HP has documented the following errors:

- [Browsing for OCSP certificates on Critical Path](#) on page 233
- [Generic Problems](#) on page 234
- [Microsoft Certificates and Failed Signing](#) on page 234
- [Problems Specific to IIS](#) on page 235
- [Problems Specific to Apache](#) on page 235

## Browsing for OCSP certificates on Critical Path

**Q--->Why does the Policy Validator have problems locating the OCSP certificate authentication service's certificate I uploaded?**

**A--->**This problem occurs because you have not configured the `usercertificate` attribute to specify what type of search the Policy Validator can make on its values. You can configure the type of search the Policy Validator can make to find the certificate entry with a Critical Path's feature called "matching rules":

- a In Critical Path's InJoin Directory Server Configurer, display the **Attributes Registry** page for the `usercertificate` attribute.
- b Configure the **Matching Rules** properties for this attribute. Do this by checking the following boxes: **Presence** under the `inv` column and **PresenceMatch** under the `match` column.



For explicit details on the **Matching Rules** table, click the **Help** button on this page.

- c Click the **Change Attributes** button to record these changes.
- d Restart Critical Path to use these new settings.

## Generic Problems

### Q--->Why am I having problems using certificates with Select Access?

A--->For the certificate plugin to locate an identity:

- a The Subject DN of the certificate must meet one of the following conditions:
  - Exactly match the DN in the identity's profile.
  - Contain a `uid` attribute that exactly matches the `uid` attribute in the identity's profile.
  - Contain a `cn` attribute that exactly matches the `cn` attribute in the identity's profile.
- b The identity's profile can have a `userCertificate;binary` attribute that contains the certificate used to authenticate components.
- c The `userCertificate` and `caCertificate` attributes in LDAP must also have the `;binary` tag attached. For details, see Section 6.5 of the RFC 2252 document, "Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions" (available at <http://www.ietf.org/rfc/rfc2252.txt>).

## Microsoft Certificates and Failed Signing

### Q--->When I use a Microsoft certificate, data signing fails. Why does this happen?

A--->If you are using a Microsoft certificate with data signing, the Policy Validator may generate a message stating that XML signing has failed and data is or is not validated. There are two things that might cause this error:

- *Attributes include an underscore ( \_ ) in the attribute value.* This character adds extra characters when you view the certificate's attributes on the directory server. For example, if the certificate's CN has a value of `xml_cert`, it would appear as follows when viewed with an LDAP browser:

```
#1E1E0074006500730074005F0075006E00640065007200730063006F0072006
```

As a result, when the Policy Validator tries to verify signed data the attributes do not match. To avoid this problem, prepend `\x00` to each character in the attribute value for the **Data Signer CN** field of the Administration Server's **Data Signing** setup screen (which is only displayed when you choose a **Custom** setup). For example, if the certificate's CN has a value of `xml_cert`, you would set `ldap_signed_user` to:

```
ldap_signed_user cn=\x00x\x00m\x00l\x00_\x00c\x00e\x00r\x00t,
ou=support,o=mycompany.com
```

- *Certificates may include an email address.* The way in which Microsoft delineates the email address differs from the entry for the certificate in the directory server. For example, if you view the certificate with an LDAP browser, the directory server may delineate an email address as:

```
e=help@mycompany.com
```

But if you view the certificate via an LDAP browser, the certificate may instead delineate this same email address as:

```
emailaddress=help@mycompany.com
```

Again, when the Policy Validator tries to verify signed data the certificate subject does not match. To avoid this problem, do the following:

- a Determine what the Policy Validator is expecting. Configure your audit settings. To capture information regarding Microsoft certificates and failed data signing, set Operation to Debug level. Policy Validator can output the messages to any destination you choose.
- b Replicate the email address attribute definition in for the **Data Signer CN** field of the Administration Server's **Data Signing** setup screen (which is only displayed when you choose a **Custom** setup). For example:

```
ldap_signed_user cn=cert1, ou=support,  
o=mycompany.com, email=help@mycompany.com
```

## Problems Specific to IIS

**Q--->Why am I having certificate authentication problems with IIS?**

**A--->**Check the following:

- Make sure you are using IIS 4.0 SP4 or later.
- If you are using Internet Explorer 5 or later, enable the use of PCT 1.0 in IIS:
  - a Choose **Tools** → **Internet Options**.
  - b On the **Advanced** tab, in the **Security** section, select the **Use PCT 1.0** checkbox.



You can also check the Microsoft knowledge base for known issues with IIS certificate authentication.

## Problems Specific to Apache

**Q--->Why does mod\_enforcer get a malformed certificate when it retrieves SSL session information from the Policy Validator's cache?**

**A--->**This occurs because the Apache 2 Enforcer plugin appears not to correctly save the client certificate. As a result, when it passes this malformed to the certificate, Policy Validator rejects it.

To fix this problem consider either of the following alternatives:

- Turn off SSL session caching on Apache. You can do this by commenting out all `SSLSessionCache` entries.
- Build Apache with the MM shared memory library and use one of the following shared memory caches: `shmmt:` or `shmcb: .`

## Browser Errors

HP has documented the following error:

- [SSO Failing on Internet Explorer](#) on page 236

## SSO Failing on Internet Explorer

**Q--->Why does Single sign-on (SSO) fail on IE sometimes?**

**A--->**SSO always fails on IE when identities link from a protected (HTTPS) to a non-protected (HTTP) site. This failure happens because the HTTP Referer header is not being sent when connecting to or from a non-protected page. Microsoft does this to prevent secure data from being accidentally transferred to unsecured sites. Depending on how you configure their Web servers, you might store secure information in the URL during a GET request to CGI or ISAPI applications. Microsoft circumvents this practice by restricting certain SSO connections.

## Logging Errors

HP has documented the following error:

- Database and email outputs creates XML error on page 236

### Database and email outputs creates XML error

**Q--->Why has one of my Policy Validators or Enforcer plugins generated the following message: Error in Logger XML configuration: No factory found for output element “database/email”.**

**A--->**The Policy Validator and Enforcer plugin cannot log messages to database or email directly for an individual instance of either of these components. Because you have configured an individual instance to one of these outputs, the Policy Validator and Enforcer plugin has generated the message described above. You can only select database or email as the **Audit Trail** when they are:

- Part of Select Access’ common audit settings that you configure with the Administration server’s setup.
- Part of the default group settings for all Policy Validators or all Enforcer plugins.
- The component is a client of the Secure Audit server that outputs to this destination.

## Personalization Problems

HP has documented the following error:

- Empty Dynamic Group Attribute Values on page 236

### Empty Dynamic Group Attribute Values

**Q--->I have set up personalization so that it returns dynamic group and group information and some attributes in the dynamic groups. Why do I get**



**“attribute=”, with nothing appearing after the equals symbol for those attributes?**

A-->The attribute is not an attribute of the dynamic group or group. As a result, the value appears empty. For details on which attributes you can use, see [About Directory Attributes](#) on page 24 of the *HP OpenView Select Access 6.1 Concepts Guide*.

## Password Management Problems

HP has documented the following error:

- [Active Directory 2003 and Profile Password Setup Problems](#) on page 232



# glossary

## A

### **Access Control**

The authorization policies and conditions that regulate identity access to resources with a goal towards preventing unauthorized use or use in an unauthorized manner.

### **Administration server**

The server that administers Select Access' configuration parameters, policy data, and certificates. This component writes all relevant details to the Policy Store.

### **Administrator**

An identity with delegated entitlements. Only delegated entitlements are available when the individual runs the Policy Builder in delegated mode or Web administration. See also [Delegation](#) and [System Administrator](#).

### **Alias**

A pointer or shortcut to the actual identity profile (also known as directory entry), which is typically shown under any group to which the identity belongs. See also [Identity Profile](#).

### **Approval Process**

The process of approving the grant, modification, or revocation of entitlements for an identity. Often organizations employ manual approval processes. A compelling benefit of Select Access is the automation of these processes through its workflow feature. See also [Approver](#) and [Workflow](#).

### **Approver**

An administrator who has been given workflow approval rights via the Workflow function entitlement.

### **Attribute**

One or more characteristics that are part of an identity profile. Attributes are name/value pairs with a type that is assigned a value. For example, an attribute called "Department" may be assigned the values of, "IT", "Sales", or "Support". These attributes are interpreted and assigned appropriately to profiles in different applications (LDAP-compliant directories, databases, SAPs, and so on) based on the mapping rules defined for that application.

### **Audit Policy**

A policy that defines which events are logged for a given Select Access component. Audit policies monitor stability, ensure data integrity, and maintain corporate security. See also [Audit Trail](#).

## **Audit Trail**

A log destination to which time-based messages of a given severity are recorded. Select Access allows you to output messages to destinations like the Secure Audit servers, databases, files, and so on. See also [Audit Policy](#).

## **Authentication**

The act of verifying the credentials of an identity and matching them with an identity profile. The evaluation of credentials ensures that the identity is truly who or what they claim to be. See also [Authorization](#).

**Authentication Service** One of the supported methods used by the Select Access system to verify login credentials claimed by or for an identity. Authentication services can use different mechanisms, which can include tokens, certificates, secrets, or simply IDs/names and password combinations.

## **Authorization**

The process of defining and enforcing the entitlements of an identity. Authentication is a prerequisite for authorization. See [Access Control](#) and [Authentication](#).

# **B**

## **Branch (true/false)**

The logical connections among two or more nodes in a conditional access rule:

- **If the request does match the criteria:** It is considered *true* and follows the true branch to the next node in the rule.
- **If the request does *not* match the criteria:** It is considered *false* and follows the false branch to the next node in the rule.

See also [Node](#) and [Rule](#).

# **C**

## **Caching**

The ability to retrieve recently accessed data in order to speed up repeated access to the same data.

## **Challenge-Response**

A common authentication technique that prompts an identity (the challenge) to provide some data only known by the identity (the response). An example of challenge-response authentication is a smart card.

## **Conditional Access**

See [Access Control](#), [Policy](#) and [Rule](#).

# **D**

## **Data Signing**

See [Signature](#).

## **Data Location**

A directory server that acts as a repository for identity profiles. See also [Identity Profile](#) and [Policy Store](#).

## Delegation

The act of assigning administration or even registration entitlements to another identity. For example, by delegating registration, you are entitled to perform registration on behalf of another identity.

## Dynamic Group

Sometimes referred to as a Role in LDAP directories. A named collection of identities and possibly other groups whose membership is based on attribute values in the identity profile. Unlike Groups which are static, Dynamic Groups do not allow you to directly add additional members. Assignment to a dynamic group is automatic and shifts over time. For example, you can create a Dynamic Group called “Big Spenders”. To become and remain a member of this dynamic group, an attribute called “Monthly Purchases” must be higher than \$500.00. See also [Group](#).

## E

### Entitlement

Administrative functions of Select Access that are used by the system to:

- Control access.
- Manage identities and resources.
- Manage internal components.

For example, in Select Access, a typical administrative entitlement is the delegation of component configuration responsibilities to other/additional administrators on your team.

### Entity

An individual, a corporate body, a federation, an application, or a service that can be described conceptually by a set of attributes. For example, you can have an Employee entity with attributes values such as Last Name, First Name, Address, and so on. You can also have a Server entity with attribute values such as Domain, Type, Organization, and so on. See also [Identity Profile](#).

## F

### Failover

The transfer of operation from a failed component (for example, directory, server, system) to a similar, redundant component. In Select Access specifically, redundant Policy Validators and directory servers ensure that data flow remains uninterrupted and your access control system operable.

**Federation** The combination of business and technology practices to enable identities to span systems, networks and domains in a secure and trustworthy fashion. This is analogous to how passports are used to assert our identity as we travel between countries.

## G

### Group

A named collection of identities and possibly other groups. You can directly make an identity a member of a group or indirectly through membership in a sub-group. A group is often composed to apply similar access control rights. For example, you can create a group for all your customers, another group for your suppliers, and another group for your employees. When you create an access rule for a group, all group members inherit the access policy, unless you override it. See also [Dynamic Group](#).

**H** There are no terms that begin with this letter.

**I** **Identity location**

See [Data Location](#).

**Identity Management (IdM)**

The process of identifying entities in a system and controlling their access to resources within that system. In Select Access, access is typically controlled by associating rights and restrictions with the established identity profile. You can use additional software (for example, Select Identity) to automate many administrative tasks associated with the management of identity profiles (for example, creating, deleting, modifying, and so on). See also [Entity](#) and [Identity Profile](#).

**Identity Profile**

A database record or directory entry that includes a set of authentication credentials, profile attributes, and entitlements for a single entity. Identity is often used as a synonym for “user”, although identity is not restricted to an individual. See also [Entity](#).

**Inheritance**

Occurs when the authorization policies of a defined group or folder are applied to each constituent (identities or resources) within that group.

**J** There are no terms that begin with this letter.

**K** There are no terms that begin with this letter.

**L** **LDAP (Lightweight Directory Access Protocol)**

A set of open protocols for accessing information directories. LDAP can make the physical network topology and protocols transparent so that a network identity can access any resource without knowing where or how it is physically connected.

**M** There are no terms that begin with this letter.

**N** **Network Resource**

See [Resource](#).

**Network Service**

See [Resource Service](#).

**Node**

In a rule decision tree, a point where two or more true/false branches meet. A node can be a decision point (where outcomes are evaluated based on criteria configured by an administrator) or a terminal point (where final outcomes are triggered).

## **Nonce**

An opaque piece of data created by the Policy Validator and placed in a cookie. In Select Access, a nonce is an important component of an authentication and authorization protocol.

## **O**

There are no terms that begin with this letter.

## **P**

### **Password Management**

The process of securely setting, maintaining, and synchronizing passwords in an identity profile. See also [Identity Profile](#), [Password Synchronization: Forward/Reverse](#), [Password Reconciliation](#) and [Password Reset](#).

### **Password Synchronization: Forward/Reverse**

The business policies/processes, software, and network infrastructure that enable identities to maintain a single Password value that is accepted across multiple Login Accounts, domains, applications, and so on. Password synchronization can be forward sync mechanisms (where the password in the identity profile is shared with multiple systems) or reverse sync mechanisms (where one of the multiple systems writes the password to the identity profile). See also [Identity Profile](#), [Password Management](#), [Password Reconciliation](#) and [Password Reset](#).

### **Password Reconciliation**

The process of adopting passwords in the identity profile when:

- The identity has a recognized profile.
- An aliasing technology is used.

See also [Identity Profile](#), [Password Management](#), [Password Synchronization: Forward/Reverse](#) and [Password Reset](#).

### **Password Reset**

The business policies, software, and network infrastructure that determines when and how an Password values in an identity profile can be securely changed if they are forgotten. See also [Identity Profile](#), [Password Management](#), [Password Reconciliation](#) and [Password Synchronization: Forward/Reverse](#).

### **Policy**

A set of defined practices or a formal statement of operational rules, set by an organization to assist in managing some aspect of its business. For example, in Select Access, an access control policy determines identity-based level of access (allow/deny/conditional) for specific internal and external resources.

### **Policy Query**

A request for a resource made by an Enforcer plugin to the Policy Validator. The Policy Validator evaluates the identity's authorization policy to determine whether an identity is allowed access to the network resource. The access decision is sent to the Enforcer plugin. See also [Policy Reply](#).

### **Policy Reply**

A decision to a resource request made by the Policy Validator via an Enforcer plugin. Based on the identity's authorization policy, the Policy Validator replies with an allow, deny or conditional decision. See also [Policy Query](#).

### **Policy Signing**

See [Data Signing](#).

### **Policy Store**

A directory server that acts as a repository for policy data and configuration information. See also [Data Location](#).

### **Profile**

See [Identity Profile](#).

### **Profile Self-Management**

Also known as Self-Service. The business policies, software, and network infrastructure that determines when and how identities can securely update attribute values in their profile. Select Access supports self-management with conditional rules that include a Profile Self-Management terminal point. See also [Password Management](#).

### **Provisioning**

The automation of all business processes and tools to centrally manage the life cycle of an identity. For example, the creation and modification of profile attributes, the propagation of data to affiliated systems, the delegation of identity authentication and authorization, the decommissioning the profile, and so on.

## **Q**

### **Query**

See [Policy Query](#).

## **R**

### **Referral**

A response that redirects the Select Access component to the directory server that holds the data it requires.

### **Registration**

The business policies, software, and network infrastructure that allows an unknown identity to become a known and authenticatable identity by formally recording attributes and values in a central repository for future identity verification. Registration is typically performed by an end-user that is requesting resource access. However, registration can also be delegated. See also [Delegation](#).

### **Resource**

A discrete piece of information, such as a file or URL, that you can access on a network. A resource can contain other resources. On the Resources tree, a resource must be stored below a service. The Resource plug-in is used to gather resource URLs and add them to the Resources tree. See also [Resource Service](#).



## **Resource Service**

A computer or device on a network that manages network resources. A service provides access to a resource via one or more protocols, for example, HTTP or FTP. Examples of services include file servers, Web servers, an NT domains, Certificate servers. A service can also provide access to other services, and can be represented in the Resources Tree by a host name. For example, a Web server may be shown in the tree according to the server's host name, for example, www.acme.com. See also [Resource](#).

## **Rule**

A programmatic control over system behavior. Rules are typically used for intelligent assignment of entitlements or for the capture of granular access criteria and/or conditions.

## **S**

### **Self-Registration**

See [Registration](#).

### **Self-Service**

See [Profile Self-Management](#).

### **Signature**

An encrypted digital text block that authenticates the identity of the sender of a message, or of the signer of a document. By signing data with a digital signature, you can also ensure that the original data is untampered with.

### **System Administrator**

Also known as the super administrator. A system administrator is the root administrator of the Policy Builder, and has all features and functions activated. The system administrator can also use Web administration if she chooses. See also [Administrator](#).

## **T**

There are no terms that begin with this letter.

## **U**

There are no terms that begin with this letter.

## **V**

There are no terms that begin with this letter.

## **W**

### **Workflow**

A business process that helps to ensure data integrity by tracking administrative events and automatically routing the outcome of these events to an approver. Only after approval does the change become implemented. Workflow is considered a multi-administrator, multi-stage process, because two or more administrators collectively share, manage, and operate on a shared repository of information.

## **X**

There are no terms that begin with this letter.

## **Z**

There are no terms that begin with this letter.



# Index

## Symbols

- .NET framework
  - Enforcer plugin for, 10, 131
  - Enforcer plugin for. *See also* Enforcer plugins
  - platform support for, 10, 12

## A

### Addresses

- directory server, 69, 82
- entering in browser, 203
- entity, attribute for, 241
- for Administration server, 74, 75
- for directory server, 75
- for IIS Web servers, 158
- for Policy Validator, 118, 119, 122, 123, 131
- for Secure Audit server, 97
- NAT, configuring list of, 149
- pass-through domains, 145
- to Administration server, 121, 136, 165, 197
- virtual, 145

### Administration modes

- configuring, 75
- types. *See* Modes

### Administration server

- address for, 74, 75, 119, 121, 136, 165, 197
- auditing settings, 83
- certificates, 75
- configuring, 63, 64, 65, 66, 69, 95, 117, 118, 130
- data signing, 79
- multiple installations of, scenarios for, 86, 169
- platform availability, 10
- Policy store configuration, 69, 121, 165
- recovering, 86, 169
- setup, custom, 64
- setup, typical, 64

### Alerts

- configuring, 108, 109
- deployment example with, 16

### Apache Web servers

- configuring, 157
- Enforcer plugin for, 9, 131
- Enforcer plugin for. *See also* Enforcer plugins
- platform support for, 10, 12
- restarting, after configuring, 157

Application servers, supported, 12

### Attributes

- agreeing on, 20
- troubleshooting, 236

### Audit

- common settings, 57
- entry, 84, 99, 124, 147
- overview, 95
- policy, overall setup of, 101
- policy, procedure for, 111
- settings, Administration server, 83
- settings, Enforcer plugin, 124, 146
- settings, global/default, 94
- settings, Policy Validator, 124
- settings, Secure Audit server, 95, 98, 101
- stream, signing, 99
- trail, 83, 124, 147
- trail, specifying, 101
- troubleshooting, 236

### Axis application server

- bypassing Enforcer plugin security, 144
- configuring with Enforcer, 155, 159
- Enforcer plugin for, 131
- Enforcer plugin for. *See Also* Enforcer plugins
- ignored filemames list for, 144
- platform support for
- restarting, 155, 159

## B

Backing up, Administration server data, 86, 169

### Bootstrap files

- contents of, 56
- writing to, 86

### Browsers

- character sets, 215
- errors, 235, 236
- issue with uppercase characters, 139

## C

### Cache

- cleanup, 128, 204, 206
- fast cache response, 229
- preventing caching of Web pages, 153
- refresh interval, Policy Validator, 127

### Certificates

- data signing, 79, 99
- delegated administration, 86
- for data signing, 79
- for delegated administration, 86
- for directory servers, 75, 78, 79
- signing data, 79, 84
- standard installed, 87
- troubleshooting, 228, 233, 234, 235
- verify intervals, 79, 82

### CGI, troubleshooting, 236

### Character set, configuring, 152

### Components, installing specific, 40, 46

### Configuring

- components. *See also* Setup Tool
- email alerts, 108
- in console mode, 53, 58
- Select Access, parameter types, 56
- selectaccess.conf, 56

### Console mode

- configuring Select Access in, 53, 58
- installing Select Access in, 52

### Content folder, defining location of, 52

### Control Panel, adding and removing components, 177, 188, 194

### Cookies

- creating, overview, 119
- domain, 139
- encryption settings for, 125
- sharing among Validators, 19
- signing, 116
- tracking credentials with, 125
- troubleshooting, 227, 236
- verifying, 116, 125
- Web session, 153

### CPU, exceeding capacity of, 16

### CRLs

- Administration server, 79
- Validator, 81

### Custom Enforcer plugins, configuring, 131

## D

### Daemons

- entropy gathering, 35

## Data

- auditing. *See* Auditing, 94
- backing up, 170
- configuration, recording of, 55
- converting characters, 152
- distributed directory topology, 16
- encryption of, 17, 78, 119, 125
- enhancing throughput of, 25
- fault tolerance of, 19
- generating random, 35
- monitoring integrity of, 93
- planning redundancy of, 16, 18, 19
- policy location. *See* Policy Store
- signing. *See* Certificates, 99

### Databases

- creating tables, 106
- deploying Select Access with, 26
- JDBC, 18, 85, 102, 104
- logging events to, 84
- migrating data in, 84
- reporting, 84, 85
- using with Secure Audit server, 102

### Debugging

- command line options, 160, 204, 206, 207
- messages, Secure Audit server, 146
- mode, Policy Validator, 180, 186
- mode, Secure Audit server, 112

### Decider plugins, 115

### Defaults

- Administration server's execute path, 37
- audit settings, global, 83
- configuration parameters, 57, 63, 83
- configuration parameters, Select Access, 56
- gzip path, 36
- HP-UX performance parameters, 35
- installation directory, Select Access, 39, 46
- installation mode, 37, 44
- referrals, directory servers, 20
- restoring to, 40, 46, 178, 190
- selectaccess.conf, 56
- selectaccess.conf, location of, 55
- set in XML bootstrap files, 56
- SSL port, 70

### Delegated Administration

- CA certificates for, 86, 87
- configuring values for, 76
- description, 75
- regenerating certificate for, 73
- scalability, 21
- server resources for, 76

### Delegated Administration mode

- troubleshooting, 225

- Deployment issues
  - affiliates or partners, 20
  - content servers and third-party technologies, 21
  - corporate security, 17
  - directory topology, 18, 20
  - growth potential, 21
  - overview, 15
  - redundancy policy, 18
  - scenarios, 22

- Deregistering components, 196, 197

- Digital signatures
  - signing audit stream, 96, 99
  - signing policy, 17, 67, 79
  - troubleshooting, 234

- Directory servers
  - certificates, 75
  - characters, invalid, list of, 11
  - configuring identity location in, 66, 71
  - distributing data in, 20
  - list of supported, 11
  - protecting data of, 79
  - replicating, 19, 67, 82
  - setting up, 69, 70
  - supported LDAP servers, 11
  - topology, 20, 21
  - troubleshooting, 232, 233

- Disk space, minimum requirements for, 9

- Domains
  - enabling reverse lookup of, 160
  - setup of multiple, 133, 140
  - setup of pass-through, 134, 145
  - setup of single, 133, 138, 139

- Domino application server
  - Enforcer plugin for, 131

- Dynamic groups
  - definition, 241
  - troubleshooting, 236

## E

- Email. *See* Alerts

- Encryption settings, 125

- Enforcer API library
  - custom Enforcer plugin, configuring, 131
  - operating systems available for, 9

- Enforcer plugins

- balancing queries using round-robin, 149
- bootstrap XML file for, 155
- descriptions of supported types, 131
- failover, supporting, 148
- how to configure, 130, 163
- HTTP headers, using, 144
- list of installable, 10
- operating system support for, 9
- platform availability, 10
- Policy Validator, quit attempt to open connection, 152
- proxy mode, enabling, 153
- restarting with server, 156
- See Also* Apache Web server, Axis application server, IIS Web server, Netscape/iPlanet/Sun ONE Web server, Oracle application server, Servlet Enforcer plugin, TCP Enforcer plugin,
  - setup, custom, 66, 119, 130, 133
  - setup, typical, 66, 119, 130, 133
  - supporting Integrated Windows authentication, 131
  - troubleshooting, 230, 231, 236

- Entropy gathering daemon, 35

- Errors

- browser, 235, 236
- configuring to a standard stream, 110
- denied access, to service, 231
- denied access, Web page, 231
- logging, 112, 236
- Policy Builder, 224
- runtime, system log, 83
- Secure Audit server, 102
- XML, 236

- Events, logs, 83, 99, 124, 147

## F

- Failover

- deploying Select Access for, 19, 20
- of the Administration server, 86, 169
- support, Enforcer plugins, 148
- troubleshooting, 148

- Fatal exceptions, 112

- Federation, deployment example, 20

- Files, ignored by Enforcer, 141, 143

- Filtering

- events, 111, 112

- Firewalls

- deploying with, 149
- NAT mapping for, 135

## Forms

- defining location of content folder, 52
- login, 229
- templates *See also* Templates

## G

Guide, contents of, 13

GZIP, path, 36

## H

Hardware requirements, 9

Hostnames. *See* Addresses, 69

## HP-UX

- deleting old files from, 34
- gzip, using with, 36
- minimum requirements for, 9
- platform availability for, 9
- recommended performance parameter, 35, 36
- setting printev for, 37
- starting Apache manually on, 157

## HTTP

- basic authentication, 229
- domains, protecting. *See* Domains
- GET request, 236
- headers, 144, 236
- paths. *See also* URLs
- SOAP. *See* SOAP
- tags, troubleshooting, 224

## HTTPS

- running Netscape/iPlanet/Sun ONE over, 156
- SSO failing over, 236

## I

IBM, protecting on Windows, 32

## Identities

- credentials, troubleshooting, 229

## Identity credentials

- authenticating with certificates, 86
- configuring, 19
- creating, 125
- evaluating, 116

Identity data location. *See* Identity store

## Identity store

- configuring location for, 66, 71
- distributing data in, 20, 21
- See Also* Policy Store

Ignored filenames, 141, 143

## IIS Web Server

- configuring with enforcer, 154
- restarting, 155, 158

## IIS Web servers

- platform support for, 10, 12

inetd, using, 159

## Installing Select Access

- in console mode, 52
- in default mode, 38
- mode overview, 38
- system requirements, 9

## Integrated Windows authentication

- Enforcer plugin support for, 131
- troubleshooting, 230

## Integrations

- overview, 7

Internet Information Service. *See* IIS

IP addresses. *See* Addresses, 69

ISAPI, 236

IWA *see* Integrated Windows authentication

## J

Java Virtual Machine, 53

## JDBC

- database, as audit repository, 102
- database, configuring, 102, 104
- database, logsetup utility, 106
- database, requirements for, 106
- reporting, 84

## L

Level, logging hierarchy, 111, 112

License agreement, 39, 45, 172, 179, 184, 190

Links, symbolic, 37, 52

## Linux

- deleting old files from, 34
- minimum requirements for, 9
- platform availability for, 9
- setting printev for, 37

## Lists

- available Policy Validators, 149
- character sets, 215
- Pass-through domains, 146
- protected Web sites, 140
- revocation, 79
- virtual Web sites, 145

Load balancing, 18, 21, 125, 134, 148, 149

Localizing Select Access, 61

Login forms. *See* Templates

Lookup, reverse, 160

Looping queries, 228

## M

- Maintaining components, 171, 184
- Memory, minimum requirements for, 9
- Modes
  - console, installer, 52
  - console, setting up, 53, 58
  - Delegated Administration, 21, 76
  - Self Administration, 76, 77
  - Web Administration, 76, 77

## N

- NAT
  - devices, communicating over, 149
  - mapping addresses, 135, 150
  - port for, 150
- Netscape/iPlanet/Sun ONE Web servers
  - Enforcer plugin for, 131
  - modifying configuration of, 156
  - platform support for, 10, 12
  - restarting, 155
  - running out of stack, 156
- Network
  - address translation. *See* NAT, 149
  - discovery, troubleshooting, 224

## O

- OCSP, 81
  - server URL, 79
  - timeouts, 79, 151, 228
  - troubleshooting, 228, 233
- Operating systems
  - Enforcer plugin support for, 9
  - minimum requirements for, 9
  - platform availability for, 9
- Oracle
  - Enforcer plugin, 131
  - entry point for, 85
  - migrating data, 84
  - supported application server, 12
  - supported directory server, 11

## P

- Parameters
  - common parameters, 57
  - default group parameters, 57
  - ignored filenames, 141, 143
  - override parameters, 57
  - pass-through domains, 145
- Pass-through domains, 145
- PDFs, troubleshooting, 230

- Personalization
  - improving performance for, 128
  - old tags for, 162
  - troubleshooting, 236
  - using. *See Also* HTTP headers
- Platforms. *See* Operating systems
- Policies, audit, 110
- Policy Builder
  - default port, 76, 77
  - description, 10
  - errors, 224
  - operating systems available for, 9
  - password dictionary, 126
  - platform availability, 10
  - running in Delegated Administration mode, 225
  - troubleshooting, 231
- Policy data location. *See* Policy Store
- Policy signing
  - enabling, 80
  - importing certificate and key, 81
  - setup screen for, 67, 79
  - using with SSL, 78
- Policy Store
  - backing up, 169
  - defining directory location of, 70, 71
  - preventing unauthorized changes to, 79
  - See Also* Identity Store
  - signing data in. *See* Policy signing
  - SSL certificate for, 17, 79
  - storing revocation list in, 79
- Policy Validator
  - cache refresh interval, 127
  - Configuration Editor, 9
  - configuring, 115, 160
  - custom setup, 117
  - Enforcer plugin, 151
  - logging, 112, 229
  - operating systems available for, 9
  - platform availability, 10
  - plugins for, 115
  - port, 119, 123
  - registration, 226
  - server pool, 149
  - startup script, running manually, 205
  - troubleshooting, 226, 227, 228, 231, 233, 234, 236
  - typical setup, 117
  - uninstalling, 160
- Portal servers, supported, 12

## Ports

- administration modes, Delegated, 76
- administration modes, overview, 75
- administration modes, Root, 76
- administration modes, Self, 77
- administration modes, Web, 77
- Administration Server, 136, 165, 197
- directory server, 70, 82
- NAT, 150
- Policy Validator, 118, 119, 121, 123, 131
- Secure Audit server, 97, 98
- SSL vs non-SSL, 70

printenv, path to, 37

Processor, minimum requirements for, 9

## Proxy

- mode, enabling, 153

## Q

### Queries

- auditing. *See* Secure Audit server
- authentication, 129
- copying user data into, 128
- details, customizing data in, 152
- increasing fault tolerance, 19, 148
- increasing performance, 18, 148
- looping, 228
- OCSP. *See* OCSP
- overview, 115
- redirecting, 21, 148
- retrying Policy Validators, 151
- timeouts, avoiding, 151
- troubleshooting, 228
- utility program for, 11
- XML, maximum size, 128

## R

Recovering, the Administration server, 86, 169

Red Hat Linux. *See* Linux

Registering, Policy Validator, 226

Registry entries, 37

Registry entries, creating, 37

Repairing components, 171

### Reports

- backing up, 170
- configuring, 84, 85
- coordinating with the Secure Audit server, 26
- enabling, 18, 68, 85
- from runtime messages, 94, 124, 147
- requiring, 18
- SQL scripts for, 84

## Requirements

- Administration server, configuring, 53
- Axis Lib folder, 42
- content forms, 56
- deployment, planning, 15
- files used by Select Access, 56
- GAC, 33
- JVM, 53
- parameters, configuration, 57
- registry entries, 37
- schema updates, 11, 30
- system, summary of, 9

Reverse lookup, 160

Revocation list, configuring, 79

## Round robin

- definition of, 148
- publishing keys, 125

## S

SAML server, removing, 31, 32, 33

### Schemas

- updates, 11, 30
- uploading, 70

### Secure Audit server

- configuring databases for, 102
- connection timeouts, 100
- debugging, 112
- platform availability, 10
- port, 97, 98
- setting up clients of, 83
- signing data digitally, 99
- SOAP, 98
- timeouts for, 100



- Select Access
    - Administration Server. *see* Administration server
    - bootstrap file, defaults in, 56
    - component redundancy, planning, 18
    - default installation directory, 39, 46
    - deploying for fault-tolerance, 19, 20
    - deregistering components, 196, 197
    - Enforcer plugins. *See* Enforcer plugins
    - fault tolerance of, 19
    - installing, 34, 38, 45, 187
    - integration overview, 7
    - modifying installed components, 171, 184
    - operating systems available for, 9
    - platform availability, 9
    - Policy Builder. *See* Policy Builder
    - Policy Validator. *See* Policy Validator
    - query program, 11
    - repairing installed components, 171
    - Secure Audit Server. *See* Secure Audit server
    - selectaccess.conf, 55
    - Setup Tool. *See* Setup Tool
    - startup script, running manually, 205
    - system requirements, 9
    - uninstalling installed components, 171, 194, 195
  - selectaccess.conf
    - timeout parameter in, 100
    - writing to, 44, 52, 55, 177, 183, 188, 194
  - Self administration
    - configuring, 77
    - overview, 66, 76
  - Server pool, 149
  - Service name, Web administration, 77
  - Servlet Enforcer plugin
    - description, 131
  - Setup Tool
    - Administration server, configuring with, 63 to 86
    - custom settings, configuring with, 161 to 166
    - Enforcer plugin, configuring with, 132 to 155
    - platform availability, 10
    - Policy Validator, configuring with, 118 to 128
    - Secure Audit server, configuring with, 95 to 96
  - Signatures, digital
    - cookies and nonces, 125
    - definition, 245
    - for audit stream, 99
    - signing for data, 67, 79
    - signing for SSL, 17
    - troubleshooting, 234
    - wrong signatures, 79
  - SOAP messages
    - encrypting, 142
    - protocol, 98
    - signing, 141
  - Software requirements, 9
  - Solaris
    - deleting old files from, 34
    - localizing Select Access on, 61
    - minimum requirements for, 9
    - platform availability for, 9
    - setting printev for, 37
  - SQL, scripts for database tables, 106
  - SSL
    - certificates needed, 75, 79
    - configuring port for, 70
    - directory server setup, 78
    - gathering random data, 35
    - port to disable, 70
    - regenerate, 73, 122, 137
    - troubleshooting, 228, 233
  - SSO
    - creating cookies for, 138
    - multiple DNS domain, 133, 140
    - single DNS domain, 133, 139
    - troubleshooting cookies, 227, 236
  - Startup script
    - Administration server, starting manually, 205
    - options for, 207
    - Policy Validator, starting manually, 205
    - Setup Tool, starting manually, 202
  - Symbolic links, 37, 52
  - Synthetic identities. *See* Transient identities, 112
  - System defaults, configuration parameters, 63
  - System requirements for Select Access installation, 9
- ## T
- Tables, creating for SQL databases, 106
  - TCP Enforcer plugin
    - configuring, 159
    - description of, 131
  - Telnet, accessing resources, 229
  - Templates
    - folder for, 56
    - HTML forms, 153, 229
  - Timeouts
    - OCSP, 151, 228
    - parameter for Secure Audit server, 100
  - Transient identities
    - certificates for, 112

- Troubleshooting
  - attributes, 236
  - browser errors, 235, 236
  - certificates, 228, 233, 234, 235
  - CGI, 236
  - denied access, to service, 231
  - denied access, to Web page, 231
  - digital signatures, 234
  - directory servers, 232, 233
  - Enforcer plugin, 230
  - forms, 229
  - HTTP basic authentication, 229
  - HTTP headers, 236
  - integrated Windows authentication, 230
  - ISAPI, 236
  - logging, 236
  - network discovery, 224
  - network services, 231
  - OCSP, 233
  - PDFs, 230
  - personalization, 236
  - Policy Builder, 224, 225, 231
  - Policy Validator, 226, 227, 228, 233, 234
  - referrer headers, 236
  - registration, 226
  - roles, 236
  - SSL, 228, 233
  - SSO cookies, 227, 236
  - URLs, 224
  - virtual servers, 229
  - Web servers, 228
  - XML, 236

Trusted servers, deployment example, 20

Typical setup, administration server, 64

## U

Uninstalling

- components, 171, 194, 195
- Policy Validator, 160
- Policy Validator manually, 205, 207

Unix, console mode, 52, 53, 58

Upgrading, removing files, 34

URLs

- enabling proxy format, 153
- path to Administration login page, 136
- troubleshooting, 224

Utility programs, query utility, 11

## V

Video card, minimum requirements for, 9

Virtual Web sites, 145

VNC, 37

## W

Web administration, configuring, 77

Web sites

- denied access to, 231
- troubleshooting, 228
- virtual, 229

Windows

- minimum requirements for, 9
- platform availability for, 9

WSE Enforcer plugin, 131

## X

XML

- bootstrap file, writing to, 56
- signing, troubleshooting, 234
- troubleshooting, 236

X-Windows, 37