

HP OpenView Select Access

Installation Guide

Software Version: 6.0

for HP-UX, Linux, Solaris, and Windows operating systems



March 2004

© Copyright 2000-2004 Hewlett-Packard Development Company, L.P.

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 2000-2004 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.

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's `<install_path>/3rd_party_license` directory.

Trademark Notices

- Intel® and Pentium® are registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
- Java™ is a US trademark of Sun Microsystems, Inc.
- Linux is a U.S. registered trademark of Linus Torvalds.
- Microsoft®, Windows®, and Windows NT® are U.S. registered trademarks of Microsoft Corporation.
- Oracle® is a registered US trademark of Oracle Corporation, Redwood City, California.
- UNIX® is a registered trademark of The Open Group.

Support

Please visit the HP OpenView Select Access web site at:

<http://www.openview.hp.com/products/select/index.html>

There you will find contact information and details about the products, services, and support that HP OpenView Select Access offers.

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

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

The support site includes:

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

Contents

Chapter 1: Introduction	1
Who is it for?	2
What does it assume you already know?	2
About the Select Access documentation set	2
Related references	3
Chapter 2: Select Access: components and requirements	5
What does Select Access do?	5
Supports single sign-on	5
Enables user profiling	6
Provides user password and profile management	6
Delegates administration	7
Provides an end-to-end auditing system	7
Automates the discovery and maintenance of corporate resources	7
How does Select Access work?	8
Other Select Access components	8
Third-party components Select Access integrates with	9
Custom plugins you can customize functionality with	9
Gauging your installation environment	10
System requirements	11
Platform availability	11
Supported LDAP directory servers	14
Supported third-party servers	15
Chapter 3: Installing Select Access	17
Before you begin—choosing your installation scenario	17
Installing Select Access for the first time	18
Upgrading from version 5.2	19
Upgrading from versions 5.1 or 5.0	19
Upgrading from a version previous to 5.0	20
What upgrade issues you face	22
Installation directory changes	22
Installing the WSE Enforcer plugin	22
Using signed audit logs	23
Attributes disabled in attribute logic decision point	23
Policy signing disabled	23
Self-registration cookie incompatibility	24
Manually deleting old files on Unix	24
Password and registration authentication behavior	24
Mounting your CD drive on HP-UX	25
Running the Select Access 6.0 installer	26
Before you begin	26
Running the installer—a mode overview	29
Chapter 4: Configuring Select Access	51
About the selectaccess.conf file	52
Understanding setup methods and parameter types	52
Using the Setup Tool	53
How to set up Select Access	54

Things to check before you finish	57
Chapter 5: Configuring the Administration server	59
What the Administration server does	59
Configuring the Administration server	60
The Administration server's main setup types	60
Using the Setup Tool to configure the Administration server	60
Defining the Administrator credentials	63
Defining your Policy Store	64
Specifying the Policy Data Location	66
Preconfiguring a User Location	68
Choosing your setup type	69
Defining the Administration server connection information	70
Configuring the Policy Builder administration modes	71
Configuring the web-based administration services	73
Setting up SSL connection handling	74
Configuring the directory server's certificate	75
Configuring Policy Store data signing	76
Verifying the signer's certificate	78
Creating a replicated directory servers list	79
Configuring global audit settings	80
Configuring database reporting	82
Completing the Administration server setup process	83
Failing over to another Administration server	84
Adding Delegated Administration CA certificates	84
Different certificate types	85
Chapter 6: Configuring the Secure Audit server	91
About client/server auditing with the Secure Audit server	92
Configuring the Secure Audit server	93
Using the Setup Tool to configure the Secure Audit server	93
Configuring the Secure Audit server connection information	95
Configuring server-specific audit settings	96
Configuring audit stream signing	97
Completing the Secure Audit server setup process	99
Configuring an Audit Trail	99
Configuring a Secure Audit server	101
Configuring a database	103
Creating database tables	105
Configuring a log file	106
Configuring an email alert	108
Configuring system logging	109
Configuring a standard error stream	110
Configuring an Audit Policy	110
How you create audit policies	110
Supported audit policy combinations	113
Starting the Secure Audit server	119
Windows—starting the Secure Audit server manually	119
Unix—starting the Secure Audit server manually	120
Chapter 7: Configuring the Policy Validator	121
How does the Policy Validator work?	121
Configuring the Policy Validator	123
The Policy Validator's main setup types	123

Using the Setup Tool to configure the Policy Validator	123
Connecting to the Administration Server	126
Choosing your setup type	127
Setting connection parameters for the Policy Validator	129
Configuring validator-specific audit settings	130
Defining data encryption settings	131
Specifying a password dictionary	133
Tuning your Policy Validator.	133
Completing the Policy Validator setup process	135
Starting the Policy Validator	136
Windows—starting the Policy Validator manually.	136
Unix—starting the Policy Validator manually.	138
Uninstalling the Policy Validator.	138
Chapter 8: Configuring the Enforcer plugins.	139
How Enforcer plugins work.	139
Configuring the Enforcer plugin	139
The Enforcer plugins' main setup types	139
A note about enforcer-specific setup wizards	140
Using the Setup Tool to configure the Enforcer plugin	141
Connecting to the Administration Server	146
Choosing your setup type	147
Defining an Enforcer plugin ID	148
Setting up single domain single sign-on.	149
Setting up multidomain single sign-on	151
Setting up SOAP message signing	152
Setting up SOAP message encrypting.	154
Setting up a list of ignored filenames.	155
Setting up a list of pass-through domains	158
Configuring enforcer-specific audit settings.	159
Configuring Policy Validator settings.	161
Mapping Policy Validators to NAT addresses.	163
Tuning your Enforcer plugin.	164
Completing the Enforcer plugin setup process	167
Starting your Enforcer plugin	170
The Sun ONE Web Server dialog	170
The Apache Web Server dialog	171
The IIS Web Server dialog	172
The Axis Host Application dialog	173
Manually configuring inetd to start the TCP Enforcer plugin.	174
Uninstalling the Enforcer plugins.	175
Chapter 9: Configuring the SAML server.	177
What is the SAML server?.	177
Using the Setup Tool to configure the SAML server	177
Connecting to the Administration Server	180
Defining a SAML server ID.	181
Configuring basic setup parameters.	181
Setting up a SAML destination partners list.	185
Setting up a SAML source partners list	188
Completing the SAML server setup process	193
Starting your SAML server	195
Windows—starting the SAML server manually	196
Unix—starting the SAML server manually.	196

Uninstalling the SAML server	196
Chapter 10: Configuring custom settings	197
When is it necessary to configure custom settings?	197
Configuring the Custom Settings Flags	198
Predefined flags	198
Using the Setup Tool to configure the custom settings flags	198
Connecting to the Administration Server	200
Enabling custom settings flags	201
Completing the custom settings setup process	202
.	202
Chapter 11: Maintaining Select Access: failovers, repairs, and updates	203
Failing over to another Administration server	203
Tips for ensuring a smooth recovery	203
Maintaining Select Access	205
Repairing Select Access	205
Modifying Select Access	220
Uninstalling Select Access	234
Appendix A: Localizing Select Access interfaces and rendering localized data	241
Translating and loading localized resource bundles	241
Using Select Access's resource bundle	242
Translating extracted resource bundles	243
Converting translated files to Unicode	244
Supporting internationalized data	244
Using your own fonts	244
Rendering localized fonts in Select Access	246
Identifying your locale on Solaris	247
Identifying physical fonts on Windows	249
Installing the correct font on Solaris	250
Mapping the physical font to a logical name on Windows	250
Mapping the physical font to a logical name on Solaris	254
Querying multilingual URLs	258
Appendix B: Character set listing	259
Appendix C: Troubleshooting	267
Policy Builder errors	267
Network Discovery not detecting redirects	267
Policy Validator errors	267
Policy Validator generates error when installing	267
Policy Validator failing at startup	268
Policy Validator and hostnames	268
iPlanet 4.0 and Sun ONE 6.0: cookies not refreshed on IE	269
Policy Validator looping	269
Policy Validator short circuits	269
Policy Validator missing SSL session information	270
Web server/Application server errors	270
HTTP basic authentication problematic	270
Restricted IBM HTTP server resources	270
Virtual Web server support problems with IIS	271
Caching problems with IIS	271
Integrated Windows authentication issues on IIS	272

Denied access errors 272

 Denied access to service 272

 Denied access on default page 273

 Browser gets deny yet Policy Validator gives allow 273

Directory Server errors 273

 iPlanet and iPlanet Unicode problems 273

 Critical Path and Siemens over SSL problems. 273

Certificate errors 274

 Browsing for OCSP certificates on Critical Path 274

 Generic problems 274

 Microsoft certificates and failed signing 275

 Problems specific to IIS 276

 Problems specific to Apache 276

Browser errors 277

 SSO failing on Internet Explorer 277

Logging errors 277

 Database and email outputs creates XML error 277

Personalization problems 277

 Empty role attribute values 277

Glossary 279

Index 301

Chapter 1

Introduction

This *HP OpenView Select Access 6.0 Installation Guide* describes how to install and configure the Select Access components. The table that follows provides an overview of this guide's contents.



See the *HP OpenView Select Access 6.0 Release Notes* ([relnotes.pdf](#)) on the Select Access installation CD for known installation issues at the time of this release.

Table 1: Guide overview

Chapter	Description
Chapter 2, <i>Select Access: components and requirements</i>	Gives an introduction to Select Access: what it is, what it does, and how it works.
Chapter 3, <i>Installing Select Access</i>	Provides an overview of how to install Select Access.
Chapter 4, <i>Configuring Select Access</i>	Provides an overview of how to configure Select Access.
Chapter 5, <i>Configuring the Administration server</i>	Gives specific details on how to set up the Administration server.
Chapter 6, <i>Configuring the Secure Audit server</i>	Provides an introduction to the Secure Audit server, and platform-specific instructions for setting up logging across multiple Select Access components.
Chapter 7, <i>Configuring the Policy Validator</i>	Describes how to start, stop, and configure one or more Policy Validators.
Chapter 8, <i>Configuring the Enforcer plugins</i>	Provides platform-specific details on how to start, stop, and configure one or more Enforcer plugins.

Table 1: Guide overview (Continued)

Chapter	Description
Chapter 9, <i>Configuring the SAML server</i>	Describes how to set up the SAML server.
Chapter 10, <i>Configuring custom settings</i>	Describes how to set flags for backwards compatibility.
Chapter 11, <i>Maintaining Select Access: failovers, repairs, and updates</i>	Describes how you can recover if the host of your Administration server fails.
Appendix A, <i>Localizing Select Access interfaces and rendering localized data</i>	Provides details on setting internationalization with your system.
Appendix B, <i>Character set listing</i>	Lists all the supported character set available to be used with the Enforcer plugin.
Appendix C, <i>Troubleshooting</i>	List solutions to problems you may experience.

Who is it for?

This guide is intended for individuals or teams responsible for installing and configuring Select Access with existing network technologies.

What does it assume you already know?

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.

About the Select Access documentation set

The documentation set includes:

- `readme.txt`
- *HP OpenView Select Access 6.0 Release Notes*
- *HP OpenView Select Access 6.0 Installation Guide*
- *HP OpenView Select Access 6.0 Network Integration Guide*
- *HP OpenView Select Access 6.0 Policy Builder Guide*

- *HP OpenView Select Access 6.0 Developer's Tutorial Guide*
- *HP OpenView Select Access 6.0 Developer's Reference Guide*
- *HP OpenView Select Access 6.0 SAML Solution Guide*
- Select Access third-party *Integration Papers*.
- Online Help: Setup Tool and Policy Builder

Related references

- *HP OpenView Select Access 6.0 Network Integration Guide*, © Copyright 2000-2004 Hewlett-Packard Development Company, L.P. ([network_integration_guide.pdf](#))
- *HP OpenView Select Access 6.0 Policy Builder Guide*, © Copyright 2000-2004 Hewlett-Packard Development Company, L.P. ([policy_builder_guide.pdf](#))
- *HP OpenView Select Access 6.0 Developer's Tutorial Guide*, © Copyright 2000-2004 Hewlett-Packard Development Company, L.P. ([developers_tutorial_guide.pdf](#))
- *HP OpenView Select Access 6.0 Developer's Reference Guide*, © Copyright 2000-2004 Hewlett-Packard Development Company, L.P. ([developers_reference_guide.pdf](#))
- *HP OpenView Select Access 6.0 SAML Solution Guide*, © Copyright 2000-2004 Hewlett-Packard Development Company, L.P. ([saml_solutions_guide.pdf](#))

Select Access: components and requirements

Select Access is a centralized access management system that provides you with a unified approach to defining authorization policies and securely managing role-based access to on-line resources. It uses a collection of components that integrate with your network, to give you and your partners the ability to capitalize on the potential of extranets, intranets and portals. These components, along with the access policies you set, offer your Web and wireless users a seamless user experience by connecting them to dispersed resources and applications.

What does Select Access do?

Several features of Select Access extend its functionality beyond that of a simple authorization administration tool. It is a complete access management system, offering you a set of features to support your online relationships with your users and your content partners:

- *Supports single sign-on*
- *Enables user profiling*
- *Provides user password and profile management*
- *Delegates administration*
- *Provides an end-to-end auditing system*
- *Automates the discovery and maintenance of corporate resources*

Together, this extended functionality provides a simplified experience for both the end user and those responsible for managing what the user sees and interacts with.

Supports single sign-on

To improve user satisfaction, Select Access incorporates a Web Single Sign-On (SSO) capability. This means users can sign on once to access all permitted resources and have their information stored for future access. Select Access supports transparent navigation between:

- **Multiple proprietary domains:** For organizations with ownership of multiple Web sites.

- Multiple partnering domains: For on-line business partners, so they can securely share authentication and authorization information across corporate boundaries that have separate:
 - user databases
 - authorization policies
 - access management products

Using SSO means that users do not have to remember multiple passwords or PINs, thereby reducing the amount of help desk support.

Enables user profiling

A user is represented as a user entry that is stored in a directory server. When you create a user entry, you can also define a set of attributes that describe that user, which become part of the user's profile. The values contained in the attribute can be used in two ways:

- *To determine level-of-access with roles:* Role-based access allows you to configure and apply policies automatically, according to the attribute values stored in the user's profile.
- *To determine delivery-of-content:* Select Access exports user attributes and their values as environment variables, so that applications can use the profile information to personalize Web pages and to conduct transactions.



A user's profile dynamically changes as a user conducts transactions with your organization. As attributes in the profile change, so too can the role the user belongs to. For example, a customer's profile may contain his current bank balance, date of last transaction, and current credit limit—any of which can change from moment to moment.

This capability of Select Access makes development of Web applications much easier, because programmers do not have to develop (or maintain) complex directory or database access codes to extract entitlement information about each user.

Provides user password and profile management

Select Access's password and profile management feature makes it easy for users to conduct business and minimize the demand on technical resources that can best be employed elsewhere. This feature includes the following principles:

- *Password administration:* Allows you to set the policies and expiration times for user passwords. Select Access automates reminders and messages. Other administration features include:
 - Profile lockout and re-activation
 - Password history lists
- *Self-servicing:* Allows users to initiate:

- The definition of new or existing passwords, which are controlled by the password policy you create.
- The modification of profile data, which is predefined by the attributes you select. Typically, these attributes are the same attributes the user provides when they register with your organization. If the user is already known to you (like an employee or a supplier), you can pre-populate the values for them.

By allowing users to self-manage passwords and profile data, you reduce the amount of help desk support.

Delegates administration

Delegated Administration allows for delegation of both user and policy management, providing more control for decentralized administrators. Select Access's delegation is highly efficient: it supports sub-delegation to multiple tiers of administrators, which mimics real-world organization charts. This decentralized approach to administration:

- Reduces administrative bottlenecks and costs.
- Puts the power to manage users in the hands of those who best understand those users.

Provides an end-to-end auditing system

Select Access can record all access and authorization actions, as well as all policy administrative changes to any number of outputs, such as:

- The HP Secure Audit server
- JDBC-compliant databases
- Local files
- Platform-specific log files
- Email

Of all output choices, the Secure Audit server is the most useful: not only does it collect messages from different components on a distributed network, but it also allows you to digitally-sign all audit entries and ultimately create a report from the outputs collected.

Automates the discovery and maintenance of corporate resources

In order to define and enforce authorization, Select Access must be aware of all the resources on your network, as well as the users who want to access them. Select Access uses the directory server as the central repository for policy data, which includes the resource listing. You can deploy special HTTP/HTTPS-specific plugins to automatically scan any given network, thereby enumerating available services and resources. As services and resources are enumerated by the plugin, it adds them hierarchically in the Policy Builder's Policy Matrix. Unlike other products that require manual data input (where a simple typing error can put the security of resources at risk) Select Access saves administrators' time and improves accuracy.

How does Select Access work?

Select Access delivers the core of its authorization and authentication functionality with the following technical components:

- *Policy Builder*: Allows full or delegated administrators to define the authentication methods and authorization policies with an easy-to-use administration grid.
- *Policy Validator*: Serves the access decision to the Enforcer plugin after it accepts and evaluates the user's access request with the policy information retrieved from the directory server that holds your Policy Store.
- *Enforcer plugin*: Acts as the agent for Select Access on the Web/application server. The Enforcer plugin enforces the outcome of the access request that has been evaluated by the Policy Validator.
- *SAML server*: Handles the logistics of transferring users between your web sites and those of your partners.

These core components form a sophisticated and consistent architecture that easily adapts to any existing network infrastructure. Primarily XML and Java-based, you can readily extend Select Access to meet the needs of future security requirements.

The authentication process

Select Access's authentication and authorization of Web-based or wireless users takes place within a small number of basic steps. Select Access components communicate via XML documents known as queries and responses. XML offers Select Access complete flexibility for data transmission and integration into existing and future applications, whether Web or non-Web based. Select Access's authentication and authorization process follows these steps:

1. A user makes a request to access a resource.
2. The Enforcer plugin passes details of the request to the Policy Validator, including any authentication information provided.
3. The Policy Validator collects user and policy data from the directory and then caches it for future retrieval.
4. Based on this combination of information, the Policy Validator returns a policy decision to the Enforcer plugin, including relevant information to dynamically personalize the user experience.

Other Select Access components

Other Select Access components provide the support system for Select Access's core components:

- *Administration server & Setup Tool*: As a mini Web server, the Administration server is responsible for the configuration of core components and deployment of the Policy Builder applet in a user's browser. The Setup Tool is a client of the Administration

server: it is the interface that allows you to quickly set up and deploy Select Access.

- *Secure Audit server*: Collects and manages incoming log messages from Select Access components on a network.

Third-party components Select Access integrates with

Other third-party components that are integral to an effective Select Access solution:

- *Directory server – LDAP v3.0 compliant*: is the foundation of a Select Access-protected system. It acts as the repository of information. Depending on how you have set up your directory system, Select Access can use one or more directory servers to store:
 - A single policy data location
 - One or more user data locations
- *Web/Application/Portal/Provisioning servers*: are third-party technologies that use Select Access as their authorization and access management system. Depending on your server technology, you can use Select Access’s native SSO and/or personalization solution rather than use the server’s built-in alternative for a more robust solution.

Figure 1 illustrates how Select Access and third-party components interact with each other.

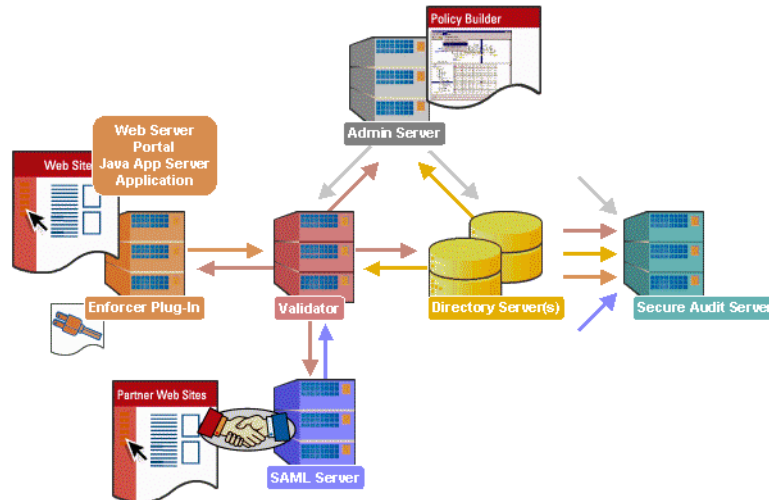


Figure 1: Select Access system architecture

Custom plugins you can customize functionality with

To more efficiently capture your organization’s business logic, you can use Select Access’s APIs to build custom plugins. Plugins that you can customize functionality with include:

- *Authentication plugins*: A custom Policy Builder authentication plugin allows you to tailor which kinds of authentication methods are available to better meet the needs of your organization. A Policy Builder authentication method plugin

allows administrators to use and configure the authentication server for this method via a dialog box. As with the decision point plugin, this dialog box is a property editor that allows security administrators to configure the authentication server.

- *Decision point plugins*: A custom Rule Builder decision point plugin allows you to tailor how rules are built to better meet the needs of your organization. A Rule Builder decision point plugin allows administrators to use and configure the criteria for the decision point via:
 - The icons that represent that decision point on both the toolbar and the rule tree.
 - The dialog box, known as a property editor, that allows security administrators to configure it.
- *Policy Validator decider plugins*: The Validator-specific counterpart of a decision point plugin, the decider plugin allows you to capture the evaluation logic for your custom decision point (described above), so that the Policy Validator can evaluate users based on the information it collects.
- *Resource discovery plugins*: These plugins allow you to customize how resources are scanned on your network.
- *Enforcer plugins*: A new Enforcer plugin allows you to customize the backend application logic by enforcing the decision that the Policy Validator returns to the Enforcer plugin's query.
- *Additional Web/Application/Portal/Provisioning server specific plugins*: These plugins can be included to handle specific integration details between the third-party technology and Select Access. For example, the Domino server requires a `site_data` plugin if you need to transfer site data between Select Access and Domino.

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:

- *System requirements* on page 11
- *Platform availability* on page 11

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 14
- *Supported third-party servers* on page 15

System requirements

To install any of the Select Access components, your system must meet the minimum hardware and software requirements outlined in Table 2.

Table 2: Minimum system requirements

Hardware and software	Minimum on Windows	Minimum on Unix
Processor	Pentium 3 450 MHz	<i>For Linux:</i> Pentium 133 <i>For Solaris:</i> Sun Ultra5 <i>For HP-UX:</i> HP-UX 9000
Memory	256 MB RAM	64 MB RAM
Disk space (combination of temporary space and real space required for a full install)	250 MB	<i>For Linux:</i> 150 MB <i>For Solaris:</i> 300 MB <i>For HP-UX:</i> 220 MB
Video card	256 colors	256 colors
Operating systems Note: Not all components are supported on all operating systems. See <i>Platform availability</i> on page 11 for details.	Windows NT 4.0 Service Pack 6a Windows 98 Windows 2000 Professional Service Pack 2 Windows 2000 Server Service Pack 2 WindowsXP	Red Hat Linux 7.3 Solaris 2.8, patch 108940-07 from www.sun.com HP-UX 11.B.11.00 64 bit with all required patches

Platform availability The Select Access components are available for the following platforms: Windows (Windows 98, Windows NT, Windows 2000, and Windows XP) and Unix (Linux, Solaris, and HP-UX).

You can install Select Access components on different platforms; all components communicate with each other irrespective of the platform you installed them on. Table 3 provides a comprehensive list of components and their corresponding supported platforms. For information on Select Access components, see *How does Select Access work?* on page 8.



Due to the dissolution of the relationship between Netscape and Sun, iPlanet Web servers have been renamed to Sun ONE. Note that this name change affects the name of the Enforcer plugin for this server. The Sun ONE (iPlanet) Enforcer plugin still supports existing iPlanet Web servers as well as the newly named Sun ONE 6.0 Web servers.

Table 3: Platform availability

Components	Platform						
	Windows 98	Windows NT	Windows 2000	Windows XP	Linux 7.2	Solaris 2.8	HP-UX 11
Front-end (GUI) components							
<i>Setup Tool:</i> A standalone configuration utility that is installed on any computer that hosts any Select Access component.	✓	✓	✓	✓	✓	✓	✓
<i>Policy Builder:</i> The interface used to manage access policies and delegate and/or subdelegate administration duties to other users.	✓	✓	✓	✓		✓	✓
Back-end components							
<i>Administration server:</i> Select Access’s Web server-based component that conducts administrative functions such as component configuration, certificate management, and policy data administration.		✓	✓			✓	✓
<i>SAML server:</i> Select Access’s server that enables SSO for authenticated users of partner organizations using a protocol known as Security Assertions Markup Language.		✓	✓			✓	✓
<i>Policy Validator:</i> Select Access’s decision-making component that determines whether user access is allowed or denied.		✓	✓			✓	✓
<i>Secure Audit server:</i> Select Access’s log tool that collects and manages incoming log messages from components on a network.		✓	✓			✓	✓
<i>Enforcer plugins:</i> Select Access’s decision-enforcement component. Select Access includes Enforcer plugins for the following Web servers:							

Table 3: Platform availability (Continued)

Components	Platform						
	Windows 98	Windows NT	Windows 2000	Windows XP	Linux 7.2	Solaris 2.8	HP-UX 11
<ul style="list-style-type: none"> • Apache Enforcer plugin for version 1.3.22 of Apache (as well as 1.3.19 on HP-UX) <p>Note: On HP-UX, the Apache Enforcer plugin works with <code>mod-ssl</code>.</p> <p>Note: If you are using 2.0 of Apache on Linux 7.2, a plugin is included on the CD with Select Access, but not installed. See the <i>Apache 2.0 Integration Paper</i> for details.</p>					✓	✓	✓
<ul style="list-style-type: none"> • Apache Enforcer plugin for HP-UX with <code>mod-ssl</code> 							✓
<ul style="list-style-type: none"> • Axis Enforcer plugin 					✓	✓	
<ul style="list-style-type: none"> • Domino Enforcer plugin 							
<ul style="list-style-type: none"> • IBM HTTPD Enforcer plugin for WebSphere 		✓	✓	✓			
<ul style="list-style-type: none"> • IIS Enforcer plugin 		✓	✓	✓			
<ul style="list-style-type: none"> • Oracle Enforcer plugin 					✓	✓	✓
<ul style="list-style-type: none"> • Sun ONE (iPlanet) Enforcer plugin for Sun ONE 6.0 Web servers and iPlanet 4.0 Web servers 		✓	✓		✓	✓	✓
<ul style="list-style-type: none"> • TCP Enforcer plugin 					✓	✓	✓
<ul style="list-style-type: none"> • WSE Enforcer plugin (Available only if the .NET framework and associated utilities have been installed.) 			✓	✓			
Utility programs							
<p><i>Query program:</i> A command line application that sends queries to a Policy Validator. These queries do large test runs that check its performance.</p>		✓	✓	✓	✓	✓	✓
Support and development files							

Table 3: Platform availability (Continued)

Components	Platform						
	Windows 98	Windows NT	Windows 2000	Windows XP	Linux 7.2	Solaris 2.8	HP-UX 11
<i>Enforcer API library (C/C++, COM, Java):</i> A set of routines and protocols that pass access queries from a resource server to the Policy Validator.		✓	✓	✓	✓	✓	✓
<i>Policy API:</i> A set of routines and protocols that give clients a greater ability to query Select Access to see if a user has access to certain links, so that supported Web pages like ASP and JSP can decide whether or not to even display the link. Note: The Policy API is also dependent upon Microsoft DLLs. Due to legal restrictions, HP cannot ship these DLLs along with Select Access. For more information, see the <i>HP OpenView Select Access 6.0 Developer's Tutorial Guide</i> .		✓	✓	✓	✓	✓	✓
<i>Logger API:</i> A set of method for logging events and messages using Select Access's framework.		✓	✓	✓	✓	✓	✓
<i>Code examples:</i> A set of examples that illustrate how to create custom plugins for Select Access.		✓	✓	✓	✓	✓	✓
<i>Documentation set:</i> A set of documents that are designed to help you use Select Access.		✓	✓	✓	✓	✓	✓

Supported LDAP directory servers

Select Access uses LDAP v.3-compliant directory servers for searching and storing user information. By integrating with standards-compliant LDAP servers and meta-directories for access to legacy user data stores, information can be easily synchronized across a globally

dispersed network, including those with multiple delegated administrators.



If your directory server(s) 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 5, *Preconfiguring a directory server*, in the *HP OpenView Select Access 6.0 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 v.3-compliant directory servers:

- iPlanet 5.0
- Sun ONE 5.1
- Netscape 6.01
- Novell eDirectory 8.5.1 and 8.6.2
- Siemens DirX 6.0A10
- Critical Path Directory 4.0 and 4.1
- Microsoft Active Directory 5.0
- Oracle Internet Directory (9i) 3.0.1.1 + patches
- CA eTrust Directory Server 3.6 sp2

For more information on whether or not your directory server requires a manual schema update, see Chapter 5, *Preconfiguring a directory server*, in the *HP OpenView Select Access 6.0 Network Integration Guide*.



To see a list of which characters are supported by specific directory servers only, see Appendix B, *Invalid characters* in the *HP OpenView Select Access 6.0 Policy Builder Guide*.

Supported third-party servers

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

- *Application/Web servers*: A content delivery server program in a computer that is usually part of a three-tier configuration: a client, an application server, and a database. Select Access supports the following application servers:
 - BEA WebLogic 6.1
 - IBM WebSphere 4.0
 - HP Application Server 8.0
 - SilverStream 3.7
 - iPlanet Application Server

- Domino 5.0.8 Application Server
- Oracle 9i Application Server
- Outlook Web Access Server for Windows 2000
- Apache 2.0 on RedHat Linux 7.2
- Apache Reverse Proxy Server 1.3.22
- Tomcat 4.0.3 on Apache 1.3.22
- Tomcat 4.0.3 servlet engine – standalone
- Citrix NFuse Server 1.6 or 1.7 on MetaFrame 1.8 or XP
- Siebel 7.0.4
- *Corporate portal servers*: A server that centralizes access to information and applications for employees and customers. Select Access supports the Plumtree Corporate Portal.
- *E-provisioning servers*: A server that facilitates the way in which physical and digital resources are allocated to new or existing users. Select Access supports Access 360's enRole server.

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.

This chapter provides an overview of how to install the Select Access components on your network. It describes what deployment options are available to you depending on the size of your organization. Important topics to carefully read before beginning include:

- *Before you begin – choosing your installation scenario* on page 17
- *Running the Select Access 6.0 installer* on page 26

Installing Select Access is greatly simplified with the installer and the Setup Tool. However, before installing Select Access, read Chapter 4, *Deploying Select Access on your network*, in the *HP OpenView Select Access 6.0 Network Integration Guide*. This chapter describes deployment options you can consider, depending on the size of your organization.

Before you begin—choosing your installation scenario

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 4.

Table 4: Different deployment scenarios

This scenario...	For details, see...
A new install of Select Access. Because you have never installed Select Access before, this installation is relatively straightforward. Few caveats apply.	<i>Installing Select Access for the first time</i> on page 18

Table 4: Different deployment scenarios (Continued)

This scenario...	For details, see...
<p>A minor upgrade.</p> <p>This means that your previous version was one of SelectAccess 5.0, SelectAccess 5.1, or Select Access 5.2.</p> <p>Upgrading from version 5.2 is straightforward. If you are upgrading from versions 5.0 or 5.1, there are two categories of upgrades:</p> <ul style="list-style-type: none"> • Upgrading from a patched version of SelectAccess. • Upgrading from an unpatched version of SelectAccess. <p>If you have applied any patches, your installation of Select Access is typically slightly more complex.</p>	<p><i>Upgrading from version 5.2 on page 19</i></p> <p><i>Upgrading from versions 5.1 or 5.0 on page 19</i></p>
<p>A major upgrade.</p> <p>This means that your previous version was any version prior to Select Access 5.0. This is the most complex scenario, due to the number and complexity of changes that occurred to Select Access since version 5.0. For this reason, you must carefully review all sections relating to this scenario.</p>	<p><i>Upgrading from a version previous to 5.0 on page 20</i></p>

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 5.

Table 5: First-time installations

This step...	For details, see...
<p>1. To help you understand installation and configuration options, analyze your network architecture.</p>	<p><i>Chapter 4, Deploying Select Access on your network, in the HP OpenView Select Access 6.0 Network Integration Guide</i></p>
<p>2. Depending on your directory server, you may need to modify its schema to ensure Select Access can upload it.</p>	<p><i>Chapter 5, Preconfiguring a directory server, in the HP OpenView Select Access 6.0 Network Integration Guide</i></p>

Table 5: First-time installations (Continued)

This step...	For details, see...
3. If you are installing on an HP-UX host, mount your CD drive.	<i>Mounting your CD drive on HP-UX on page 25</i>
4. Install Select Access 6.0.	<i>Running the Select Access 6.0 installer on page 26</i>
5. Configure the components you installed.	<i>Using the Setup Tool on page 53</i>

Upgrading from version 5.2 Upgrading from Select Access 5.2 is a straightforward process. The procedure is documented in Table 6.

Table 6: Upgrading from Select Access 5.2

This step...	For details, see...
1. Run the Policy Builder. Click Help>About and check whether or not you have a patched version of Select Access installed. The About dialog appears displaying your explicit version of Select Access.	N/A
2. 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 6.0.	<i>Updating certain directory servers' schemas on page 63 in the HP OpenView Select Access 6.0 Network Integration Guide</i>
3. If you are installing on an HP-UX host, mount your CD drive.	<i>Mounting your CD drive on HP-UX on page 25</i>
4. Upgrade to Select Access 6.0 by running the installer for this version. You do not need to uninstall your current installation. You do not need to reconfigure components once they have been upgraded, unless you want to change their configuration.	<i>To run the installer in default mode over top of Select Access 5.0, 5.1, or 5.2 on page 38</i>
5. Configure the components you installed. Warning: If you are installing over a unpatched version of Select Access, regenerate SSL certificates for all Select Access components. Failing to do so can cause SSL communication to fail between the Policy Validator and other components.	<i>Using the Setup Tool on page 53</i>

Upgrading from versions 5.1 or 5.0 Upgrading from Select Access 5.0 or 5.1 is relatively simple. Depending on whether or not you applied patches to this version of

Select Access, the procedure will vary slightly, as documented by Table 7.

Table 7: Upgrading from a patched/unpatched version of Select Access 5.0 or 5.1

This step...	For details, see...
1. Run the Policy Builder. Click Help>About and check whether or not you have a patched version of Select Access installed. The About dialog appears displaying your explicit version of Select Access.	N/A
2. 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 6.0.	<i>Updating certain directory servers' schemas on page 63 in the HP OpenView Select Access 6.0 Network Integration Guide</i>
3. Because HP modified Oracle and MSSQL server scripts, migrate the data in these tables to use this new format. This is only required if your Secure Audit server logs to a JDBC-compliant database.	N/A
4. If you are installing on an HP-UX host, mount your CD drive.	<i>Mounting your CD drive on HP-UX on page 25</i>
5. Upgrade to Select Access 6.0 by running the installer for this version. You do not need to uninstall your current installation. You do not need to reconfigure components once they have been upgraded	<i>To run the installer in default mode over top of Select Access 5.0, 5.1, or 5.2 on page 38</i>
6. Check for any patches for this release and update this version.	
7. Configure the components you installed. Note: If you are installing over a unpatched version of Select Access, regenerate SSL certificates for all Select Access components. Failing to do so can cause SSL communication to fail between the Policy Validator and other components.	<i>Using the Setup Tool on page 53</i>

Upgrading from a version previous to 5.0

Upgrading from a version previous to Select Access 5.0 (for example, Select Access 3.5.1), is the most complex upgrade process. Because of substantial changes that affect the Policy Store, not to mention a host

of existing and new components, you must carefully understand the upgrade process. Table 8 outlines the upgrade process in this scenario.

Table 8: Upgrading from an early version of Select Access

This step...	For details, see...
1. Understand the upgrade issues that exist for these early versions of Select Access.	<i>What upgrade issues you face on page 22</i>
2. 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 6.0.	<i>Updating certain directory servers' schemas on page 63 in the HP OpenView Select Access 6.0 Network Integration Guide</i>
3. Because HP modified Oracle and MSSQL server scripts, migrate the data in these tables to use this new format. This is only required if your Secure Audit server logs to a JDBC-compliant database.	N/A
4. Uninstall your current installation of Select Access completely from all host computers. When you uninstall the product, the following files remain: <install_path>\bin\enforcer.conf <install_path>\bin\Validator.conf These files can be used as reference when you configure your upgraded components.	<i>SelectAccess Installation Guide (3.5.1 or earlier)</i>
5. If you are installing on an HP-UX host, mount your CD drive.	<i>Mounting your CD drive on HP-UX on page 25</i>
6. Install Select Access 6.0.	<i>Running the Select Access 6.0 installer on page 26</i>
7. Check for any patches for this release and update this version.	
8. Configure your components as required, using the files described in step 4 as a reference.	<i>To configure Select Access with the Setup Tool on page 54</i>
9. Once your system is working, delete the files listed in step 4 from your system.	N/A

What upgrade issues you face

Due to the many product enhancements that have occurred since Select Access 5.0, be aware of the following issues when upgrading to this version from a version of Select Access previous to 6.0:

- *Installation directory changes* on page 22
- *Using signed audit logs* on page 23
- *Attributes disabled in attribute logic decision point* on page 23
- *Policy signing disabled* on page 23
- *Self-registration cookie incompatibility* on page 24
- *Manually deleting old files on Unix* on page 24
- *Password and registration authentication behavior* on page 24
- *Mounting your CD drive on HP-UX* on page 25

Installation directory changes

As of Select Access 5.2, the default installation directory for Select Access has changed. The new installation directories are defined in Table 9.

Table 9: Default Select Access Installation directories

Platform	Installation directory
Windows	HP OpenView\Select Access
Unix	/opt/OV/SelectAccess

Because the Select Access 6.0 installer takes care of managing the transition from the old directory to the new one, the impact of this change is small.

If you are upgrading from a version previous to 5.2, the installer will:

1. Back up all configuration files, log files, and forms to a temporary directory.
2. Entirely remove the earlier installation.
3. Install Select Access 6.0 to the new location.
4. Copy all the backed up files to the appropriate locations in the new installation.

Because all the configuration files are left intact, you do not need to reconfigure the components once Select Access has been installed unless you want to make changes.

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 General 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 on the **Assembly Cache** entry.
3. Add the WSE Enforcer plugin assemblies to the GAC. To add the assemblies:
 - a. Select **Action>Add**. The **Add an Assembly** dialog box appears.
 - b. Select the `Interop.ENFORCERLib.dll` and click **Open**.
 - a. Select **Action>Add**. The **Add an Assembly** dialog box appears.
 - b. Select the `WSEEnforcer.dll` and click **Open**.
4. Close the **.Net Framework Configuration** window.

Using signed audit logs

If you try to use a signed audit log from Select Access 5.0, the log may not be accepted by Select Access 6.0—unless you installed Patch 2. Patch 2 resolved a data signing issue that existed in Select Access 5.0. This issue prevents this version of from using logs prior to Patch 2.

Attributes disabled in attribute logic decision point

When upgrading to Select Access 6.0 from 3.5, attributes you activated for rules containing an attribute logic decision point become disabled. Check the properties of these decision points when you load Policy Builder 6.0 and reactivate attributes as needed.



You may want to print out the text-based equivalents of these rules so you have a record of them before you uninstall version 3.5. That way, when you install, configure, and run version 6.0, you can refer to these documents when reactivating attributes.

Policy signing disabled

If you turned on policy signing in your existing version of Select Access, the Setup Tool disables it automatically in Select Access 6.0 when you choose a **Typical** setup for the Administration server. A **Typical** setup of any component results in using HP defaults and recommended values for most environments. Therefore if you want to continue to use the policy signing feature in this version, ensure you perform a **Custom** setup of the Administration server and check the **Sign data** box on the **Data Signing** setup screen. For details, see *To configure the Administration server* on page 60.

Self-registration cookie incompatibility

Self-registration cookies from Select Access versions prior to version 5.0 are not compatible with Select Access 6.0. After the upgrade process, all users who have self-registered with you must reauthenticate. For details, see Chapter 8, *Enabling single sign-on*, in the *HP OpenView Select Access 6.0 Network Integration Guide*.

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 users need to delete the following files from their system:

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

HP-UX users need to delete the following files:

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

Password and registration authentication behavior

With the addition of multiple user location support, Select Access requires that the base DNs of user entries on your Users Tree not overlap. This means that components can no longer browse for subdirectories for entries since old DNs overlap. For example, a legal tree created with a previous version of Select Access can look like this:

```
mycompany.com
  users
    research
    management
    marketing
```

Table 10 further shows how authentication combinations can be configured against these branches.

Table 10: Example configuration of password servers

This authentication server...	Authenticates the users on this branch...
Password_RnD	ou=research,ou=users,o=mycompany.com
Password_Mgmt	ou=management,ou=users,o=mycompany.com
Password_Mktg	ou=marketing,ou=users,o=mycompany.com

However, because these DNs overlap, this version of Select Access changes the Users Tree to look like the example that follows and modifies all servers to authenticate all users on this branch:

```
mycompany.com
  users
```

In most cases, this automatic update of your Users Tree is a timesaving measure. This update only creates a problem for users if you have assigned a specific password or registration server to each

individual branch of this tree as illustrated in Table 10. If the upgrade process changes behavior you require, return authentication behavior back to its previous state by modifying access policy and authentication server combinations.

For example, the Password_RnD server authenticates all users on this branch `ou=users, o=mycompany.com`. To replicate the behavior shown in Table 10, create a conditional rule using just the Password_RnD server and apply it to all users who belong to the RnD team. This denies access to all other users.

Mounting your CD drive on HP-UX

If you intend to install supported components of Select Access on HP-UX, you need to use a PFS mount.

To mount the Select Access installation CD

1. Check that the `/usr/sbin` directory is in your path. This directory containing the PFS utilities is required to mount your CD drive.
2. Edit your `/etc/pfs_fstab` file so that it contains the following line:

```
<reader> <mount_dir> pfs-rrip xlat=rrip 0 0
```

where:

- `<reader>` is the path to your CD-ROM reader.
- `<mount_dir>` is the path to an existing directory where the CD-ROM is mounted.

For example, your line resembles the following one:

```
< /dev/dsk/clt2d0> </rr_cdrom> pfs-rrip xlat=rrip 0 0
```

3. Run the following commands that start the necessary daemons:
 - `pfs_mountd &`
 - `pfsd 4 &`



You can start these daemons from `rc` if necessary.

4. Mount the drive with this command:

```
pfs_mount <reader> | <mount_dir>
```

To see which files `pfs` has mounted currently, enter the following command, which shows you multiple instances of the same mount:

```
/etc/pfs_mtab
```

where:

- `<reader>` is the path to your CD-ROM reader.
- `<mount_dir>` is the path to an existing directory where the CD-ROM is mounted.

5. Unmount the drive with this command:

```
pfs_unmount <reader> | <mount_dir>
```

where:

- <reader> is the path to your CD-ROM reader.
- <mount_dir> is the path to an existing directory where the CD-ROM is mounted.

6. Open the CD drive and remove the Select Access installation CD with this command:

```
pfs_umount -c <device>
```

Running the Select Access 6.0 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.

Before you begin

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.

- *Ensuring that the Administration server can locate printenv*

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

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 our 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 8 lists HP's recommend parameter values.

Table 11: Recommended HP-UX parameter values

Parameter	Value
Out of box parameters: To ensure the successful installation of Select Access, you should change the following values.	
maxusers	512
nproc	2048
max_proc_thread	3000
nkthread	6000
nfile	4513
maxfiles	2048
maxfiles_lim	2048
ncallout	6000
maxdsiz	2063835136
Other recommended values To improve the performance of Select Access, you should change the following values.	
fs_async	0
maxssiz	134217728

Table 11: Recommended HP-UX parameter values

Parameter	Value
maxtsiz_64bit	1073741824
maxuprc	100
nflocks	200
ninode	2728
sema	1
semmap	1026
semnmi	1024
semnms	1024
semnmu	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 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.

The importance of the correct administration privileges

On Windows, HP recommends that only administrators with local administration privileges 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 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 6.0 installer in two modes: Default mode (or GUI mode) or Console mode. If you are installing Select Access on a Unix host, Console mode is particularly useful to Unix 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 49.

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`).

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 2.

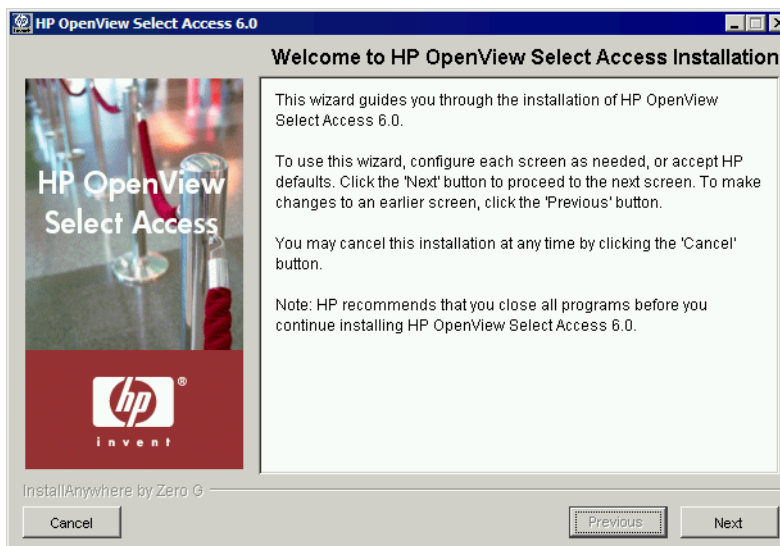


Figure 2: The Welcome to HP OpenView Select Access Installation screen

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

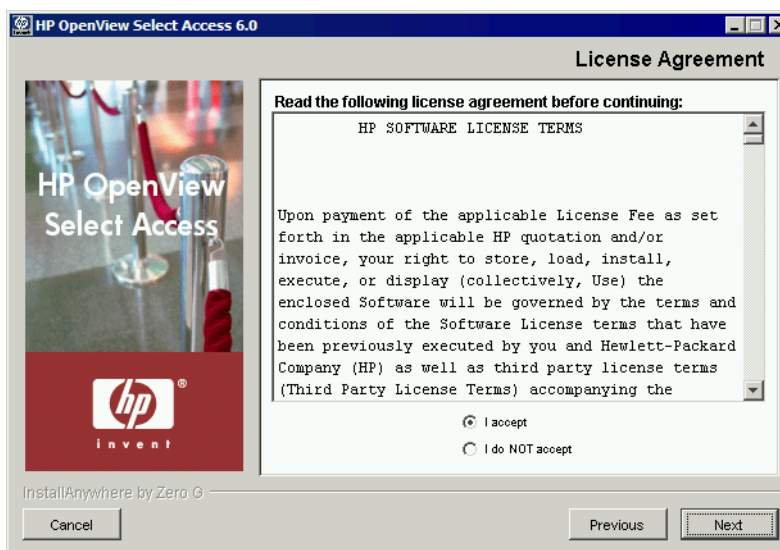


Figure 3: The License Agreement screen

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 13.

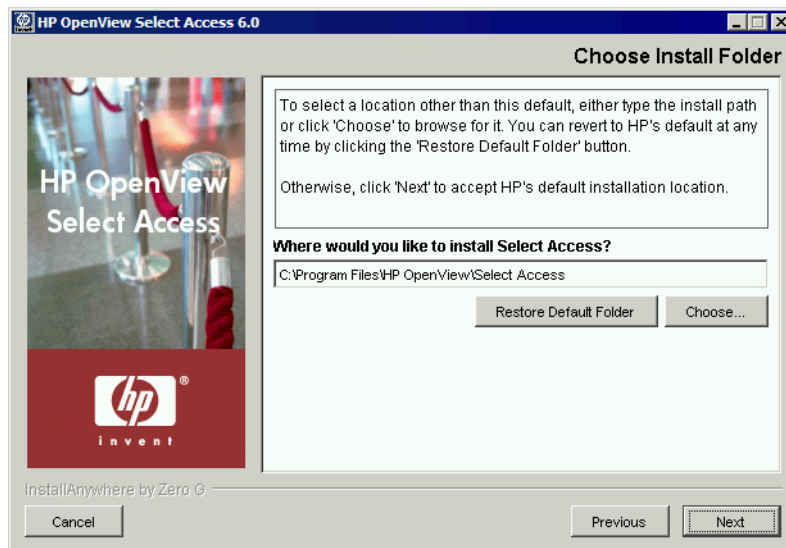


Figure 4: The Choose Install Folder screen

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 5: The 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 11.

Table 12: Select Access components

Plugin	Description
Administration server	Select Access’s Web server-based component that conducts administrative functions that include: component configuration, SSL certificate generation and management, and policy data administration. Note: Only ever 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 84.
Secure Audit server	Select Access’s log tool that collects and manages incoming log messages from components on a network.
Policy Validator	Select Access’s decision-making component. The Policy Validator evaluates Enforcer plugin queries to determine if a user is allowed or denied access.
SAML server	Select Access’s server that enables SSO for authenticated users of partnering organizations using a protocol known as Security Assertions Markup Language.
Sun ONE (iPlanet) Enforcer plugin	Select Access’s decision-enforcement component for the Sun ONE (formerly iPlanet) Web server.
Apache Enforcer plugin	Select Access’s decision-enforcement component for the Apache Web server.
IBM HTTPD Enforcer plugin	Select Access’s decision-enforcement component for the IBM HTTPD Web server.
IIS Enforcer plugin	Select Access’s decision-enforcement component for the IIS Web server. Note: 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.

Table 12: Select Access components

Plugin	Description
WSE Enforcer plugin	Select Access's decision-enforcement component for .NET Web services. Note: 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 (<i>gac_util.exe</i>). For information on installing these components, refer to your .NET documentation.
Axis Enforcer plugin	Select Access's decision-enforcement component for Java Web services.
Domino Enforcer plugin	Select Access's decision-enforcement component for the Domino Web server.
Oracle Enforcer plugin	Select Access's decision-enforcement component for the Oracle Application Server.
servlet Enforcer plugin	Select Access's decision-enforcement component for any servlet engine.
TCP Enforcer plugin	Select Access's decision-enforcement component for services configured in Inetd.
Sample Source	The C/C++ and Java project files and example source files used to build custom plugins: Enforcer, decision point, decider, and authentication. This component also includes some of Select Access's public supporting libraries.

7. Click **Next**.

- If you are installing the Axis Enforcer plugin, see step 88.
- Otherwise, see step 10.

8. If you are installing the **Axis Enforcer plugin**, the **Specify Axis Lib Directory** screen appears, as shown in Figure 6.

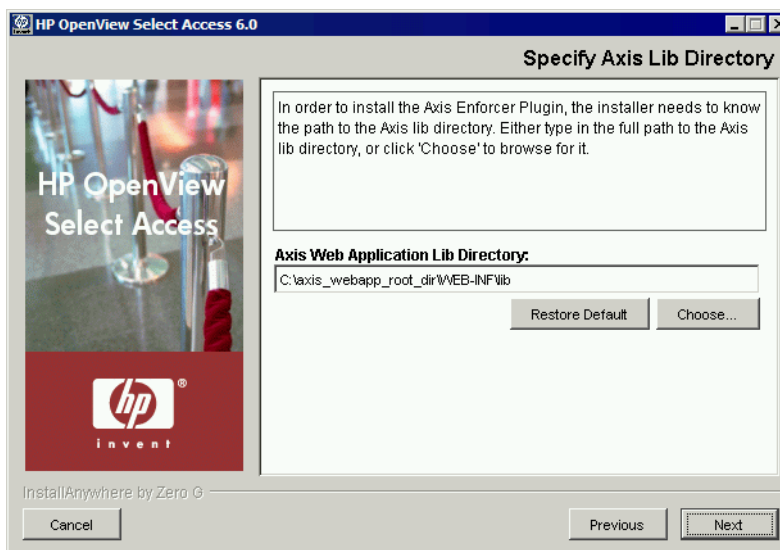


Figure 6: The Specify Axis Lib Directory screen

9. The Setup Tool installs the Axis Enforcer plugin directly into the `Axis lib` directory. In order to do so, however, the Setup Tool 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, select from one of the following configuration options:

- If the default location, `C:\axis_webapp_root_dir\WEB-INF\lib` is correct, proceed to step 10.
 - If the default directory is not correct, click the **Choose** button, select the correct directory, then click **OK**. The new directory appears in the **Axis Web Application Lib Directory** field.
 - 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 6.



Figure 7: The 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 6.0)
- The install path of Select Access.

On Windows, the install path is:

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

On Unix, the install path is:

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

- The folder that holds the program shortcuts for the Select Access administration tools (for example, Policy Builder or the Setup Tool) that is installed to the Windows **Start** menu. Program shortcuts are added to the **Start>Programs>HP OpenView>Select Access** program group. As well, Select Access shortcuts also are installed to your desktop.
- 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.

i Although a dialog appears with options for Internet Explorer and Netscape 6 when you install the Java plugin, the plugin (and therefore, the Policy Builder applet) also works on Netscape 4.

- 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 6.0** screen appears and outlines the installation progress of the components you selected to install.

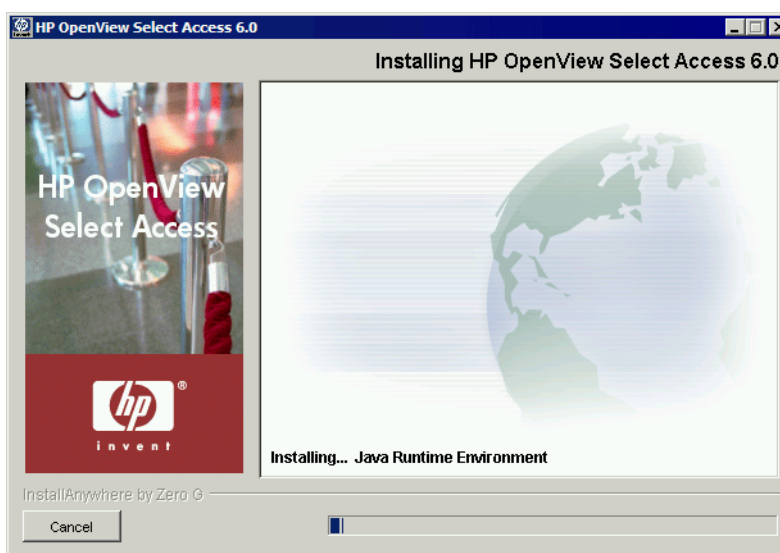


Figure 8: The Installing HP OpenView Select Access 6.0 screen

12. Upon 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.

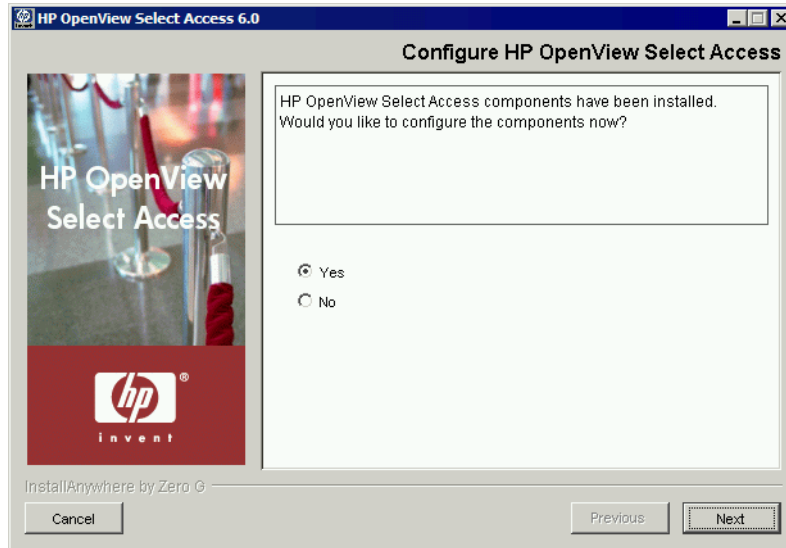


Figure 9: The Configure HP OpenView Select Access screen

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.

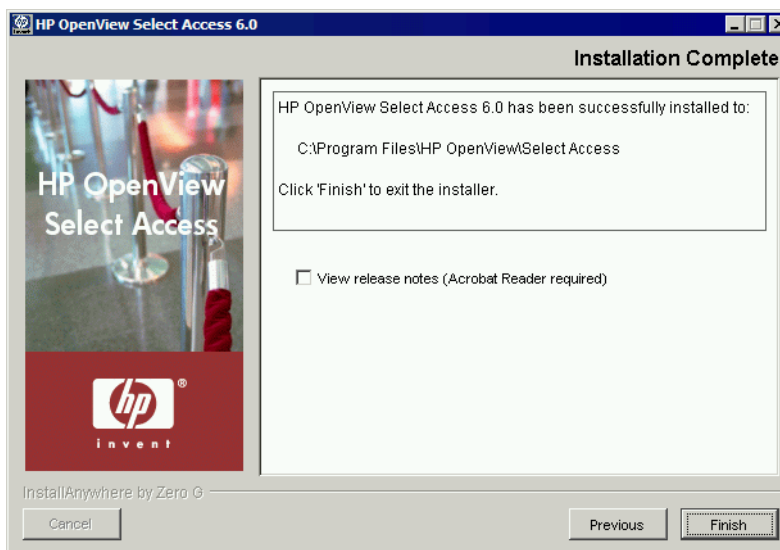


Figure 10: The Installation Complete screen

15. Click the **View Release Notes** box if you want to read the *HP OpenView Select Access 6.0 Release Notes* before continuing.
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. For details, see *About the selectaccess.conf file* on page 52.
 - Cleans up all temporary installation files.

To run the installer in default mode over top of Select Access 5.0, 5.1, or 5.2

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`).

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 6.0** screen appears.

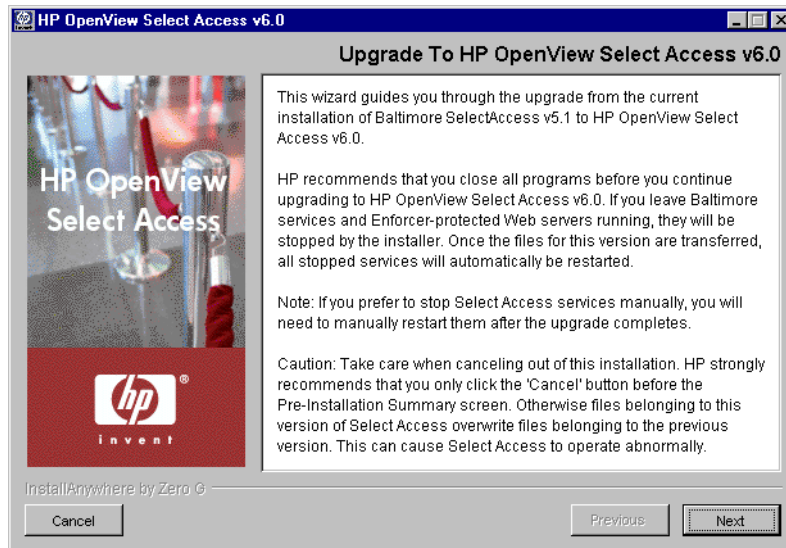


Figure 11: The Upgrade to HP OpenView Select Access 6.0 screen

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

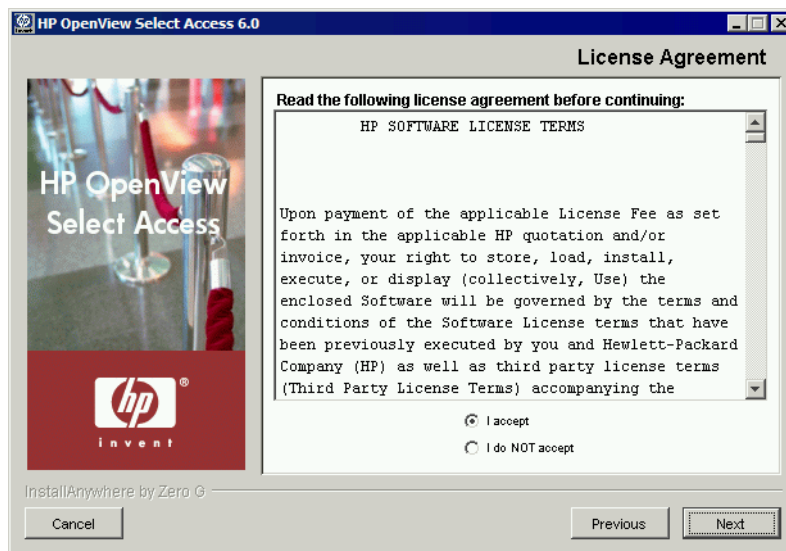


Figure 12: The License Agreement screen

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 13.



Figure 13: The 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.

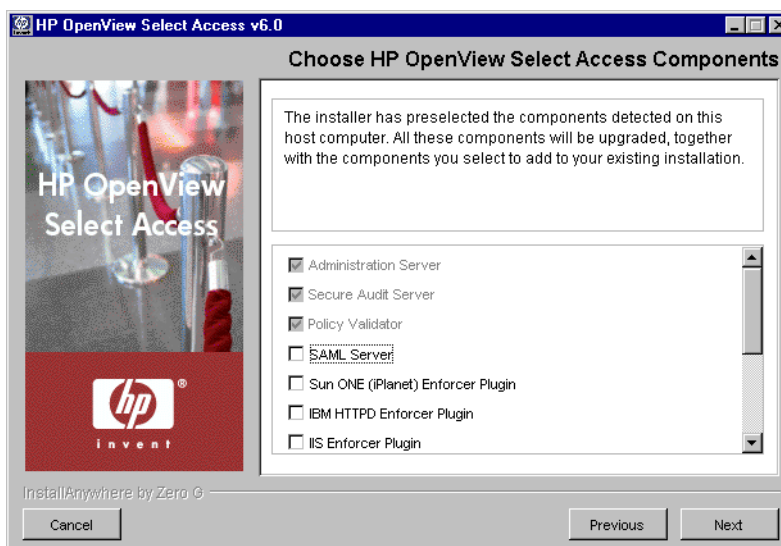


Figure 14: The Choose HP OpenView Select Access components screen

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 11.

Table 13: Select Access components

Plugin	Description
Administration server	Select Access's Web server-based component that conducts administrative functions that include: component configuration, SSL certificate generation and management, and policy data administration. Note: Only ever 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 84.
Secure Audit server	Select Access's log tool that collects and manages incoming log messages from components on a network.
Policy Validator	Select Access's decision-making component. The Policy Validator evaluates Enforcer plugin queries to determine if a user is allowed or denied access.
SAML server	Select Access's server that enables SSO for authenticated users of partnering organizations using a protocol known as Security Assertions Markup Language.
Sun ONE (iPlanet) Enforcer plugin	Select Access's decision-enforcement component for the Sun ONE (formerly iPlanet) Web server.
Apache Enforcer plugin	Select Access's decision-enforcement component for the Apache Web server.
IBM HTTPD Enforcer plugin	Select Access's decision-enforcement component for the IBM HTTPD Web server.

Table 13: Select Access components

Plugin	Description
IIS Enforcer plugin	Select Access’s decision-enforcement component for the IIS Web server. Note: 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.
WSE Enforcer plugin	Select Access’s decision-enforcement component for .NET Web services. Note: 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 (<i>gac_util.exe</i>). For information on installing these components, refer to your .NET documentation.
Axis Enforcer plugin	Select Access’s decision-enforcement component for Java Web services.
Domino Enforcer plugin	Select Access’s decision-enforcement component for the Domino Web server.
Oracle Enforcer plugin	Select Access’s decision-enforcement component for the Oracle Application Server.
servlet Enforcer plugin	Select Access’s decision-enforcement component for any servlet engine.
TCP Enforcer plugin	Select Access’s decision-enforcement component for services configured in Inetd.
Sample Source	The C/C++ and Java project files and example source files used to build custom plugins: Enforcer, decision point, decider, and authentication. This component also includes some of Select Access’s public supporting libraries.

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.



If you are running any of your Policy Validators in debug mode, the installer cannot detect that it is running. Consequently, the Policy Validator is not shut down and its files cannot be modified.



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 installing the Axis Enforcer plugin, the **Specify Axis Lib Directory** screen appears. Go to step 89.
- If you are not installing the Axis Enforcer plugin, the **Pre-Installation Summary** screen appears. Go to step 10.

9. If you are installing the **Axis Enforcer plugin**, the **Specify Axis Lib Directory** screen appears, as shown in Figure 15.

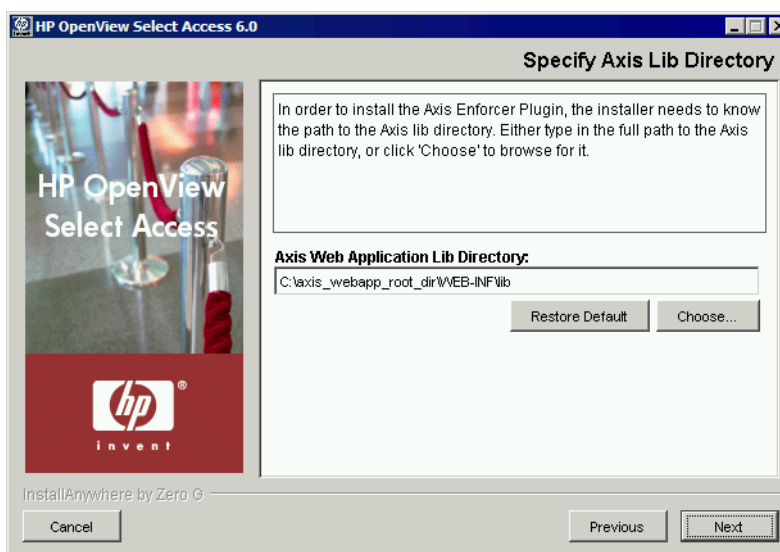


Figure 15: The Specify Axis Lib Directory screen

The Setup Tool installs the Axis Enforcer plugin directly into the `Axis lib` directory. In order to do so, however, the Setup Tool 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 accept the default directory or click the **Choose** button, select the correct directory, then click **OK**. The new directory appears in the **Axis Web Application Lib Directory** field.

10. Click **Next**. The **Pre-Installation Summary** screen appears, as shown in Figure 16.



Figure 16: The 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 6.0)

- The install path of Select Access.

On Windows, the install path is:

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

On Unix, the install path is:

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

- The folder that holds the program shortcuts for the Select Access administration tools (for example, Policy Builder or the Setup Tool) that is installed to the Windows **Start** menu. Program shortcuts are added to the **Start>Programs>HP OpenView>Select Access** program group. As well, Select Access shortcuts also are installed to your desktop.
- 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.



Although a dialog appears with options for Internet Explorer and Netscape 6 when you install the Java plugin, the plugin (and therefore, the Policy Builder applet) also works on Netscape 4.

- 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 6.0** screen appears and outlines the installation progress of the components you selected to install.

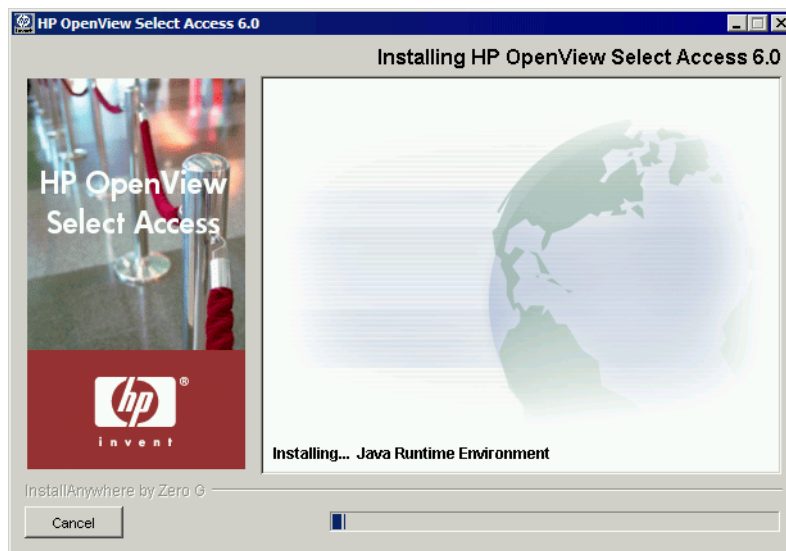


Figure 17: The Installing HP OpenView Select Access 6.0 screen

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



Figure 18: The 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.

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

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

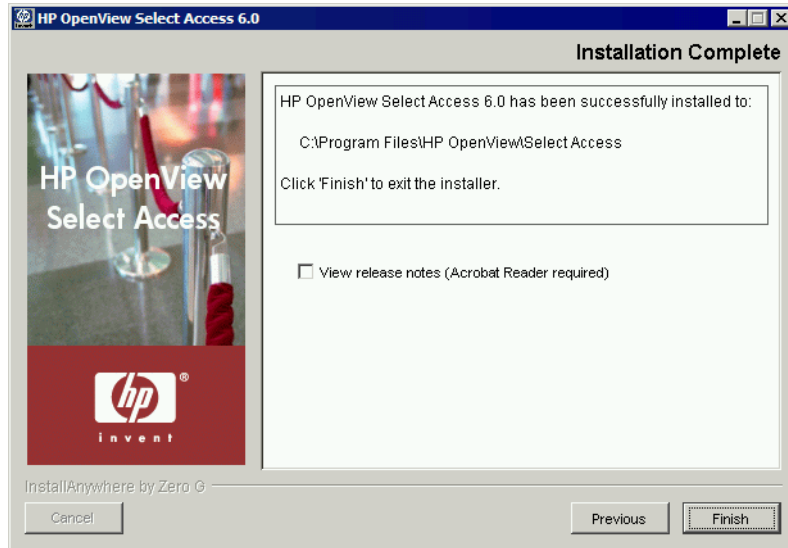



Figure 19: The Installation Complete screen

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.

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 52.
 - 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= SAML server
 - 5= Sun ONE (iPlanet) Enforcer plugin
 - 6= Apache Enforcer plugin
 - 7= TCP Enforcer plugin
 - 8= Sample source

Choose the components you wish to install, by typing in 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. HP recommends that you set up the corresponding component on Windows or a Unix computer that has X-Windows or VNC.
2. Run the Setup Tool and 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 to be 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 file(s) manually. For details, see *When to manually modify a Web server's configuration file* on page 73 in the *HP OpenView Select Access 6.0 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.

This chapter provides an overview of how to configure Select Access. 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 52.

- *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 upon startup and therefore cannot be written to the Policy Store.



If you change the values of any of these parameters, restart the component.



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.

- *The Policy Store:* This 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 14 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 14: Setup method and parameter type availability matrix

	Setup Method		
	Setup Tool	Policy Builder – Component Configuration	Manual editing of XML file
Parameter Types			
<i>Common parameters:</i> Shared by all 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 Component Configuration tool in the Policy Builder.	1st time	X	
<i>Default group parameters:</i> Parameters that are inherited by a group of component types, for example 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.	X	X	X
<i>Override parameters:</i> 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. Note: Override parameters appear bolded in the Setup Tool and the Policy Builder configuration screens.		X	X

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.

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, you cannot run the Setup Tool on these host computers. 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 49.
- *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 and the SAML server only follow 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 section that follows:

- *The Administration server's main setup types* on page 60
- *Configuring the Policy Validator* on page 123
- *Configuring the Enforcer plugin* on page 139

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 20: The 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.

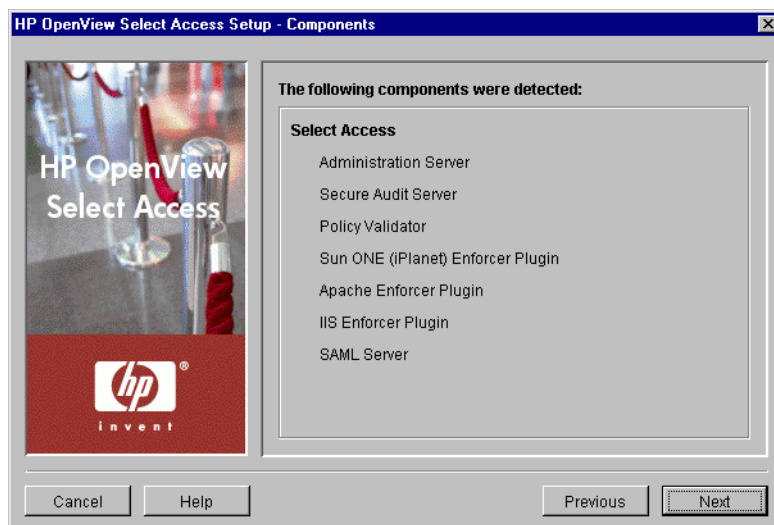


Figure 21: The Components setup screen

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**.

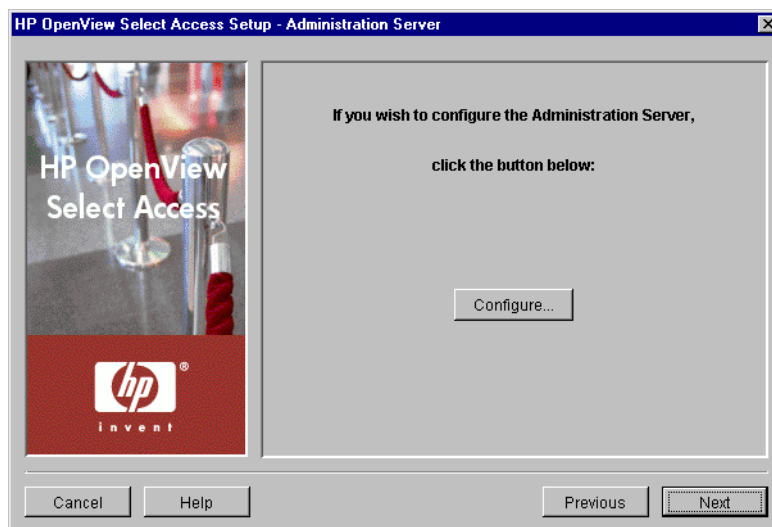


Figure 22: The Administration Server setup screen

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*
 - Chapter 9, *Configuring the SAML server*

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.

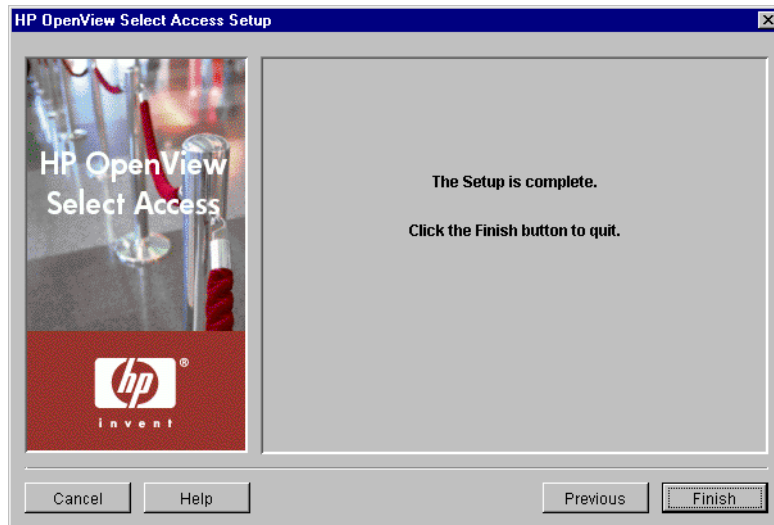



Figure 23: The Setup Complete setup screen

 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.

For details, see Chapter A, *Localizing Select Access interfaces and rendering localized data*.

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 values 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.

- If you changed SAML server settings that require information to be shared with your partners, ensure you have recorded this information so you can distribute changes to them. Otherwise, Select Access cannot complete SAML user transfers.

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.



Run the Administration server as the same user 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.

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.

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 5, *Modifying components' central configuration parameters*, in the *HP OpenView Select Access 6.0 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 recommended values are automatically configured by a **Typical** setup. To allow you to more easily identify what type of setup you need to perform, Table 15 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 24.

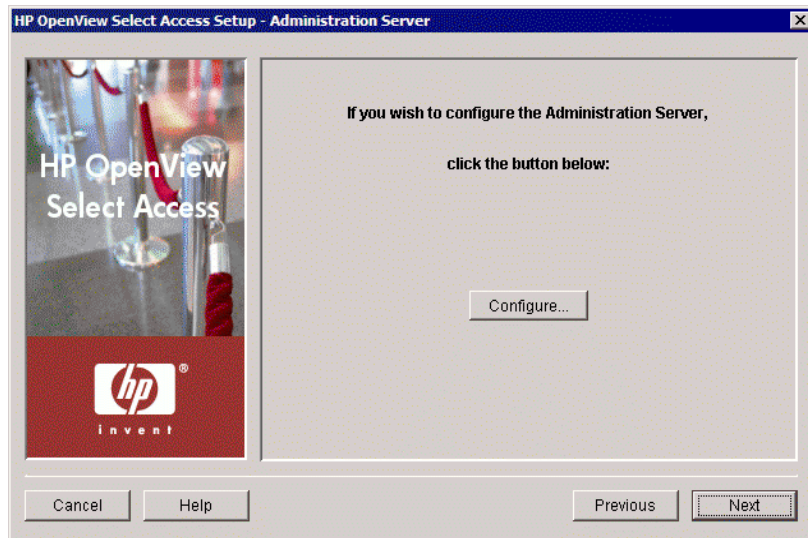


Figure 24: The Administration server setup screen

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 15, as necessary.

Table 15: Overview of Administration server setup process

Setup screen	Description	Default value(s)
Administrator setup screen	Allows you to define the administrator's login credentials. See <i>Defining the Administrator credentials</i> on page 63.	user-defined
Directory Server setup screen	If the Administration server does not detect policy data on this server, this screen allows you to define folder for this repository of policy data. See <i>Defining your Policy Store</i> on page 64.	user-defined
Policy Data Location setup screen	Allows you to define where the policy data will be stored. See <i>Specifying the Policy Data Location</i> on page 66.	user-defined
User Location setup screen	Allows you to define a default user location. The Policy Matrix displays these user entries along the Users Tree when you first launch the Policy Builder. If you do not define a user location with the Setup Tool, you can always add one or more later with the Policy Builder. See <i>Preconfiguring a User Location</i> on page 68.	User location to be defined in the Policy Builder.

Table 15: Overview of Administration server setup process

Setup screen	Description	Default value(s)
General setup screen	<p>Allows you to choose one of two setup types:</p> <ul style="list-style-type: none"> • Typical: Use HP’s recommended setup values. • Custom: Modify the recommended values to meet the needs of your network and/or business environment. <p>See <i>Choosing your setup type</i> on page 69.</p>	Typical
Connection setup screen	<p>Displayed for Custom setup type only.</p> <p>Allows you to define the connection information. Select Access components will use to connect to the Administration server. See <i>Defining the Administration server connection information</i> on page 70.</p>	auto-defined
Administration setup screen	<p>Displayed for Custom setup type only.</p> <p>Allows you to define the ports used by the Policy Builder’s Administration, Delegated Administration, and Forms Based Delegated Administration modes. See <i>Configuring the Policy Builder administration modes</i> on page 71.</p>	auto-defined
Web Administration setup screen	<p>Displayed for Custom setup type only.</p> <p>Allows you to define the ports used by the web-based administrative services, Web Administration and Self Administration. See <i>Configuring the web-based administration services</i> on page 73</p>	auto-defined
SSL Server Certificate setup screen	<p>Displayed for Custom setup type only.</p> <p>Allows you to define how the Administration server handles certificates required to encrypt sessions between administrators and the Administration server. See <i>Setting up SSL connection handling</i> on page 74</p>	handled by Select Access
Directory Server Certificate setup screen	<p>Displayed for Custom setup type <i>only</i> when using SSL.</p> <p>Allows you to customize the verification of the certificate used by the directory server that holds Policy Store data. See <i>Configuring the directory server’s certificate</i> on page 75.</p>	user-defined

Table 15: Overview of Administration server setup process

Setup screen	Description	Default value(s)
Policy Signing 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 <i>Configuring Policy Store data signing</i> on page 76.	disabled
Signer CA Certificate setup screen	Displayed for Custom setup type only. Allows you to customize certificate verification process for the directory server that holds Policy Store information. You can allow unknown CAs or you can require that they be authenticated. See <i>Verifying the signer's certificate</i> on page 78.	allow unknown CAs
Replicated Directory Servers 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 <i>Creating a replicated directory servers list</i> on page 79.	replication not used
Default Audit Settings 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 <i>Configuring global audit settings</i> on page 80.	auto-defined to log all runtime errors
Database Reporting 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 <i>Configuring database reporting</i> on page 82.	disabled
Finish setup screen	Allows you to commit your configurations settings to the Policy Store and the Administration server's bootstrap XML file, and to automatically start the server. See <i>Completing the Administration server setup process</i> on page 83	enable server restart

Defining the Administrator credentials

The Administrator setup screen, shown in Figure 25, allows you to set the username and password used to connect to the Administration server.



Figure 25: The Administrator setup screen

To set the Administrator credentials

1. In the **Username** 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.
3. You can change the Administration server's password at any time by clicking the **Change Password** button.
4. Click **Next**. The **Directory Server** setup screen appears. For details on how to configure this screen, see *Defining your Policy Store* on page 64.

Defining your Policy Store

The **Directory Server** setup screen, shown in Figure 26, allows you to customize the verification of the directory server's certificate (the one that holds Policy Store data).

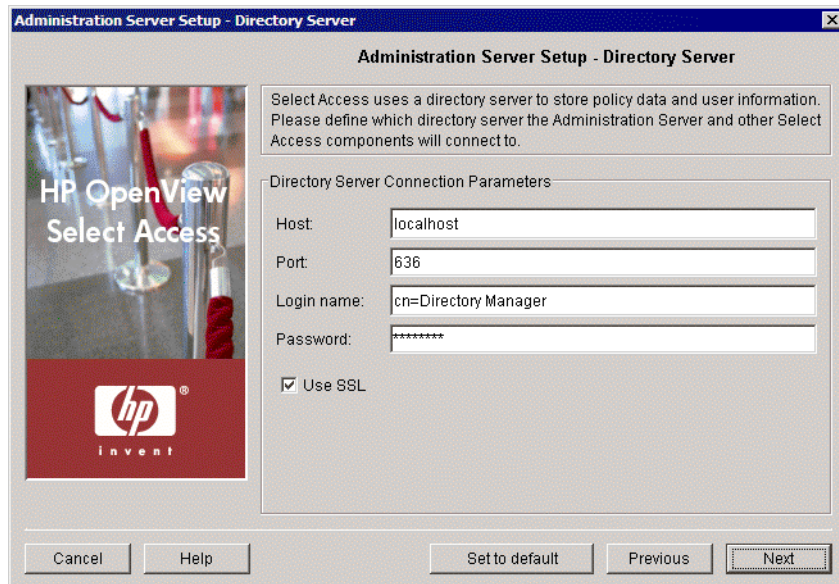


Figure 26: The Directory Server setup screen

To configure a directory server to store Select Access policy

1. Define values for the connection parameters in the **Directory Server Connection Parameters** group.



If you are upgrading from a previous version of Select Access, ensure that you use the same directory server used by the earlier version. Otherwise, the Administration server cannot update your policy information. Automatic updates of your policy information can affect the behavior of some of your access policies. For details on how upgrading to Select Access 6.0 can affect your existing system, see *Upgrading from a version previous to 5.0* on page 20.

- **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 administrator's user name to log into the directory server.

- **Password:** Required. Enter the administrator's password to log into the directory server.
- **Use SSL:** Optional. Check this box 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 Chapter 9, *Understanding certificate-based authentication*, in the *HP OpenView Select Access 6.0 Network Integration Guide*.



If you are using an Active Directory server, you need to temporarily disable SSL the first time you configure it. For details, see *To enable SSL with Active Directory* on page 54 in the *HP OpenView Select Access 6.0 Network Integration Guide*.

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 66.



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 5, *Preconfiguring a directory server*, in the *HP OpenView Select Access 6.0 Network Integration Guide*.

Specifying the Policy Data Location

The Policy Data Location setup screen, shown in Figure 27, 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 27: The 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 change in location to remaining Select Access components.

To do this:

- a. Click **Browse**. The **Select Location** dialog 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 10, *Managing your Policy Data in the HP OpenView Select Access 6.0 Policy Builder Guide*. For details on how to preconfigure your directory server to work with Select Access, see Chapter 5, *Preconfiguring a directory server*, in the *HP OpenView Select Access 6.0 Network Integration Guide*.

2. When you have finished configuring the policy data location, click **Next**. The **User Location** setup screen appears. See *Preconfiguring a User Location* on page 68.

Preconfiguring a User Location

The **User Location** setup screen, shown in Figure 28, allows you to preconfigure a user location that the Policy Builder uses to render an initial set of user entries along the Users Tree.

If you choose not to configure a user location at this time, you can do so when you first run the Policy Builder. Until you configure a user location, the Users Tree will contain no entries and you can set no policies.

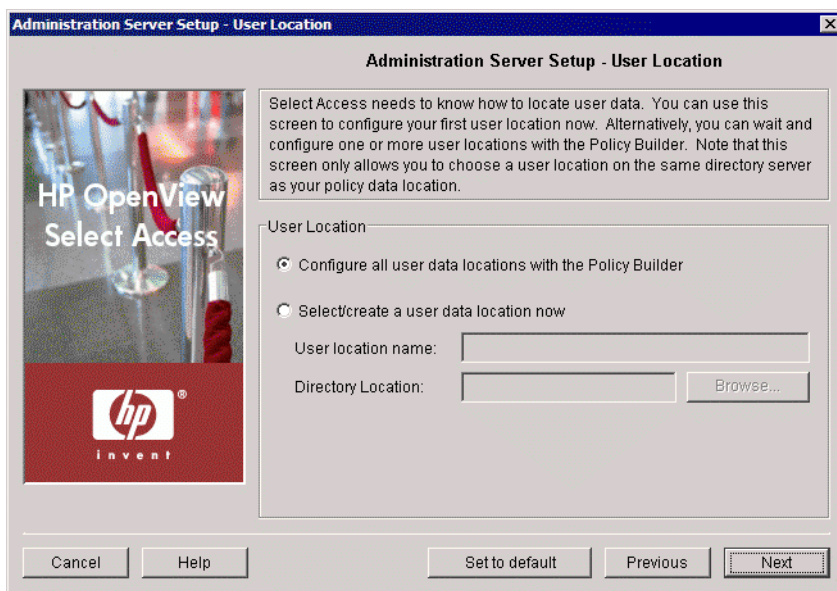



Figure 28: The User Location setup screen

To preconfigure a user location

1. Choose whether or not you want to configure an initial user data location by choosing the corresponding option:
 - **Configure all user data locations with the Policy Builder:** Choosing this option means that when you first run the Policy Builder, your Users Tree appears empty. You therefore need to define at least one user location in the Policy Builder before being able to set access policies. Skip to step 4.
 - **Select/create a user 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 entries on the Users Tree. You can change this user data location or add new ones with the Policy Builder.
2. If you are creating a user data location now, type a text string in the **User location name** field. The Policy Builder uses this string to name the new user data location branch on the Users Tree. Naming branches is particularly important if you decide to add more user locations to the Users Tree at a later date.

3. Click the **Browse** button and select the folder on the directory server that holds user data. This location appears in the **Directory Location** field.

 This user location can 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 69.

Choosing your setup type

The **General** setup screen, shown in Figure 29, allows you to choose whether you want to perform a **Typical** or a **Custom** setup.

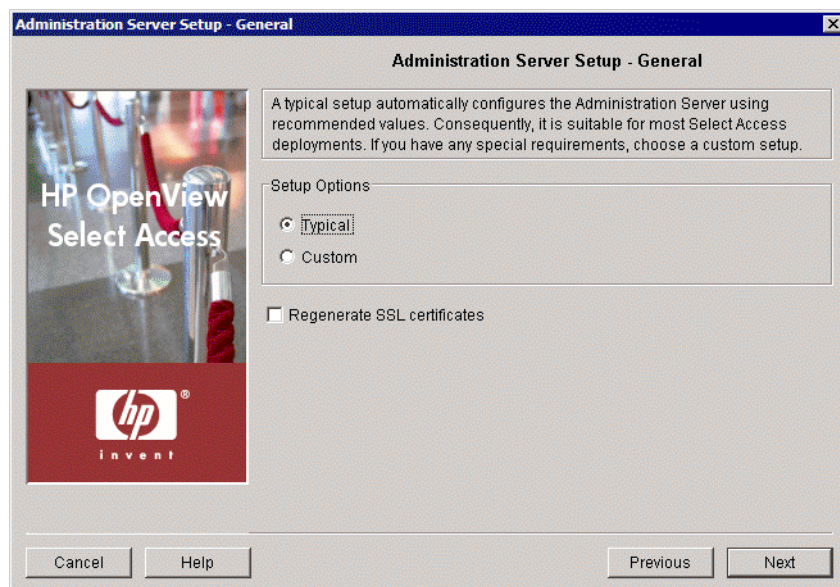



Figure 29: The General setup screen

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, 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 Chapter 9, *Understanding certificate-based authentication*, in the *HP OpenView Select Access 6.0 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 83.
 - If you are performing a **Custom** setup, the **Connection** setup screen appears. See *Defining the Administration server connection information* on page 70.

Defining the Administration server connection information

The **Connection** setup screen, shown in Figure 30, 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.

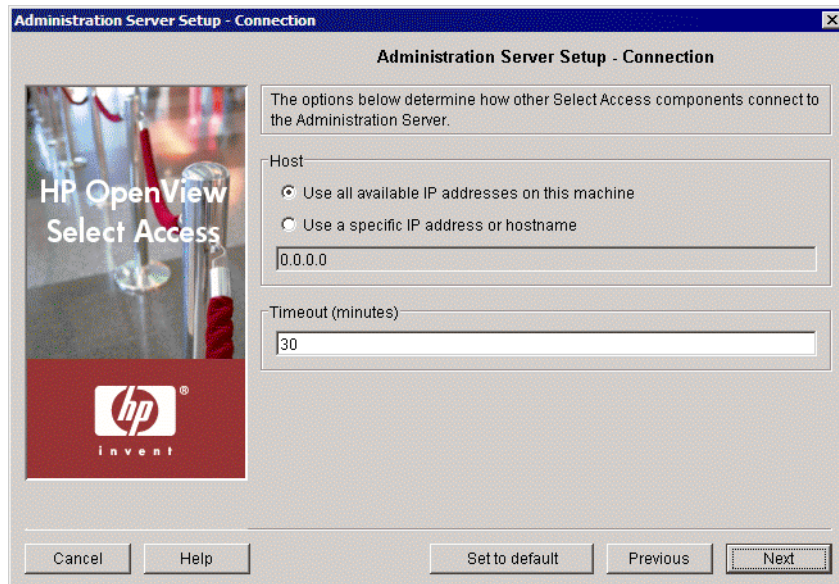


Figure 30: The Connection setup screen

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 71.

Configuring the Policy Builder administration modes

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

- **Administration:** For use exclusively by the Select Access super administrator(s), 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.

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

The **Administration** screen, shown in Figure 31, 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.



Figure 31: The Administration setup screen

To configure the Policy Builder administration modes


1. In the **Administration** group, specify the used to access the Policy Builder in full administration mode. By default, this mode uses port 9986.
2. In the **Administration Server** group, specifies 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 73.

Configuring the web-based administration services

The **Web Administration** setup screen, shown in Figure 32, allows you to configure the ports and service names for Select Access' web-based administration services.



Figure 32: The 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.

i 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 Registration/Self Management** 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 Self Administration.
 - **Registration Resource:** Specifies the path to the self-registration resource.
 - **Management Resource:** Specifies the path the to the self-management resource.
3. Click **Next**. The **SSL Server Certificate** setup screen appears. See *Setting up SSL connection handling* on page 74.

Setting up SSL connection handling

The **SSL Server Certificate** setup screen, shown in Figure 33, 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 33: The 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.
 - **Let Select Access handle SSL server certificate:** Optional. Choose this option if you want Select Access to manage the certificate.
 - **Import SSL server certificate:** Optional. Choose this option if you want to use your own certificate and key. Click the **Import SSL server 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 75.
 - If you are not using SSL, the **Policy Signing** setup screen appears. See *Configuring Policy Store data signing* on page 76.

Configuring the directory server's certificate

The **Directory Server Certificate** setup screen, shown in Figure 34, allows you to customize the verification of the certificate used by the directory server that holds Policy Store data.

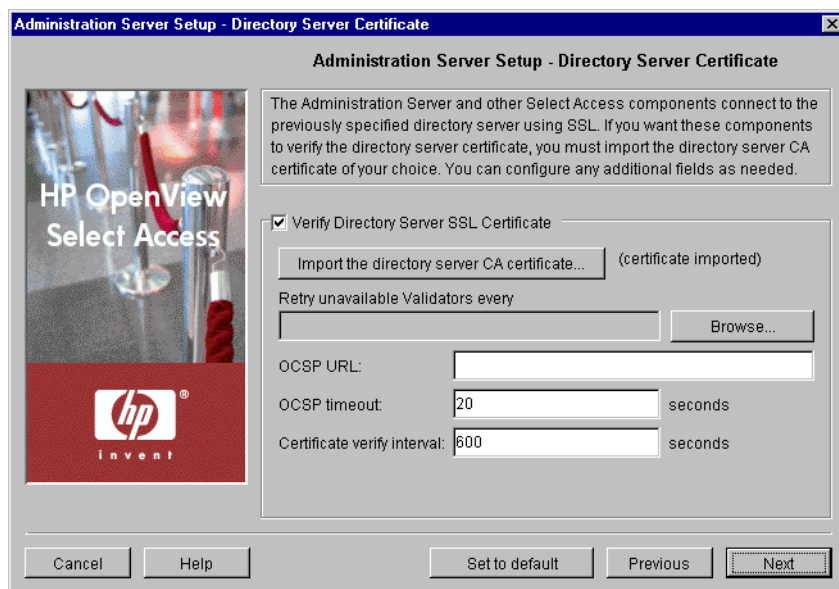


Figure 34: The Directory Server Certificate setup screen

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 76.

Configuring Policy Store data signing

The **Policy Signing** setup screen, shown in Figure 35, 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 35: The Policy Signing setup screen

To enable or disable policy signing

3. 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.
 - **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 PKCS12 certificate. Also enter the CN of the authorized administrator who has the authorization to sign data entries via Policy Builder in the **Data Signer CN** field. If you have correctly configured the **Import Signer CA** dialog, 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 entry contains a signer certificate, private key, and a CA certificate. Also ensure that CN in the **Data Signer CN** field matches the CN used in the subject field of the PKCS12 certificate.

For more details on signing policy data, see Chapter 4, *Managing your Policy Data*, in the *HP OpenView Select Access 6.0 Policy Builder Guide*.

4. 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 78.
 - 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 79.

Verifying the signer's certificate

The **Signer CA Certificate** setup screen, shown in Figure 36, 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.

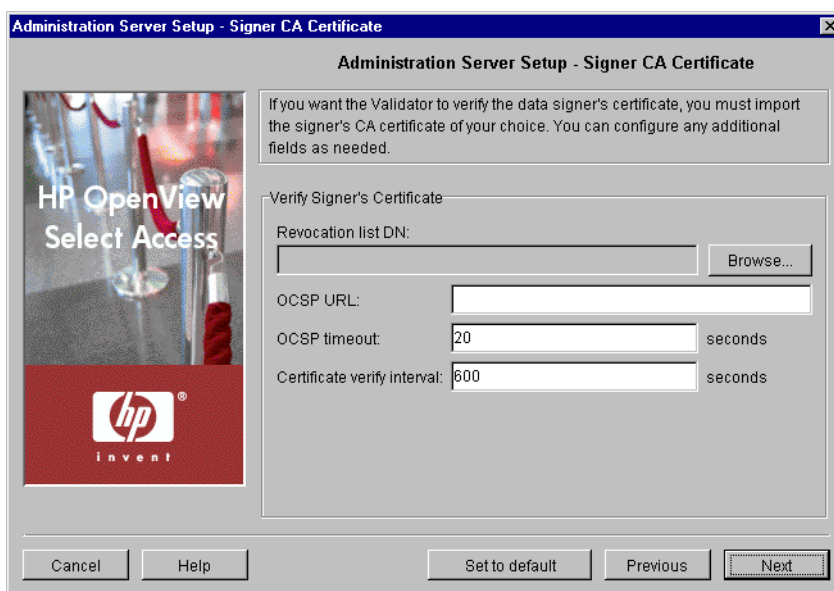


Figure 36: The Signer CA Certificate setup screen

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.

i 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 37, 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.

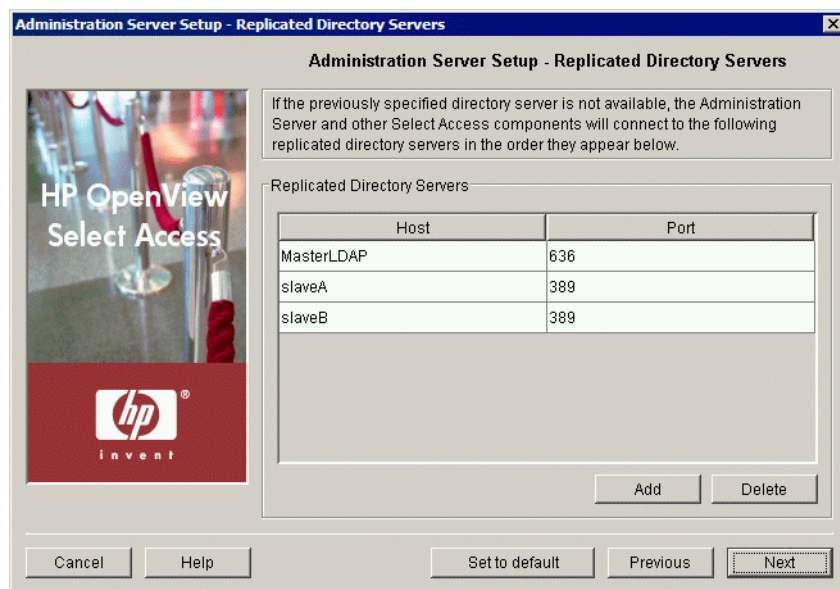


Figure 37: The Replicated Directory Servers setup screen

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 5, *Preconfiguring a directory server*, in the *HP OpenView Select Access 6.0 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 38, 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.

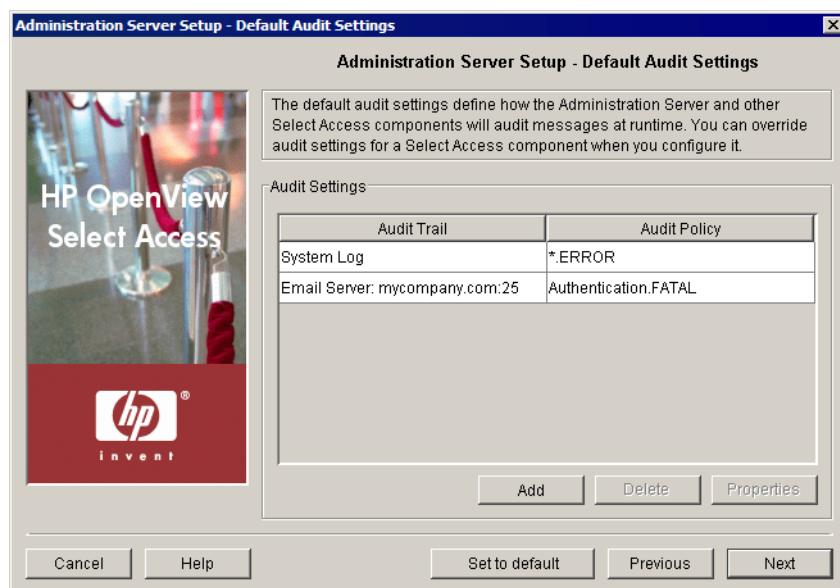


Figure 38: The Default Audit Settings setup screen

To configure 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.



Default 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.



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*.



The Administration server's Audit Policy can include both Policy and Operation components.



If you enable 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.

- To create or modify audit settings rows, click **Add** or **Properties** respectively. The **New Event Log** dialog 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 Event Log** dialog, 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 *Supported audit policy combinations* on page 113 and *Configuring an Audit Policy* on page 110.
 - 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 82.

Configuring database reporting

The Database Reporting setup screen, shown in Figure 39, allows you to set up a JDBC-compliant database if you intend to use it to write component runtime messages to it.

i 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 80 for details.

i 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.

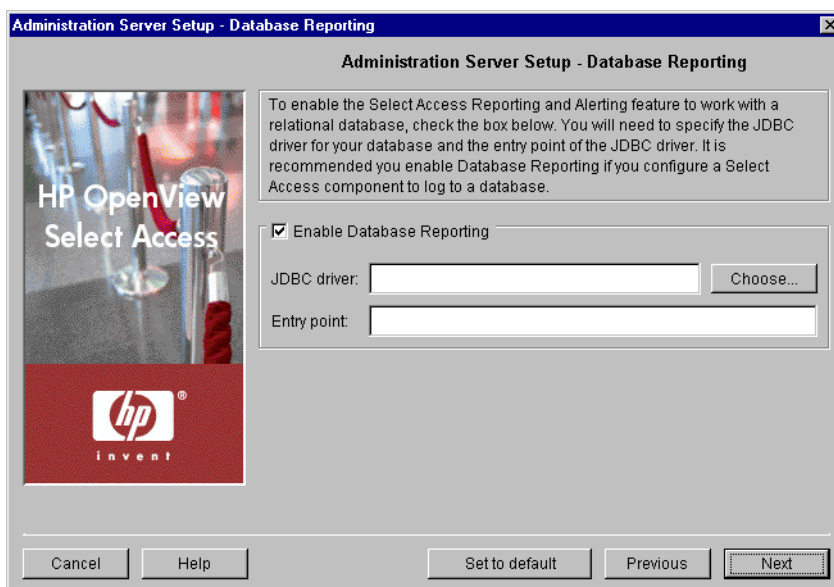


Figure 39: The Database Reporting setup screen

To configure database reporting

1. Customize any of the following as needed.

i If you enable database reporting, ensure you configure your database's tables correctly. To do this, run the corresponding SQL script installed with Select Access. For details, see *Configuring a database* on page 103.

- **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. Select Access components use this class to write events to the database.

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

i 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.

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 semicolon (;).

i 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"
```

- **Entry Point:** Enter the name of the JDBC Driver class name contained in the JDBC driver file you just defined.
-

i 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 83.

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.

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



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



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.

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 54.



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 84.

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 11, *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 users 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:* Are the certificates installed with Select Access. They include common CA certificates from authorities like:
 - Baltimore Technologies
 - Commercial Certification Authority
 - Deutsche Telekom
 - Entrust
 - EUnet International
 - First Data
 - IPS Servidores
 - Microsoft
 - Post.Trust
 - SecureNet
 - SIA Secure Client
 - TrustCenter
 - ValiCert
 - Certisign
 - CyberTrust
 - Digitrust
 - Equifax Secure Global eBusiness
 - FESTE
 - GlobalSign
 - KeyWitness
 - NetLock
 - Saunalahden Serveri
 - SecureSign
 - SwissKey
 - 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 86 in the *HP OpenView Select Access 6.0 Installation Guide*.

- *Custom certificates:* Are 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: CN=Baltimore Technologies Plc,OU=Engineering,O=Baltimore Technologies Plc,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 Trust Network,OU=(c) 1998 VeriSign Inc. - For authorized use only,OU=Class 4 Public Primary Certification Authority - G2,O=VeriSign Inc.,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 Trust Network,OU=(c) 1998 VeriSign Inc. - For authorized use only,OU=Class 4 Public Primary Certification Authority - G2,O=VeriSign Inc.,C=US
- CA Certificate: OU=VeriSign Trust Network,OU=(c) 1998 VeriSign Inc. - For authorized use only,OU=Class 3 Public Primary Certification Authority - G2,O=VeriSign Inc.,C=US
- CA Certificate: OU=VeriSign Trust Network,OU=(c) 1998 VeriSign Inc. - For authorized use only,OU=Class 3 Public Primary Certification Authority - G2,O=VeriSign Inc.,C=US
- CA Certificate: OU=VeriSign Trust Network,OU=(c) 1998 VeriSign Inc. - For authorized use only,OU=Class 2 Public Primary Certification Authority - G2,O=VeriSign Inc.,C=US
- CA Certificate: OU=VeriSign Trust Network,OU=(c) 1998 VeriSign Inc. - For authorized use only,OU=Class 2 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: OU=VeriSign Individual Software Publishers CA,O=VeriSign Inc.,L=Internet
- CA Certificate: OU=VeriSign Commercial Software Publishers CA,O=VeriSign Inc.,L=Internet
- CA Certificate: OU=VeriSign Commercial 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: EMAIL=certificate@trustcenter.de,OU=TC TrustCenter Class 3 CA,O=TC TrustCenter for Security in Data Networks GmbH,L=Hamburg,ST=Hamburg,C=DE
- CA Certificate: EMAIL=certificate@trustcenter.de,OU=TC TrustCenter Class 2 CA,O=TC TrustCenter for Security in Data Networks GmbH,L=Hamburg,ST=Hamburg,C=DE
- CA Certificate: EMAIL=certificate@trustcenter.de,OU=TC TrustCenter Class 1 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=00851000000500000192,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 RootCA3,O=Japan Certification Services Inc.,C=JP
- CA Certificate: CN=SecureSign RootCA2,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: 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: EMAIL=gold-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: EMAIL=info@valicert.com,CN=http://www.valicert.com/,OU=ValiCertClass 3 Policy Validation Authority,O=ValiCert Inc.,L=ValiCert Validation Network
- CA Certificate: EMAIL=info@valicert.com,CN=http://www.valicert.com/,OU=ValiCertClass 1 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

Configuring the Secure Audit server

The Secure Audit server is useful for monitoring stability, data integrity, and corporate security – all via a centralized server. You can configure your Select Access components, which act as clients to the server, to forward messages about:

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



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



You must configure and start the Secure Audit server before other Select Access components can log to it. Ensure the Secure Audit server is running before configuring components to use the Secure Audit server as their output target.

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 (that is, information, warning)

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

- Who has accessed a resource.

- What operations an administrator has performed during a given period of time.
- What Select Access components have generated errors.



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 9, *Creating reports from Secure Audit server output*, in the *HP OpenView Select Access 6.0 Policy Builder Guide*.

Note, however, that if you are using a signed audit log from a previous release, the log may not be accepted by Select Access 6.0 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 6.0 components from using signed logs prior to Patch 2.



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 to output events to different destinations than other Select Access components.

About client/server auditing with the Secure Audit server

Select Access components' common 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 16.

Table 16: Auditing overview

This step	For details, see...
<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"> – Separate the incoming messages into different files or databases on the Secure Audit server host – Forward certain messages to other Secure Audit servers. 	<p><i>To set up the Secure Audit server on page 94</i></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 Audit Settings 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 Audit Trail tab in the Audit Entry dialog.</p> <p>Note: 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><i>To set Policy Validator-specific audit settings on page 131</i></p> <p>OR</p> <p><i>To set enforcer-specific audit settings on page 160</i></p> <p>OR</p> <p><i>To set up the SAML server and SAML Enforcer plugin on page 178</i></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 to configure the Secure Audit server

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.
2. Click **Next** until you reach the Setup Tool’s **Secure Audit server** setup screen, as shown in Figure 40.

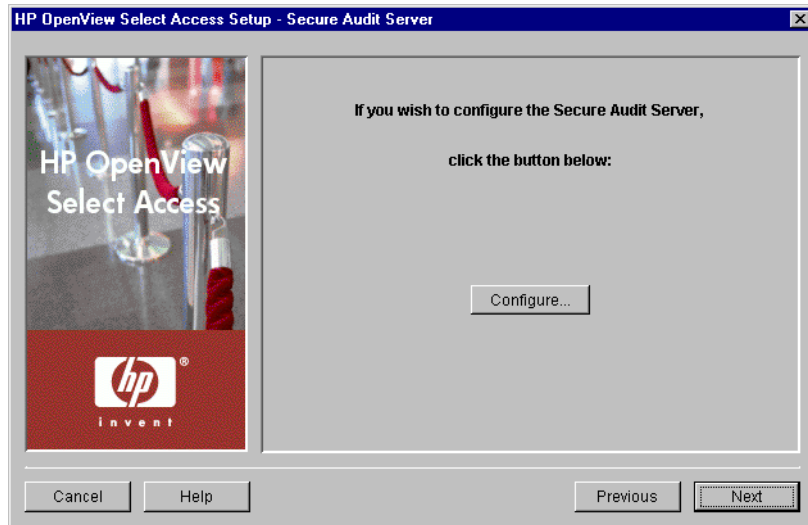


Figure 40: The Secure Audit server setup screen

3. Click the **Configure** button. The Secure Audit server setup process starts and the **Connection** setup screen appears.
4. Complete the setup screens of the Secure Audit server setup process, listed in Table 17, as necessary.

Table 17: Overview of Secure Audit server setup process

Setup screen	Description	Default value(s)
Connection 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 <i>Configuring the Secure Audit server connection information</i> on page 95.	auto-defined
Audit Settings setup screen	Allows you to configure audit settings specific to the Secure Audit server. See <i>Configuring server-specific audit settings</i> on page 96.	auto-defined to log all runtime errors
Audit Stream Signing 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 <i>Configuring audit stream signing</i> on page 97.	disabled

Table 17: Overview of Secure Audit server setup process

Setup screen	Description	Default value(s)
Finish setup screen	Allows you to commit your configurations settings to the Secure Audit server's bootstrap XML file, and automatically restart the server. See <i>Completing the Secure Audit server setup process</i> on page 99.	enables server restart

Configuring the Secure Audit server connection information

The **Connection** setup screen, shown in Figure 41, 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 41: The 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 5.0, 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 used by third-party applications.

If you are upgrading Select Access from a version previous to Select Access 5.0 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 96.

Configuring server-specific audit settings

The **Audit Settings** setup screen, shown in Figure 42, 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.

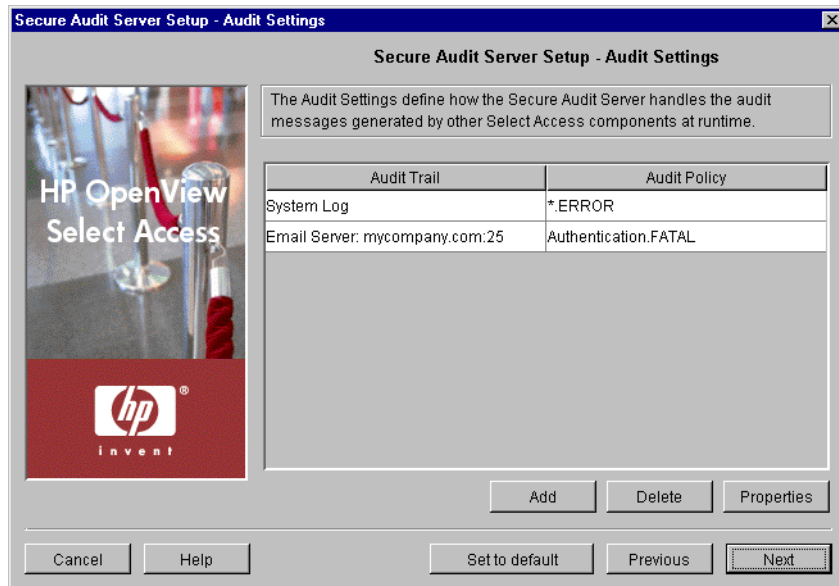


Figure 42: The Audit Settings setup screen

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 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 as necessary.
 - For information on configuring audit trail settings, see *Configuring an Audit Trail* on page 99
 - For information on setting audit policy, see *Configuring an Audit Policy* on page 110

When you configure the tabs of the **New Audit Entry** dialog, 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 97.
 - If you plan to output collected component logs to any other destination, skip to step *Completing the Secure Audit server setup process* on page 99.

Configuring audit stream signing

The **Audit Stream Signing** setup screen, shown in Figure 43, 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.

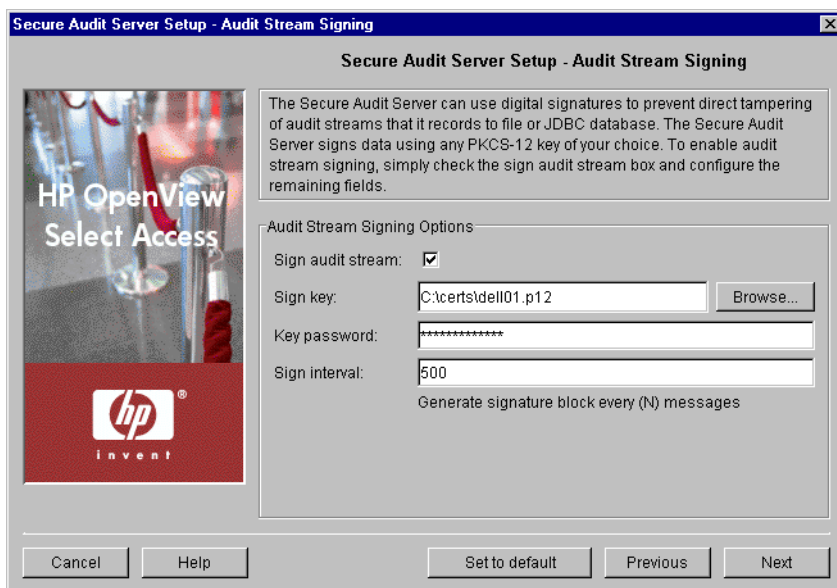


Figure 43: The Audit Stream Signing setup screen

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 the 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 one or more messages have someone has tampered with. 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 99.

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 also contains a configuration parameter that is not configurable by the Setup Tool: the Timeout parameter. The Timeout parameter specifies the amount of time a connection attempt to the Secure Audit server is made 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.



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.

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 54.

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 54.

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 appears displaying the **Audit Trail** tab as shown in Figure 44.

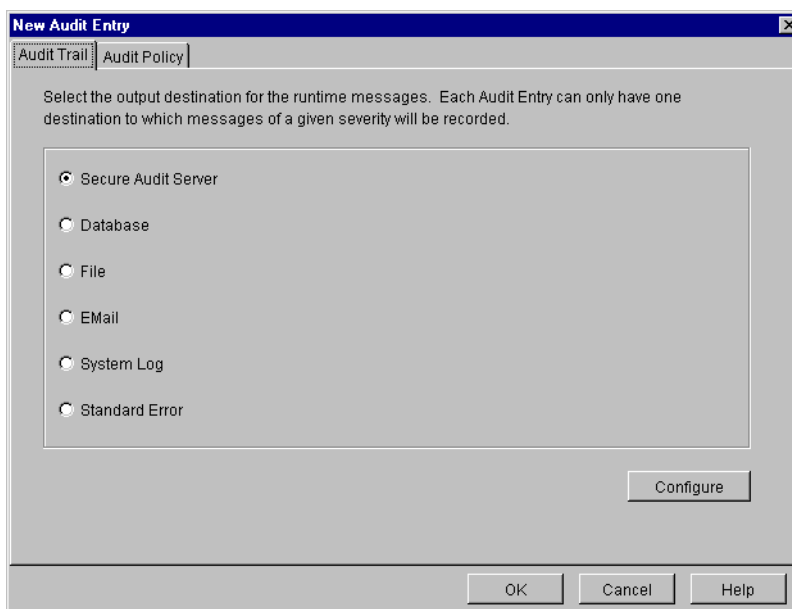


Figure 44: The Audit Trail tab

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 18: Configuring the Audit Trail tab

This output destination...	Does this...
Secure Audit Server	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.
Database	Outputs to a Java DataBase Connectivity (JDBC) compliant database.
File	Outputs to a text file. For example, you can send less important messages to a file to reduce network overhead.
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 since logs that only record a specific type of event are usually pooled before being forwarded to a single, centralized destination, as shown by the graphic below.

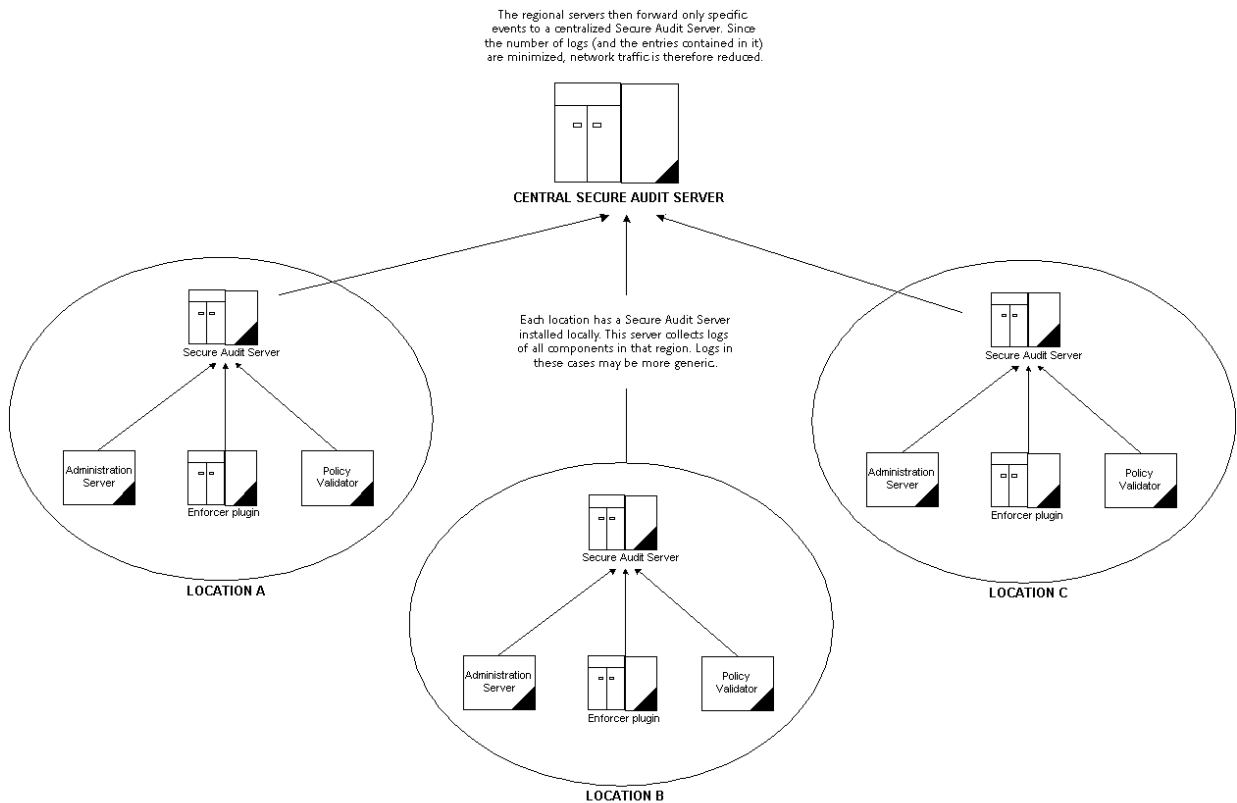


Figure 45: Secure Audit server pools forwarding events to central server

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.

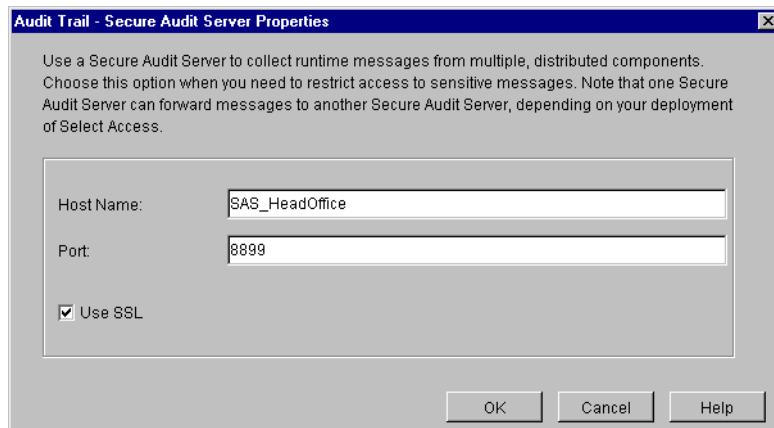


Figure 46: The Audit Trail—Secure Audit server Properties dialog box

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.



Using a database requires that you have set it up correctly. This entails enabling database reporting when you configured the Administration server when you performed a custom configuration. It also entails creating database tables correctly. For details, see *Creating database tables* on page 105. For more details on the conditions that allow you to create a report from your database, see Chapter 9, *Creating reports from Secure Audit server output*, in the *HP OpenView Select Access 6.0 Policy Builder Guide*.

To configure a database

1. Ensure you have done the following:
 - Run the correct SQL script for your database. For details, see *Creating database tables* on page 105.
 - Enabled database reporting when setting up the Administration server. For details, see *Configuring the Administration server* on page 59.
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.

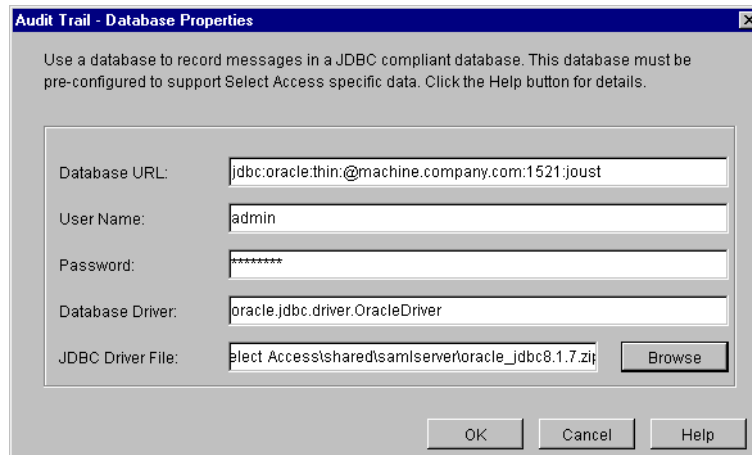


Figure 47: The Audit Trail—Database Properties dialog box

- 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


- In the **User Name** field, specify a username for this database. You need this to set up the driver.
- In the **Password** field, specify a password for this database. You need this to set up the driver.
- 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.




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

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.

 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.

For more details on how to create a report, see Chapter 9, *Creating reports from Secure Audit server output*, in the *HP OpenView Select Access 6.0 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.

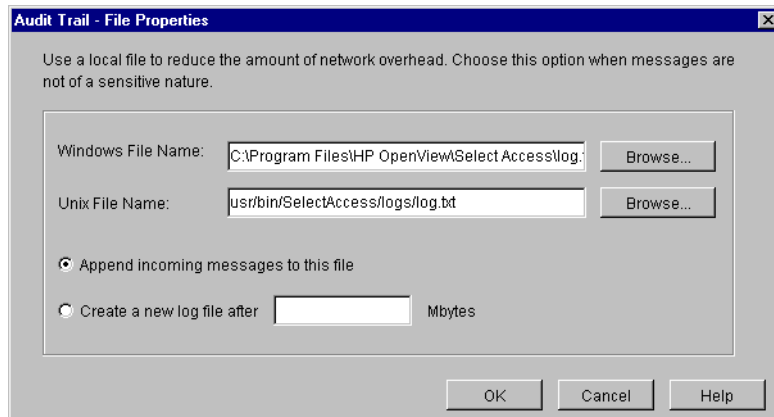


Figure 48: The Audit Trail—File Properties dialog box

2. In the **Windows/Unix File Name** fields, click **Browse** to specify the log file to which you want to record events. If the components are only running on one platform, you only need to specify a single filename.



Depending on the component you are configuring, you may not be able to use the **Browse** button if a network directory system is not available. Typically this occurs when a component is installed on a different computer than the one hosting the file. In this case, you must know the path to this file.

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 **E-Mail** option.
 - Click the **Configure** button.

The **Audit Trail—E-Mail Properties** dialog box appears.

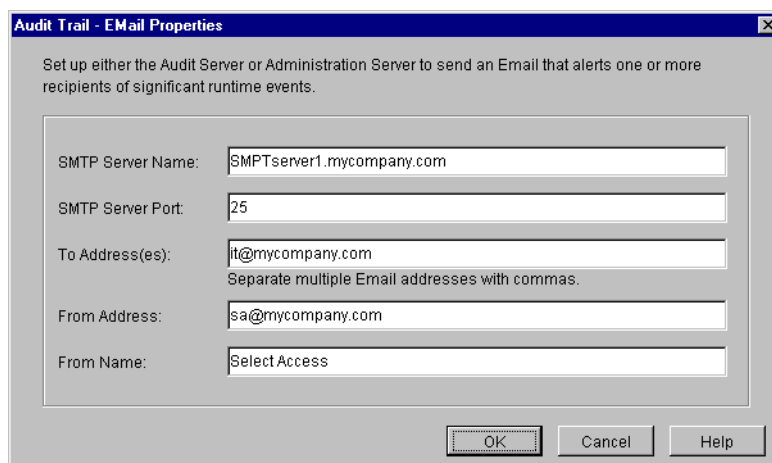


Figure 49: The **Audit Trail—E-Mail Properties** dialog box

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. The **Select Access** component sends the message when it triggers

an event. You can enter multiple email address by separating them with a comma (,).



If you incorrectly format an email address, or separate it with the wrong character, the Select Access highlights the line in red.

5. In the **From Address(es)** field, enter the email address that the component sends the message from when it triggers an event.



You can only enter one address in this field. If you enter more than one email address, the Select Access highlights the line in red.

6. In the **From Name** field, enter the sender alias that 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.
2. Select Access components automatically output events to this location depending on the host computer of the component:
 - Windows Event Log
 - Unix syslog
3. 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 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.

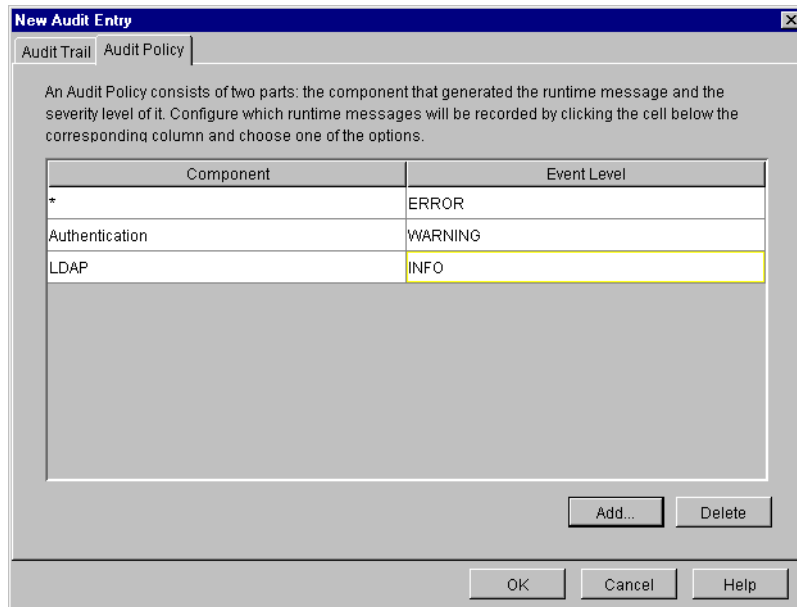


Figure 50: New Audit Entry dialog box: Audit Policy tab

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 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 user 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 user entry (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.
- **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.
- **SAML Out:** Records events and messages that relate to outgoing transfers of users from your `saml_out` servlet.
- **SAML In:** Records events and messages that relate to incoming transfers of users to your `saml_in` servlet.
- **SAML Responder:** Records other events and messages logged by your SAML server.
- **SAML Action:** A multipurpose channel for recording messages logged by other sub-component(s) of the SAML server.
- **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 respects to tamper-resistant logging, if you configure a Secure Audit server to sign its logs.

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.

Supported audit policy combinations

You can create different event logs that log different hierarchies and components of events and messages, as well as various event level combinations, depending on your business requirements and what information you are trying to capture.

The Table below outlines the kind of information recorded when you select various combinations.



Select Access does not use these **Component** and **Event Level** combinations: Certificate/Fatal, Authentication/Info, Cache/Fatal, Cache/Warning, Cache/Info, Query/Fatal, Query/Warning, System/Fatal, System/Info.

Table 19: Audit policy component and event level combinations

To capture this information...	Choose this component...	And this event level...
Policy Builder combinations		
Record startup and shutdown of the Policy Builder.	Operation	Info
Track who logs into and out of the directory server.	Admin Session	Info
Record changes made to: <ul style="list-style-type: none"> • Delegated administration • Log client configuration • Active Directory attributes 	Policy	Info

Table 19: Audit policy component and event level combinations (Continued)

To capture this information...	Choose this component...	And this event level...
Record modification to: <ul style="list-style-type: none"> • Group membership • User Tree or Resource Tree entries and folder properties • Authentication servers • Access rules 	Policy	Info
Secure Audit server combinations		
Record initialization errors.	Operation	Warning
Track log messages' process errors.	Operation	Error
Record startup and shutdown of the Secure Audit server.	Operation	Info
Record Changes made to the Secure Audit server configuration.	Admin Session	Info
Policy Validator combinations		
Track when the Policy Validator flushes the cache.	Policy	Debug
Record errors caused by: <ul style="list-style-type: none"> • The creation of OCSP requests • The inability to find CA certificates • The inability to find the issuer • Certificate expiry • Failure to connect to verifier 	Certificate	Error
List problems such as: <ul style="list-style-type: none"> • Invalid status times • Nonce is missing from a response • Failure to find certificate in directory server • Failure to find CRL 	Certificate	Warning
Inform you when: <ul style="list-style-type: none"> • Someone installs a CA certificate • The Policy Validator validates a response • The DN of a certificate on the directory server 	Certificate	Info

Table 19: Audit policy component and event level combinations (Continued)

To capture this information...	Choose this component...	And this event level...
Track when: <ul style="list-style-type: none"> • Certificate cache reloads • Certificate lookup in the directory server is successful 	Certificate	Debug
Describe failures to: <ul style="list-style-type: none"> • Generate RSA SecurID key • Make a new secret 	Authentication	Fatal
List errors caused by: <ul style="list-style-type: none"> • SSL certificate not initializing • Mismatch between private key and certificate public key 	Authentication	Error
Inform you when: <ul style="list-style-type: none"> • No secret found for directory server • User Tree entry not found by certificate authenticator 	Authentication	Warning
Tracking the: <ul style="list-style-type: none"> • Directory server's search for a certificate • Creation of new registration secret or expiry of old one • Verification process of the User ID and password during registration 	Authentication	Debug
Record failures to find message request handler during cache cleanup.	Cache	Error
Track things like: <ul style="list-style-type: none"> • Disabling of cache cleanup • Initializing of cache • Changing configuration (intervals or percentages) 	Cache	Debug
Record failures to: <ul style="list-style-type: none"> • Find Policy Validator plugin • Open configuration file or use parameters (invalid) • Initialize Policy Validator subsystem libraries 	Operation	Fatal

Table 19: Audit policy component and event level combinations (Continued)

To capture this information...	Choose this component...	And this event level...
Record problems such as: <ul style="list-style-type: none"> • Registration password too short • Log configuration not parsed • Invalid RADIUS server configuration 	Operation	Error
Record problems such as: <ul style="list-style-type: none"> • Policy Validator plugin not loaded • Policy Validator configuration contains requests for too many threads 	Operation	Warning
Record data such as: <ul style="list-style-type: none"> • Invalid encryption data format for directory server logon password • Log configuration not found • Policy Validator threads starting to handle connections • startup or shutdown of a Policy Validator 	Operation	Info
Track things like: <ul style="list-style-type: none"> • Verification of policy signature manifest • Group or role for user lookups • Construction of Policy Validator plugins • Nested invocation of rules and subrules 	Operation	Debug
List access information a such as: <ul style="list-style-type: none"> • When an ALLOW was returned • The user name, if it is known • The resource that the user accessed 	Policy	Info
List access information a such as: <ul style="list-style-type: none"> • When a DENY was returned • The user name, if it is known • The resource that the user attempted to access 	Policy	Warning
List queries missing XML start tag.	Query	Error
Display requests and responses in XML	Query	Debug

Table 19: Audit policy component and event level combinations (Continued)

To capture this information...	Choose this component...	And this event level...
List problems such as: <ul style="list-style-type: none"> • Memory allocation failure during query processing • Failure to find Windows registry key • Missing registry values • Improperly formatted registry values 	System	Error
Display registry values.	System	Debug
List invalid directory server connection parameters, as well as failure to connect to directory server.	LDAP	Fatal
Record failures to: <ul style="list-style-type: none"> • Decode the DN provided by the directory server • Add user to group during registration 	LDAP	Error
Record failures to: <ul style="list-style-type: none"> • Logon • Find entry on Resource Tree • Find policy data signing information. 	LDAP	Warning
Track all successful: <ul style="list-style-type: none"> • Logons • Policy signing enabled or disabled 	LDAP	Info
Record failures to: <ul style="list-style-type: none"> • Find parent • Use server authentication for passwords 	LDAP	Debug
Enforcer plugin combinations		
Record problems such as: <ul style="list-style-type: none"> • Enforcer API initialization errors • Enforcer configuration initialization errors • Unexpected loss of a connection to a Policy Validator 	Enforcer	Error
Inform you of every Enforcer plugin startup	Enforcer	Info

Table 19: Audit policy component and event level combinations (Continued)

To capture this information...	Choose this component...	And this event level...
Track things like: <ul style="list-style-type: none"> • SSO activities (redirects, finding SSO nonces) • Opening new Policy Validator connections 	Enforcer	Debug
SAML combinations		
<ul style="list-style-type: none"> • Records users who have been sent to a SAML server that accepts in-bound transfers 	SAML Out	Info
<ul style="list-style-type: none"> • Records users who have been transferred and accepted by a Select Access SAML server that accepts in-bound transfers 	SAML In	Info
<ul style="list-style-type: none"> • Records messages that occur as a result of a SAML server sending out-bound transfers. (For example, what the assertion artifact is.) 	SAML Responder	Warning
<ul style="list-style-type: none"> • Records messages that occur as a result of a SAML server accepting in-bound or sending out-bound transfers. (For example, whether or not a connection was successful or not.) 	SAML Action	Warning
System combinations		
Record errors caused by the writing of keys and/or values to the Windows registry	System	Debug
Describe problems such as: <ul style="list-style-type: none"> • Failing to allocate and/or read from memory • Failure to find a needed key in the Windows registry • The occurrence of an unknown exception 	System	Error
Inform you of any Windows registry does not contain an expected key and/or value	System	Warning

Starting the Secure Audit server

If you do not start the Secure Audit server immediately after you configure it, you need to use an alternative method. You must stop and restart the Secure Audit server if:

- You change the Secure Audit server's configuration.
- You change configuration details for the Administration server.
- You change the date and/or time on the computers where the Secure Audit server clients are running.

Irrespective of the platform you are running the Secure Audit server on, there are two startup methods:

- *Starting it automatically:* So it starts when the host computer starts. By default, the Setup Tool configures the Secure Audit server to start this way.
- *Starting it manually:* So it runs only when you want it to. On Windows, you can run the Secure Audit server from the command line, whereas on Unix, you must use the `auditserver` start script.

Windows—starting the Secure Audit server manually

You can start the Secure Audit server manually on Windows by running it from the command line using the startup command with any combination of options.

To start the Secure Audit server from the 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 20 describes these options.



If you use any of these options, they override any other logging configuration settings.

Table 20: 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><install_path>\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.

Unix—starting the Secure Audit server manually

You can use the `auditserver` script to start and stop the Secure Audit server.

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`

Configuring the Policy Validator

The Policy Validator is Select Access's evaluation engine. It decides when and how to authorize user access to a given resource.

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 51, 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 6.0 Developer's Tutorial Guide* and the *HP OpenView Select Access 6.0 Developer's Reference Guide*.

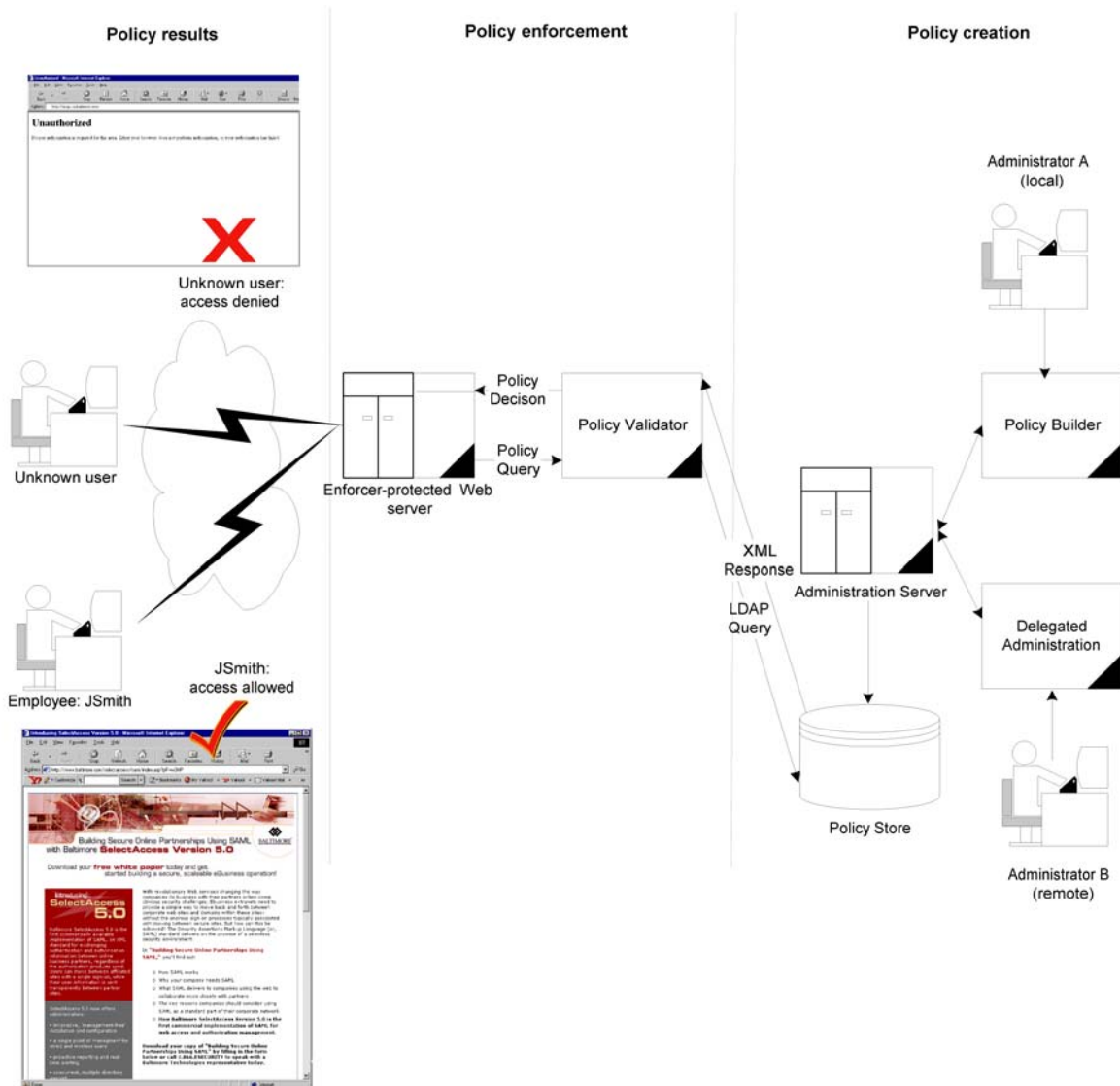


Figure 51: How the Policy Validator works

If the Policy Validator authenticates a user, it generates and signs a cookie. When that user 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 user 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 the wrong access decisions 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 5, *Modifying components' central configuration parameters*, in the *HP OpenView Select Access 6.0 Policy Builder Guide*.

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 over 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 21 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 rerunning 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 52: The 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 21, as necessary.

Table 21: Overview of Policy Validator setup process

Setup screen	Description	Default value(s)
Contact the Administration Server 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 <i>Connecting to the Administration Server</i> on page 126.	auto-defined
General setup screen	Allows you to choose one of two setup types: <ul style="list-style-type: none"> • Typical: Use HP's recommended setup values. • Custom: Modify the recommended values to meet the needs of your network and/or business environment. See <i>Choosing your setup type</i> on page 127.	Typical
Address, Port and ID setup screen	Displayed for Custom setup type only. Allows you to define the Policy Validator connection parameters. See <i>Setting connection parameters for the Policy Validator</i> on page 129.	auto-defined
Audit Settings setup screen	Displayed for Custom setup type only. Allows you to configure audit settings specific to the Policy Validator. See <i>Configuring validator-specific audit settings</i> on page 130.	inherit common settings defined by the Administration server
Secure User Credentials 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 users without requiring them to provide user credentials each time they access a Select Access-protected resource. See <i>Defining data encryption settings</i> on page 131.	auto-defined
Password Dictionary 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 user passwords from including words defined in that file. See <i>Specifying a password dictionary</i> on page 133.	no dictionary used

Table 21: Overview of Policy Validator setup process

Setup screen	Description	Default value(s)
Tuning Parameters 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 <i>Tuning your Policy Validator</i> on page 133.	auto-defined
Finish setup screen	Allows you to commit your configurations settings to the Policy Store and the Policy Validator's bootstrap XML file, and to automatically start the Policy Validator. See <i>Completing the Policy Validator setup process</i> on page 135.	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 53, 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.

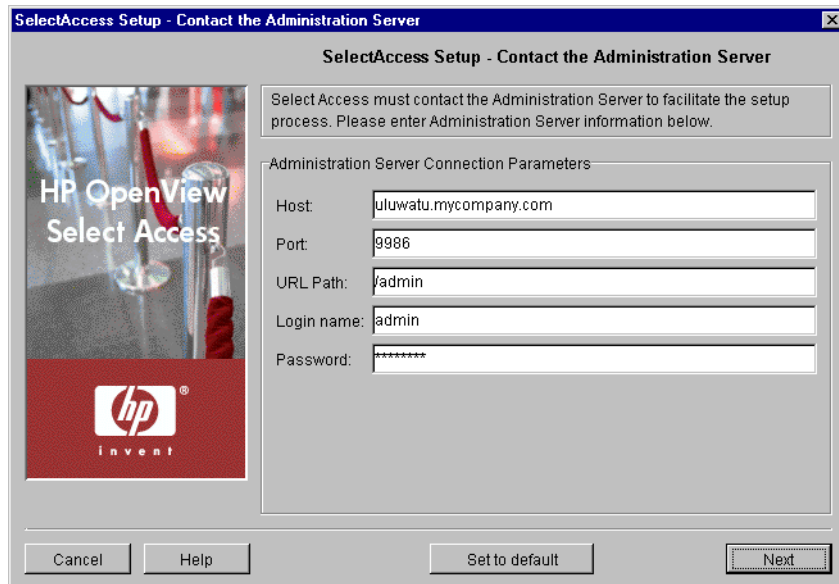


Figure 53: The Contact the Administration Server setup screen

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 user name to log 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.
3. Click **Next**. At this point, 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 54, allows you to choose whether you want to perform a **Typical** or a **Custom** setup.



Figure 54: The 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.
 For information on how to avoid regeneration when you need reinstall a component, see Chapter 9, *Understanding certificate-based authentication*, in the *HP OpenView Select Access 6.0 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 Policy Validator setup process* on page 135.
- 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 129.

Setting connection parameters for the Policy Validator

The **Address, Port and ID** setup screen, shown in Figure 55, allows you to define connection information for the Policy Validator.

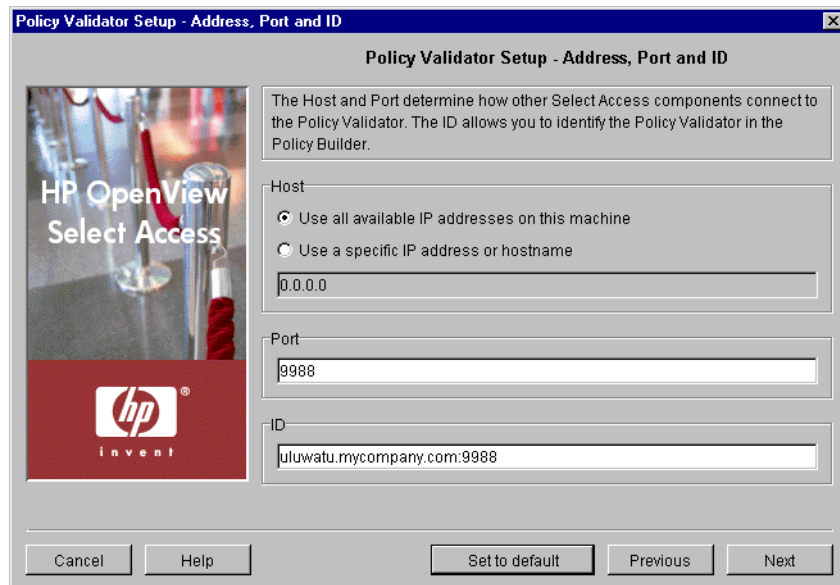


Figure 55: The Address, Port and ID setup screen

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 rerunning the Setup Tool for each plugin.

- **Host:** Required. Choose which IP address Select Access components need to connect to the host computer of the Policy Validator.

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 Policy Validator ID. Select Access components use this 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. 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 130.

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 56, allows you to create custom audit settings for a specific Policy Validator, overriding the common settings.

i 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 56: The 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 9, *Creating reports from Secure Audit server output*, in the *HP OpenView Select Access 6.0 Policy Builder Guide*.

- a. To create or modify audit settings rows, click **Add** or **Properties** respectively. The **New Audit Entry** dialog 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, 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 *Supported audit policy combinations* on page 113 and *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 User Credentials** setup screen appears. See *Setting connection parameters for the Policy Validator* on page 129.

Defining data encryption settings

The **Secure User Credentials** setup screen, shown in Table 57, allows you to configure the digital signature settings the Policy Validator needs to generate cookies and nonces. The Policy Validator uses cookies to create user 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 *Understanding nonces and cookies* on page 126 of the *HP OpenView Select Access 6.0 Network Integration Guide*.



Figure 57: The Secure User 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 User 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, users 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, a user has to access the Web site after she has authenticated 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 133.

Specifying a password dictionary

The **Password Dictionary** setup screen, shown in Table 58, allows you to specify the file that acts as your password dictionary. The password dictionary is a plain text file of words that users 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.

i The Policy Validator performs case-insensitive dictionary checks.

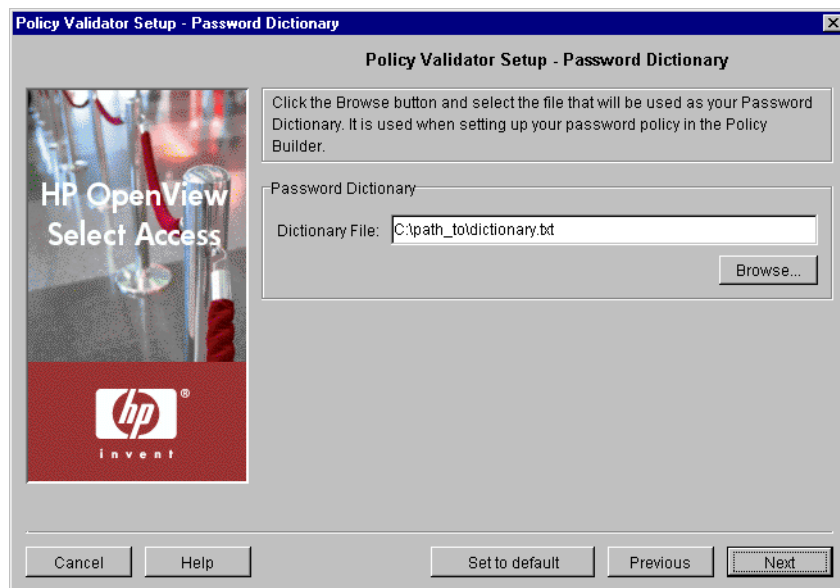


Figure 58: The Password Dictionary setup screen

To select a password dictionary

1. Locate the path to the file that acts as your password dictionary.
2. Click **Next**. The **Tuning Parameters** setup screen appears. See *Tuning your Policy Validator* on page 133.

Tuning your Policy Validator

The **Tuning Parameters** setup screen, shown in Figure 59, 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.

i Text on the **Tuning Parameters** setup screen appear bolded and italicized if the Policy Validator you are currently configuring has any override values set for it. The remaining parameters are those that are shared by all Policy Validators.

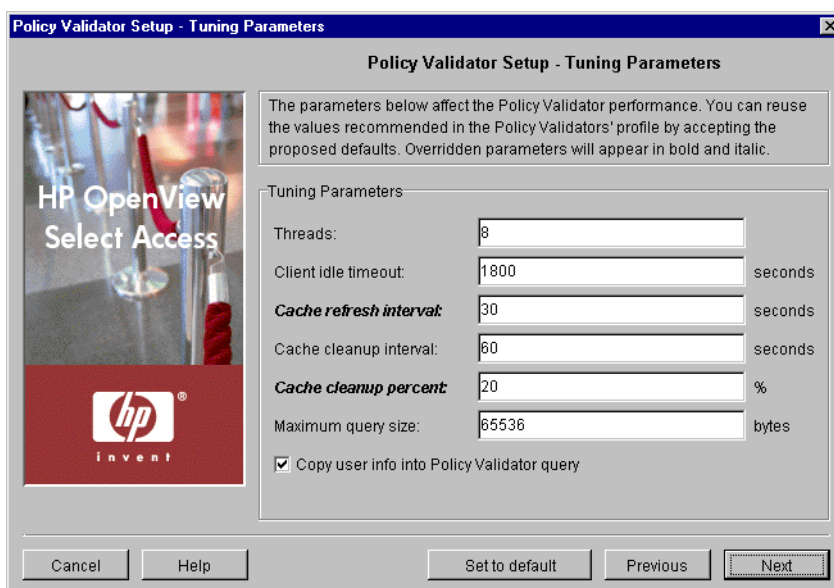


Figure 59: The Tuning Parameters setup screen

To tune your Policy Validator

1. Review HP's recommended values. To customize these values, modify fields in the **Tuning Parameters** group as needed.

i If you are creating override settings, they take precedence over group values, even if an administrator changes group values with the Policy Builder.

- **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.
- **Cache refresh interval:** Optional. The interval, in seconds, that Policy Validator refreshes its cached user 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.

i Use the Policy Builder to clear the cache when you alter policy data or add new user entries. This ensures that the Policy Validator updates the user/policy data. For details, see *Updating policy data cached by the Policy Validator* on page 218 in the *HP OpenView Select Access 6.0 Policy Builder Guide*.

- **Cache cleanup interval:** Optional. The interval, in seconds, that Policy Validator clears unused user entries from its cache. The default is 60 seconds.

- **Cache cleanup percent:** Optional. The percentage of the cache that the Policy Validator checks for unused entries.
- **Maximum query size:** Optional. The size limit of XML queries allowed.
- **Copy user info into Validator query:** Optional. Makes the attribute and value pairs of a user 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 135.

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.
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 54.

Starting the Policy Validator

If you do not start the Policy Validator immediately after you configure it, you need to use an alternative method. You must stop and restart the Policy Validator if:

- 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.

Irrespective of the platform you are running the Policy Validator on, there are two startup methods:

- *Starting it automatically:* so it runs when you boot the host computer. By default, the Setup Tool configures the Policy Validator to start this way.
- *Starting it manually:* It runs only when you want it to. On Windows, you can run the Policy Validator from the command line, whereas on Unix, you must use the `validator` startup script.

Windows—starting the Policy Validator manually

You can start the Policy Validator manually on Windows by running it from the command line using the startup command with any combination of options.



When you run the Policy Validator from the command line, all your password management settings appear. Gauge the security implications of this accordingly. For details on managing user passwords, see *Managing a user's account* on page 158 and *Setting up and maintaining password management* on page 161 of the *HP OpenView Select Access 6.0 Policy Builder Guide*.

To start the Policy Validator 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:

```
validator [options]
```

 where `[options]` are the command line parameters available to you. Table 22 describes these options.



If you use any of these options, they override any other logging configuration settings.

Table 22: 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. Note: 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. Note: 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.
-N service_name	Returns the Windows service name and exits.
-n server_threads	Specifies the number of server threads
-p server_port	Specifies the server port.
-t	Enables the tracing of requests.
-U	Uninstalls Policy Validator as a Windows service. Note: To confirm that the uninstaller has removed the service, close and reopen the Services dialog.
-v	Returns the version number of Policy Validator and exits.

Unix—starting the Policy Validator manually

You can use the `validator` script to start and stop the Policy Validator:

1. To start the Policy Validator, enter the following:
`<install_path>/validator start`
2. To stop the Policy Validator, enter the following:
`<install_path>/validator stop`

Uninstalling the Policy Validator

You can uninstall the Policy Validator using the uninstaller shipped with Select Access. For details, see *Uninstalling Select Access* on page 234.



For Unix users, run the uninstaller as root to ensure that it removes all files completely.

Configuring the Enforcer plugins

The Enforcer plugin acts as an intermediary between the user and the service it protects content on.

How Enforcer plugins work

All Enforcer plugins are responsible for:

- Examining the XML-based response from the Policy Validator
- Enforcing the authorization decision contained in the response
- Querying users for additional authentication information (for example, secret, password, username, 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 5, *Modifying components' central configuration parameters*, in the *HP OpenView Select Access 6.0 Policy Builder Guide*.

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 over 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 24 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, etc. 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.

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 23 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 23: Enforcers configured using the Select Access Setup Tool

Enforcer Type	Description
Enforcers that have an enforcer-specific setup wizard:	
Sun ONE (iPlanet) Enforcer plugin	Secures the Sun ONE Web server (formerly the iPlanet Web server)
Apache Enforcer plugin	Available on Unix only. Secures any version of the Apache Web server.
IBM HTTPD Enforcer plugin	Available on Windows only. Secures the IBM HTTPD Web server.
IIS Enforcer plugin	Secures the IIS Web server.
WSE Enforcer plugin	Secures .NET web services.
Axis Enforcer plugin	Secures Java web services.
Enforcers that require you to run the Generic setup	
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.	



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.

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 rerunning 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 5, *Modifying components' central configuration parameters*, in the *HP OpenView Select Access 6.0 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.

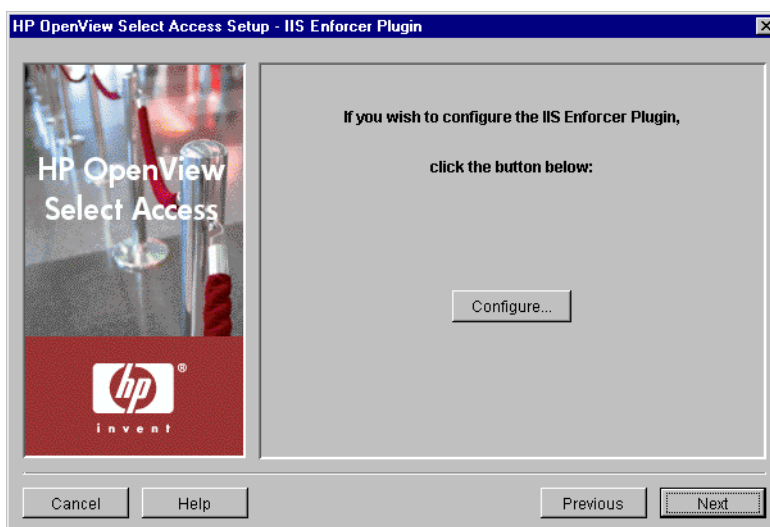




Figure 60: The Enforcer plugin setup screen

3. If you are configuring the Generic Enforcer plugin setup wizard, enter the path and filename in which the `enforcer.xml` file will be stored.

 Each Enforcer plugin must have its own bootstrap file. If you are configuring more than one Enforcer plugins 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 61.

 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 24, 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 24 identifies which plugins the task is applicable to.

Table 24: Overview of Enforcer plugin setup process

Setup screen	Description	Default value(s)
Contact the Administration Server 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 <i>Connecting to the Administration Server</i> on page 146.	auto-defined
General setup screen	Allows you to choose one of two setup types: <ul style="list-style-type: none"> • Typical: Use HP's recommended setup values. • Custom: Modify the recommended values to meet the needs of your network and/or business environment. See <i>Choosing your setup type</i> on page 147.	Typical

Table 24: Overview of Enforcer plugin setup process

Setup screen	Description	Default value(s)
ID setup screen	<p>Displayed for a Custom setup of all Enforcer plugin types.</p> <p>Allows you to define an enforcer ID which is used to identify the Enforcer plugin. See <i>Defining an Enforcer plugin ID</i> on page 148.</p>	auto-defined
Single DNS domain SSO setup screen	<p>Displayed for a Custom setup of all Enforcer plugin types excluding the Axis and WSE plugins.</p> <p>Allows you to allows you to identify the domain name across which users authenticate only once – even though they access resources on multiple subdomains. See <i>Setting up single domain single sign-on</i> on page 149.</p>	not enabled
Multiple DNS domain SSO setup screen	<p>Displayed for a Custom setup of all Enforcer plugin types excluding the Axis and WSE plugins.</p> <p>Allows you to set up SSO across multiple domains (multidomain SSO by creating a protected domains list that identifies the domains users can access without being required to reauthenticate with each new server. See <i>Setting up multidomain single sign-on</i> on page 151.</p>	not enabled
Sign SOAP XML setup screen	<p>Displayed for a Custom setup of the WSE Enforcer plugin.</p> <p>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 <i>Setting up SOAP message signing</i> on page 152.</p>	not enabled
Encrypt SOAP XML setup screen	<p>Displayed for a Custom setup of the WSE Enforcer plugin.</p> <p>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 <i>Setting up SOAP message encrypting</i> on page 154.</p>	not enabled

Table 24: Overview of Enforcer plugin setup process


Setup screen	Description	Default value(s)
Ignored Filenames setup screen	<p>Displayed for a Custom setup of all Enforcer plugin types excluding the WSE Enforcer plugin.</p> <p>Allows you to create a list of files to which access does not need to be secured. See <i>Setting up SOAP message signing</i> on page 152.</p>	not enabled
Passthrough Domains setup screen	<p>Displayed for a Custom setup of all Enforcer plugin types.</p> <p>Allows you to create a list of domains to which access does not need to be secured. See <i>Setting up a list of pass-through domains</i> on page 158.</p>	not enabled
Audit Settings setup screen	<p>Displayed for a Custom setup of all Enforcer plugins.</p> <p>Allows you to configure audit settings specific to the Enforcer plugin. See <i>Configuring enforcer-specific audit settings</i> on page 159.</p>	inherit common settings defined by the Administration server
Validators setup screen	<p>Displayed for a Custom setup of all Enforcer plugins.</p> <p>Allows you to select which Policy Validators the Enforcer plugin uses to authenticate users and authorize resource requests. You can also establish whether to use round-robinning to share loads among the Policy Validators you define. See <i>Configuring Policy Validator settings</i> on page 161.</p>	<p>auto-defined to use all runtime-available Policy Validators listed in the Policy Store.</p> <p>Load sharing is enabled.</p>
NAT setup screen	<p>Displayed for a Custom setup of all Enforcer plugins.</p> <p>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 <i>Mapping Policy Validators to NAT addresses</i> on page 163.</p>	not enabled
Tuning Parameters setup screen	<p>Displayed for a Custom setup of all Enforcer plugins.</p> <p>Allows you to specify tuning parameters so you can configure how the Enforcer plugin performs at runtime. See <i>Tuning your Enforcer plugin</i> on page 164.</p>	auto-defined


Table 24: Overview of Enforcer plugin setup process

Setup screen	Description	Default value(s)
Finish/Update Configuration setup screen (for the WSE Enforcer plugin)	Allows you to commit your configurations 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 upon startup. See <i>Completing the Enforcer plugin setup process</i> on page 167.	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 61, 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.

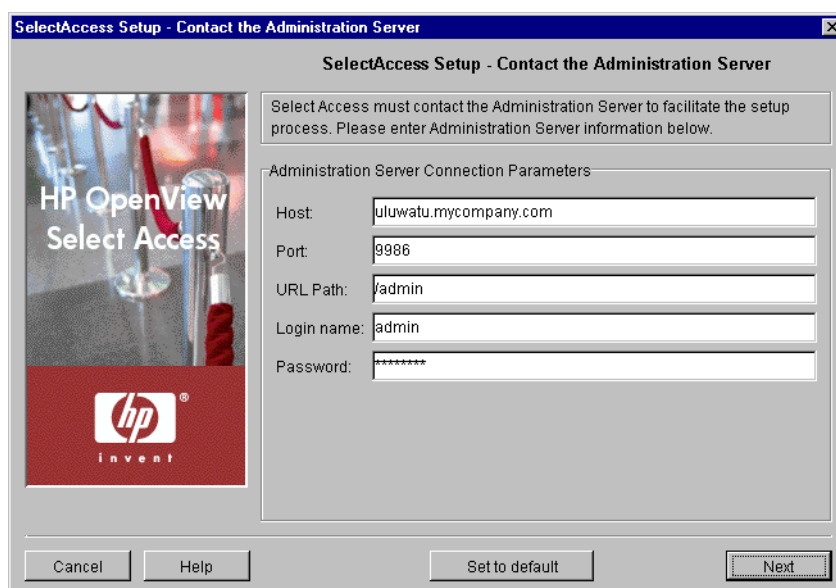


Figure 61: The Contact the Administration Server setup screen

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 user name to log 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 62, allows you to choose whether you want to perform a **Typical** or a **Custom** setup.

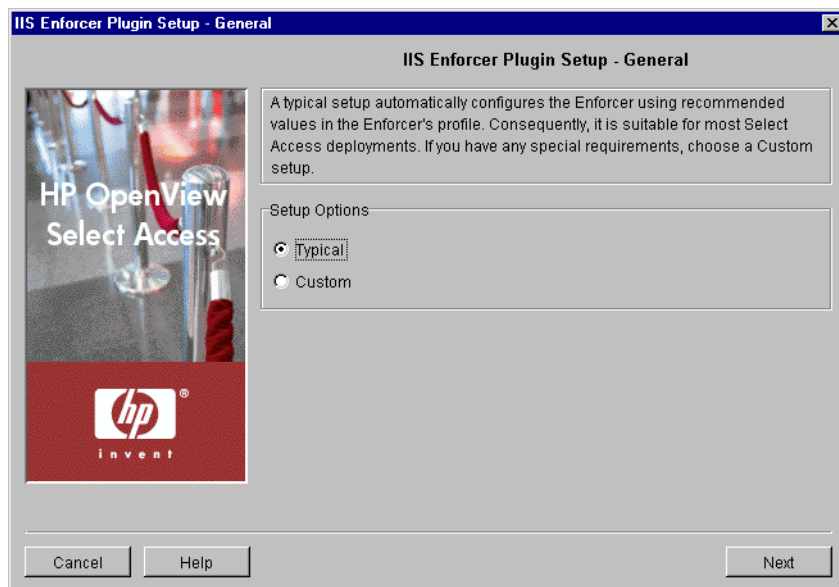


Figure 62: The General setup screen

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 Chapter 9, *Understanding certificate-based authentication*, in the *HP OpenView Select Access 6.0 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/Update Configuration** screen appears. See *Completing the Enforcer plugin setup process* on page 167.
 - If you are performing a **Custom** setup, the **ID setup** screen appears. See *Defining an Enforcer plugin ID* on page 148.

Defining an Enforcer plugin ID

The **ID setup** screen, shown in Figure 63, 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.

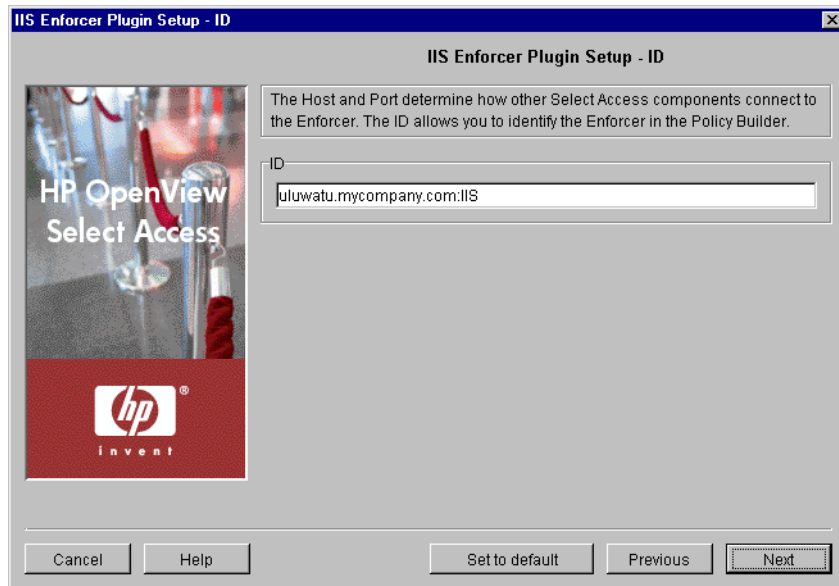


Figure 63: The ID setup screen

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 ONE (iPlanet), Apache, IBM HTTPD, IIS, or Generic Enforcer plugin, the **Single DNS Domain SSO** setup screen appears. See *Setting up single domain single sign-on* on page 149.
 - If you are configuring the WSE Enforcer plugin, the **Sign SOAP XML** setup screen appears. See *Setting up SOAP message signing* on page 152.
 - If you are configuring the Axis Enforcer plugin, the **Ignored Filenames** setup screen appears. See *Setting up a list of ignored filenames* on page 155.

Setting up single domain single sign-on

The **Single DNS Domain SSO** setup screen, shown in Figure 64, allows you to set a cookie domain. Once set, your users only need to be

authenticated once to gain access to all subdomains of a single DNS domain.

i This screen only appears if you are configuring one of the following enforcers: Sun ONE (iPlanet), Apache, IBM HTTPD, IIS, or Generic.

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



Figure 64: The Single DNS Domain SSO setup screen

To set up single domain single sign-on

1. If you want your users 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`


i The cookie domain you enter is a single DNS domain; all subdomains share the same cookie that the Policy Validator generates.


For details on how cookies are used with SSO, see *Understanding nonces and cookies* on page 126 of the *HP OpenView Select Access 6.0 Network Integration Guide*.

2. Click **Next**. The **Multiple DNS Domain SSO** setup screen appears. See *Setting up multidomain single sign-on* on page 151.

Setting up multidomain single sign-on

The **Multiple DNS Domain SSO** setup screen, shown in Figure 65, 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 ONE (iPlanet), Apache, IBM HTTPD, IIS, or Generic.

 Multidomain SSO does not apply to partner organizations or affiliates. It only applies to your network domains on Enforcer plugin-protected Web servers. To set up SSO with your partners, see *To set up the SAML server and SAML Enforcer plugin* on page 178.

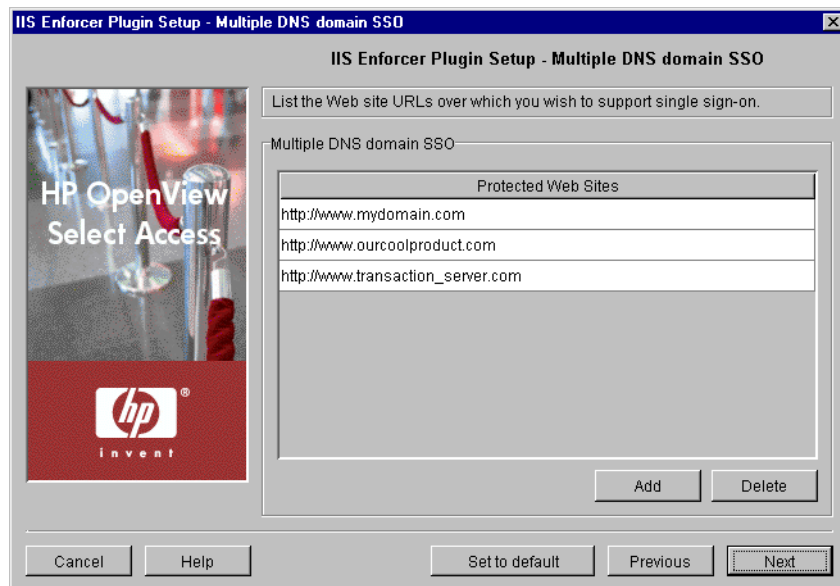


Figure 65: The Multiple DNS Domain SSO setup screen

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, say you divide your network into multiple domains to service different functions of your organization. You have one for your corporate information, another for your products, and another for your e-commerce transaction server. Therefore, to ensure all enforcers have all of these domains to 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 the exact same list. Otherwise, multidomain SSO fails.



Multidomain SSO support only works when a user is accessing content across Enforcer plugin-protected Web servers concurrently. If a user 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 site 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 *Enabling single sign-on* on page 121 of the *HP OpenView Select Access 6.0 Network Integration Guide*.

2. Click **Next**. The **Ignored Filenames** setup screen appears. See *Setting up SOAP message signing* on page 152.

Setting up SOAP message signing

The **Sign SOAP XML** setup screen, shown in Figure 66, 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.

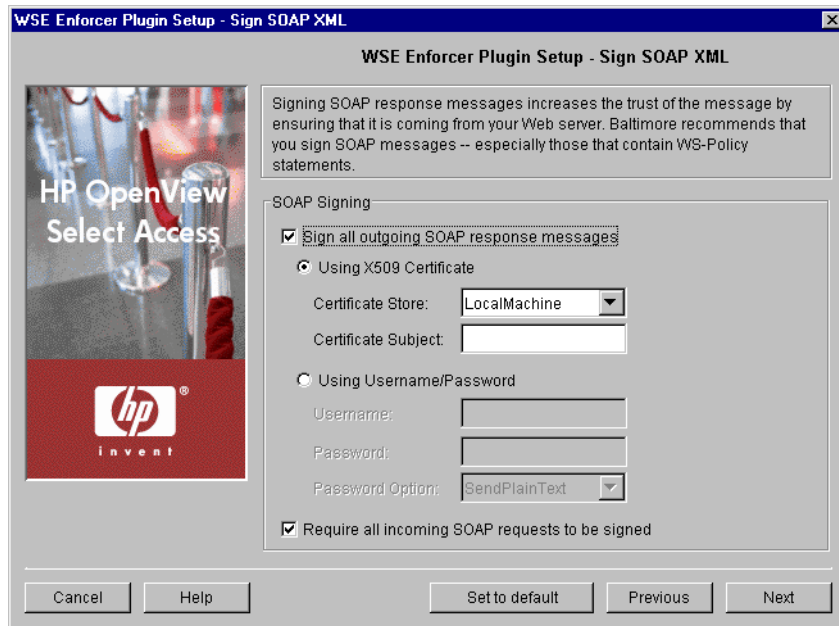


Figure 66: The Sign Soap XML setup screen

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 Local Machine or Current User.
 - **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 154.

Setting up SOAP message encrypting

The **Encrypt SOAP XML** setup screen, shown in Figure 67, 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.

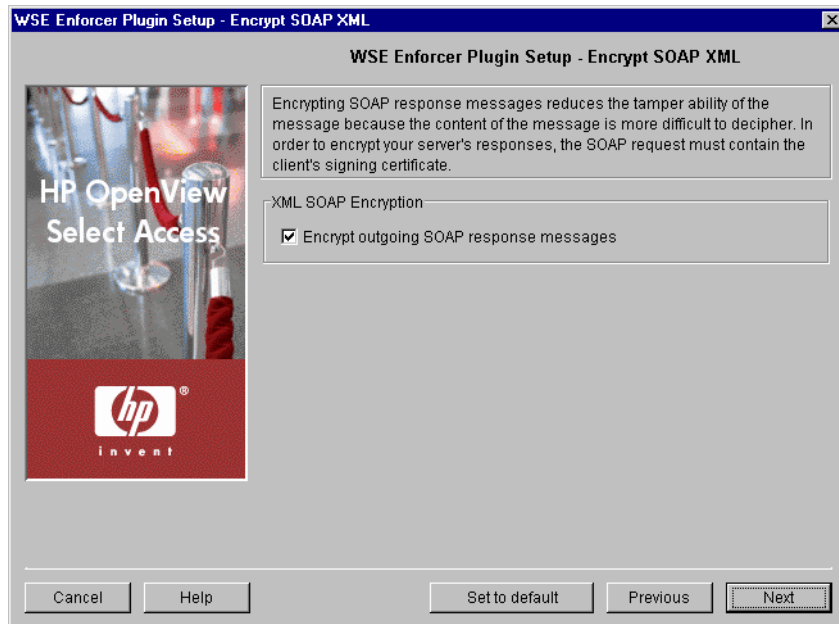


Figure 67: The Encrypt Soap XML setup screen

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.

i 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.

i The WSE Enforcer plugin can only encrypt messages using a 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 158.

Setting up a list of ignored filenames

The **Ignored Filenames** setup screen, shown in Figure 68, 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 user access to the resource. This direct response to the user'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 ONE (iPlanet), Apache, IBM HTTPD, IIS, Axis, or Generic.



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 you the URL to your web service is

`https://localhost/webservice/webservice.asmx`, you could add any of the following to the list of Ignored filenames:

```
/webservice/webservice.asmx
/webservice/*.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 the **Ignored Filenames** list as described in Step 2 of the procedure below:

```
/Axis/*
```

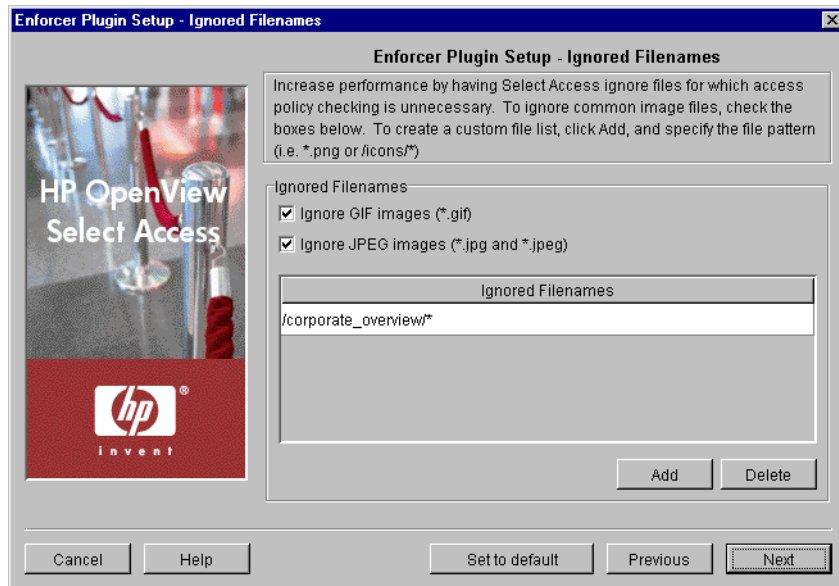


Figure 68: The Ignored Filenames setup screen

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 158.

Setting up a list of pass-through domains

The **Pass-through Domains** setup screen, shown in Figure 69, 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 ONE (iPlanet), Apache, IBM HTTPD, IIS, or Generic.

 In addition to using IP addresses or host domain names, you can also use host header-based virtual host names on Apache, IIS, iPlanet, and Sun ONE (iPlanet) servers.

For additional details on virtual Web hosting, see *Configuring your Enforcer plugin for virtual hosting* on page 90 in the *HP OpenView Select Access 6.0 Network Integration Guide*.

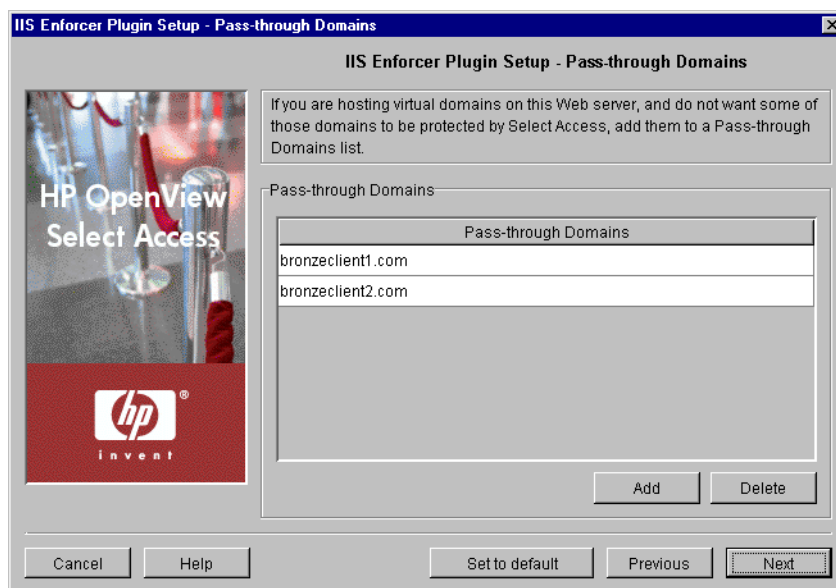


Figure 69: The Pass-through Domains setup screen

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 159.

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 70, 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. Additionally, for each message that the Enforcer plugin cannot log to an offline Secure Audit server, it logs two messages to the Windows Event Log. However, be sure 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.

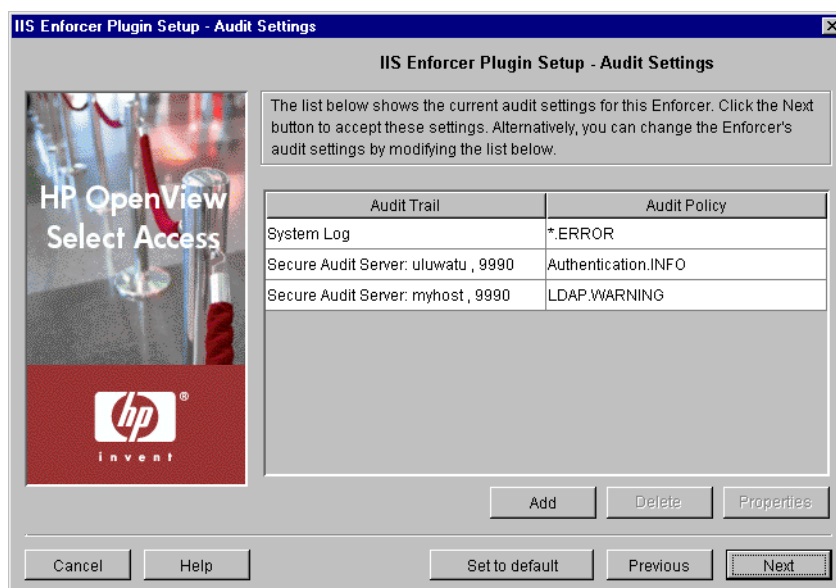


Figure 70: The Audit Settings setup screen

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 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, 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 *Supported audit policy combinations* on page 113 and *Configuring an Audit Policy* on page 110.

3. To remove an empty or populated row, select the entry in question and click **Delete**. Click **Next**. The **Validators** setup screen



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 **Tools** menu in the Policy Builder. For details, see Chapter 9, *Creating reports from Secure Audit server output*, in the *HP OpenView Select Access 6.0 Policy Builder Guide*.

appears. See *Configuring Policy Validator settings* on page 161.

Configuring Policy Validator settings

The **Validators** setup screen, shown in Figure 71, allows you to determine which Policy Validators the Enforcer plugin uses to authenticate users 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 name 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.

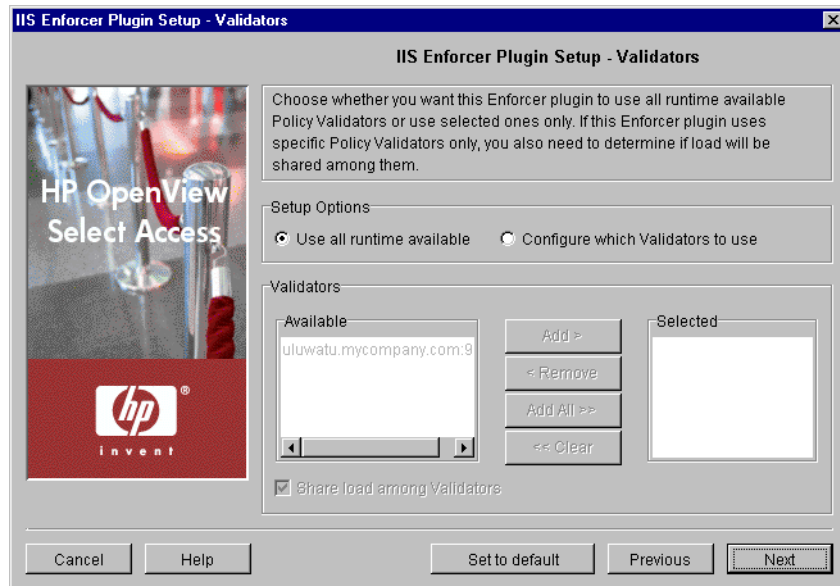


Figure 71: The Validators setup screen

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 the 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 accordingly by selecting a Policy Validator and using 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 163.

Mapping Policy Validators to NAT addresses

The NAT setup screen, shown in Figure 72, 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 161 for details.

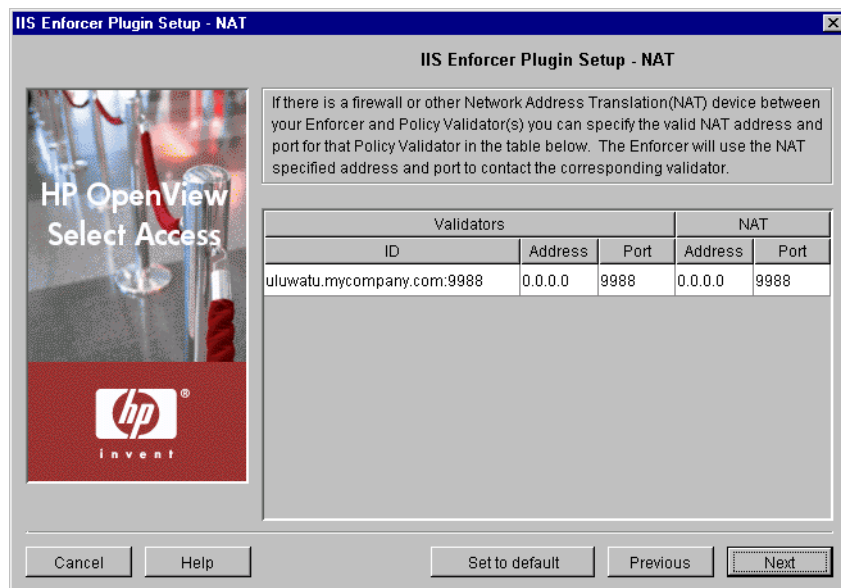


Figure 72: The NAT setup screen

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, enter 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 164.

Tuning your Enforcer plugin

The **Tuning Parameters** setup screen, shown in Figure 73, 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 bolded and italicized if the Enforcer plugin has any override values set for it. The remaining parameters are those that are shared by all Enforcer plugins.

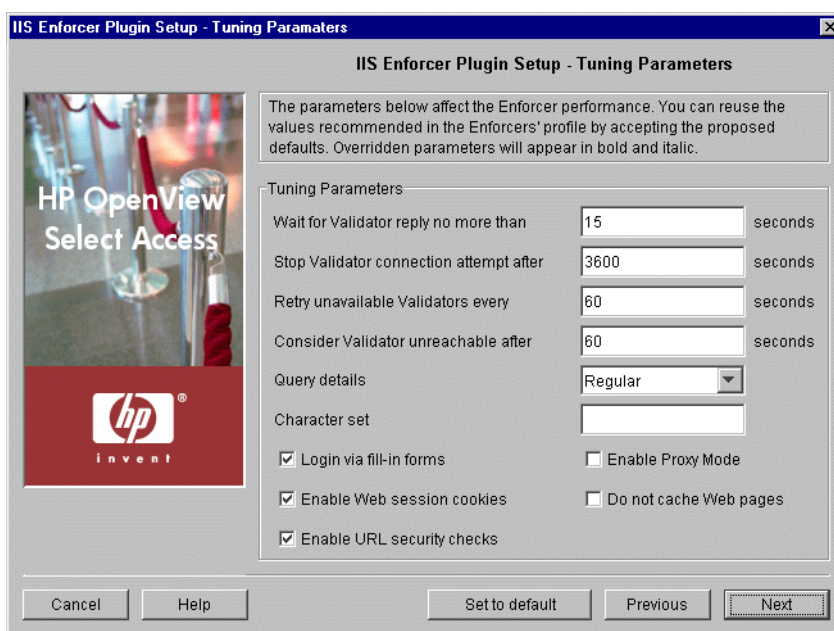


Figure 73: The Tuning Parameters setup screen

To tune your Enforcer plugin

1. 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 before it closes the connection and attempts to connect to the next Policy Validator in the server pool.



You can use a value of 0 to disable this parameter; however, this breaks failover support since the Enforcer plugin does not give up on the connection.



If you are replicating your directory servers and if you cannot set low values for connection timeouts on the host computer's operating system, consider increasing the value for this parameter accordingly.



If your Enforcer plugin's configuration uses a value for its **Wait for Validator Reply** setting of it's **Tuning** parameters, and that is less than OCSP and or directory server timeout used by the Policy Validator, it can appear as if the Policy Validator and Enforcer plugin have entered in 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. To correct this problem, increase the value of the Enforcer plugin's **Wait for Validator Reply** setting parameter.

- **Stop Validator connection attempt after:** Defines the length of time the enforcer plugin tries to establish a connection with Policy Validator. If the Policy Validator does not respond, the enforcer plugin tries to connect to the next Policy Validator in the server pool.



You can use a value of 0 to disable this parameter; however, this breaks failover support since the Enforcer plugin does not give up on the connection.

- **Retry unavailable Validators every:** Sets the time interval for an Enforcer plugin to retry opening a connection to a broken Policy Validator. If an Policy Validator fails, the Enforcer plugin marks the connection to the Policy Validator as broken and the plugin then tries to connect to the next Policy Validator in the Validator pool.
- **Consider Validator unreachable:** Each time the Enforcer plugin returns to a broken Policy Validator, it attempts to reopen the connection. If the Enforcer plugin cannot reopen a connection within the time specified, the Enforcer plugin stops all future connection attempts.
- **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.



You can create your own custom plugin to take advantage of the `site_data` query detail. For details, see Chapter 6, *Setting up your Web server*, in the *HP OpenView Select Access 6.0 Network Integration Guide*.

Table 25: Query details overview

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

- **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 user 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 Chapter B, *Character set listing*.

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



If you intend to use SecurID or RADIUS authentication, you must enable this option.

-
- **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 6.0 Release Notes*.

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



If you are using multidomain SSO with Apache, iPlanet or Sun ONE Web servers, you must check this box.

-
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 167.

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 plugin(s) 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 168 to complete the setup process.
- If you are configuring any other Enforcer plugin, see *To complete the Sun ONE (iPlanet), Apache, IBM HTTPD, IIS or Axis Enforcer plugin setup* on page 169 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. From this dialog, select which web service(s) 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 appears. This dialog allows you to provide the Start and Stop commands so that the Setup Tool can update the configuration file.

For more information, see *The IIS Web Server dialog* on page 172.



After configuring the WSE Enforcer plugin to protect the selected web services, the administrator must create the protected web service network and resource entry on the Resources Tree of the Policy Builder. .NET web service resources can be protected with following Select Access authentication servers:

- Password Certificate
- SecurID (next pin scenario is not supported)
- Windows Kerberos (the domain name must be prepended to the username)
- Windows NTLM (the domain name must be prepended to the username)

To complete the Sun ONE (iPlanet), Apache, IBM HTTPD, 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`).



These bootstrap files contain startup and general configuration information for their respective Enforcer plugin. Modifying or moving these files could result in the Enforcer plugin(s) being unable to start correctly. You should ensure that you protect these files using both logical and physical controls.

-
4. If you chose the **Update the configuration option**, one of the following dialogs appears. These dialogs request the information required to integrate the Enforcer plugin with its respective Web or Application server.
 - The **Sun ONE (iPlanet) Web Server** dialog. For more information, see *The Sun ONE Web Server dialog* on page 170.

- The **Apache Web Server** dialog. For more information, see *The Apache Web Server dialog* on page 171.
- The **IIS Web Server** dialog. For more information, see *The IIS Web Server dialog* on page 172.
- The **Axis Host Application** dialog. For more information, see *The Axis Host Application dialog* on page 173.

To locate the configuration files, the Setup Tool locates all subkeys under `LM/W3SVC` which contain an `AppRoot` key. For every subkey found, it looks up the value of their `Path` key and builds a list of directory paths. It then searches the path directory on disk for files with the `.asmx` extension.

Starting your Enforcer plugin

Because the Enforcer is a plugin, you need to configure your Web server to load the plugin upon 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 dialogs that correspond to each type of Web server, as shown in Table 26.

Table 26: Web server dialogs displayed after configuration

This server	For details, see...
Sun ONE	<i>The Sun ONE Web Server dialog</i> on page 170
Apache	<i>The Apache Web Server dialog</i> on page 171
IIS	<i>The IIS Web Server dialog</i> on page 172
Axis	<i>The Axis Host Application dialog</i> on page 173
TCP	<i>Manually configuring inetd to start the TCP Enforcer plugin</i> on page 174

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 server to use the Enforcer plugin* on page 74 in the *HP OpenView Select Access 6.0 Network Integration Guide*.

The Sun ONE Web Server dialog

This dialog 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 ONE (iPlanet) Enforcer

plugin with the Web server. Otherwise, it cannot automatically load with the Web server.



If you are running your iPlanet or 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.

Warning! When using the iPlanet or Sun ONE console, do not use the **Save and Apply Configuration Files** option. It overwrites the changes the Setup Tool automatically made to the server's configuration file. Instead, choose either **Load Configuration Files** or **Apply**.

Server version Required. Choose which server version your iPlanet or Sun ONE Web server is. You can choose from iPlanet 4.x or Sun ONE 6.x.

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 `StackSize` parameter to 393216 in the `magnus.conf` file. It does this to prevent fatal errors from occurring in the Sun ONE (iPlanet) Enforcer plugin. If it uses the default value, the Sun ONE (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 6, *Setting up your Web server*, in the *HP OpenView Select Access 6.0 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 iPlanet or Sun ONE Web Server. By default the start and stop files are `startsvr.bat` and `stopsvr.bat` respectively.

The Apache Web Server dialog The Apache Web Server dialog appears if you checked **Restart Web Server** in the **Finish** setup screen of the Apache Enforcer plugin setup wizard.

This dialog allows you to integrate the Apache 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 6, *Setting up your Web server*, in the *HP OpenView Select Access 6.0 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 172.

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 172.

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 172.

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 Enforcer plugin as needed, and use the **Apache Web Server** dialog box to start Apache.

The IIS Web Server dialog

The IIS Web Server dialog 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 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 *Configuring the IIS Web server* on page 75, in the *HP OpenView Select Access 6.0 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

The Axis Host Application dialog appears if you checked **Restart Host Application** in the **Finish** setup screen of the Axis Enforcer plugin setup wizard.

This dialog 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.

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 146.
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 27.

Table 27: Optional configuration parameters available

Parameter	Usage
<code>-c filename</code>	Specifies an enforcer configuration file. <i>filename</i> is the name and location of the enforcer configuration file. If you do not provide a <i>filename</i> , the Enforcer plugin uses its default one.
<code>-d</code>	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).

Table 27: Optional configuration parameters available (Continued)

Parameter	Usage
<code>-p protocol_name</code>	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 last string in the program as the protocol name.
<code>-r</code>	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.
<code>-v</code>	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 234.



For Unix users, run the uninstaller as root to ensure all files are completely removed.

Even though partnering Web sites are independent and use their own authentication methods and access management systems, a Select Access-protected organization can still share user information with partnering sites via a server that uses the SAML protocol.



Both the sending and receiving SAML servers need to make a reasonable effort to ensure that clock settings at both sites do not differ by more than two minutes.

What is the SAML server?

By acting as an introduction service, a SAML-enabled and Select Access-protected site can share profile information with its partners, so that they in turn can create their own profile for that individual. The SAML server:

- Evaluates incoming resource requests from users authenticated by your partners
- Forwards queries to the Policy Validator on the user's behalf



For additional details on setting up SAML servers with your partner organizations, see the *Select Access 6.0 SAML Solution Guide*.

Using the Setup Tool to configure the SAML 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 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 you refresh the Enforcer plugin's configuration by rerunning 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 5, *Modifying components' central configuration parameters*, in the *HP OpenView Select Access 6.0 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 set up the SAML server and SAML 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 **SAML server** setup screen.

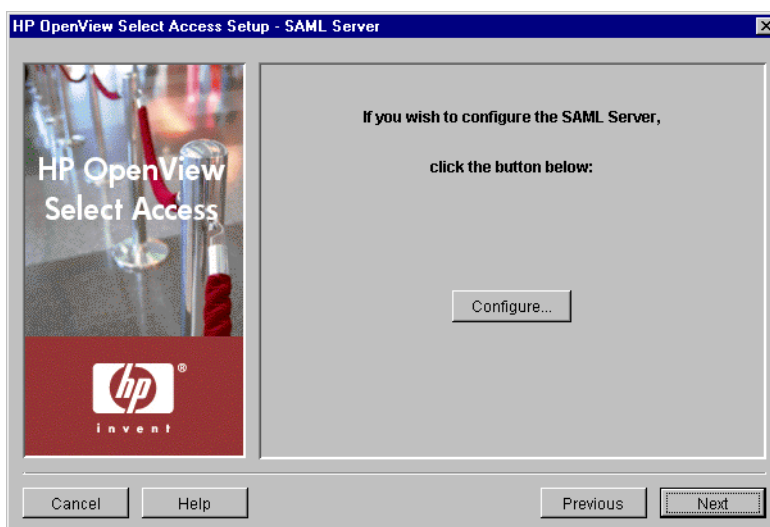


Figure 74: The SAML server setup screen

- Click the **Configure** button. The **SAML server** 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 **ID** setup screen appears instead.


- Complete the setup screens of the SAML server setup process, listed in Table 28, as necessary.


Table 28: Overview of SAML server setup process

Setup screen	Description	Default value(s)
Contact the Administration Server setup screen	Allows the Setup Tool to connect to the Administration server, so it can manage the SAML server's configuration parameters and request the common and/or group configuration parameters for it. See <i>Connecting to the Administration Server</i> on page 180.	auto-defined
ID setup screen	Allows you to define the ID used to identify your SAML server. See <i>Defining a SAML server ID</i> on page 181.	auto-defined
General Configuration setup screen	Allows you to configure basic setup parameters that define how partnering SAML servers connect to your Select Access SAML server. It also determines what actions your SAML server performs. See <i>Configuring basic setup parameters</i> on page 181.	not enabled
SSO to Partners setup screen	Allows you to define a list of SAML partners to which the Select Access SAML server may transfer users. See <i>Setting up a SAML destination partners list</i> on page 185.	not enabled
SSO from Partners setup screen	Allows you to define a list of SAML partners from which the Select Access SAML server will accept transferred users. See <i>Setting up a SAML source partners list</i> on page 188.	not enabled
SAML server Enforcer plugin setup screens and Finish setup screen	The SAML server Enforcer plugin setup screens allow you to configure the Enforcer plugin required to secure the SAML server. The Finish setup screen allows you to commit your configurations settings to the Policy Store and the SAML server's bootstrap XML file, and to automatically start the SAML server. See <i>Completing the SAML server setup process</i> on page 193.	enable SAML server restart

Connecting to the Administration Server

In order to configure the SAML server, the Setup wizard must be able to connect to the Administration server. The Administration server stores and manages the configuration data for the SAML server. The **Contact the Administration server** setup screen, shown in Figure 75, allows you to provide the connection parameters.

 If you have installed the SAML server 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. In this case, the **ID** setup screen appears.

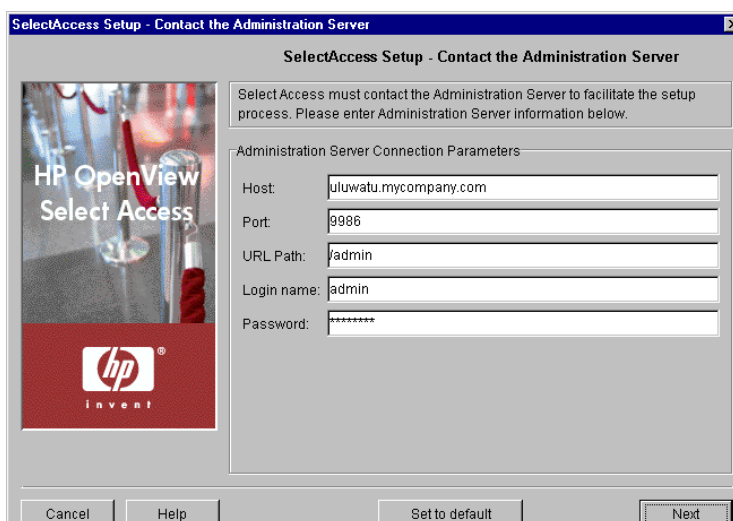


Figure 75: The Contact the Administration Server setup screen

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 user name to log into the Administration Server.

- **Password:** Required. Enter the password to log into the Administration Server.
2. Click **Next**. At this point, the Setup Tool tries to connect to the Administration server. If it connects successfully, the ID setup screen appears.

Defining a SAML server ID

The ID setup screen, shown in Figure 76, allows you to define a SAML server ID. The ID identifies a SAML server to the Administration server. 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.

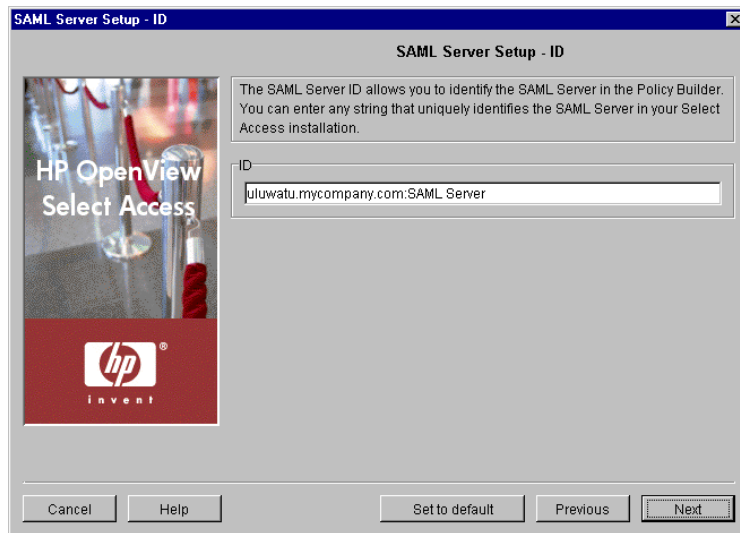


Figure 76: The ID setup screen

To define the SAML server ID

1. In the ID group, specify the ID which will be used to identify the SAML server.
2. Click **Next**. The **General Configuration** setup screen appears. See *Configuring basic setup parameters* on page 181.

Configuring basic setup parameters

The **General Configuration** setup screen, shown in Figure 77, allows you to configure basic setup parameters that define how partnering SAML servers connect to your Select Access SAML server. It also determines what actions your SAML server performs.

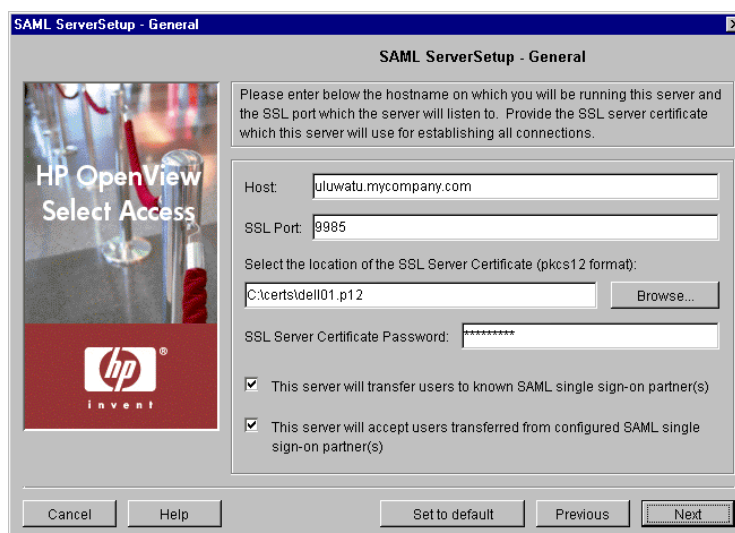


Figure 77: The General setup screen

To configure basic SAML server parameters

1. Review HP's recommended values. To customize these values, modify the screen's fields as needed.
 - **Host:** Required. Enter the IP address or host name that servers use to connect to the SAML host computer.
 - **SSL Port:** Required. Enter the port the SAML Server is running on. If you leave it blank, the SAML server uses the default port of 9985.



Port values can potentially be different on each SAML partner site. You do not need to define the same SAML port as your partners.



The SAML server runs on two ports. The default port value you enter is used for all communications that occur after the partner is authenticated. The default port minus 1 (in this example, 9984) is used for authentication only.

Both port numbers become part of the SAML server's service entry properties that are automatically created when you finish the server's configuration.

- **Select the location of the SSL certificate:** Required. Select a PKCS#12 format SSL certificate. The SAML server uses this certificate to encrypt SSL sessions among partnering SAML servers.
- **SSL Server Certificate Password:** Required. Enter the password to unlock the SSL certificate you just selected.
- **The server will transfer users to known SAML single sign-on partners:** Optional. Check this box if you want your Select Access SAML

server to transfer authenticated users to partnering SAML servers so they can seamlessly access third-party content.



If you do not enable this option, the **SSO to Partners** setup screen will not appear. This screen does not appear unless you have checked this box.

- **The server will accept users transferred from configured SAML single sign-on partners:** Optional. Check this box if you want your Select Access SAML server to accept authenticated users from partnering SAML servers so they can seamlessly access your content from a third-party site.
-



If you do not enable this option, the **SSO from Partners** setup screen will not appear. This screen does not appear unless you have checked this box.

2. Click **Next**.

- If this is the first time you are configuring the SAML server, the **Setup SAML Server's Assertion Properties** dialog appears. See step 3.
- If you are modifying a previously configured SAML server, the **SSO to Partners** setup screen appears. See *Setting up a SAML destination partners list* on page 185.

3. Review HP's recommended values. The **Setup SAML Server's Assertion Properties** dialog, shown in Figure 78, allows you to set up the SAML assertions properties of your Select Access server. The Setup Tool can export information you define here to a text file. Exporting this information guarantees that all partner sites configure their servers using the exact information you specify with this dialog.



If partner servers misconfigure this information, SAML exchanges cannot occur.

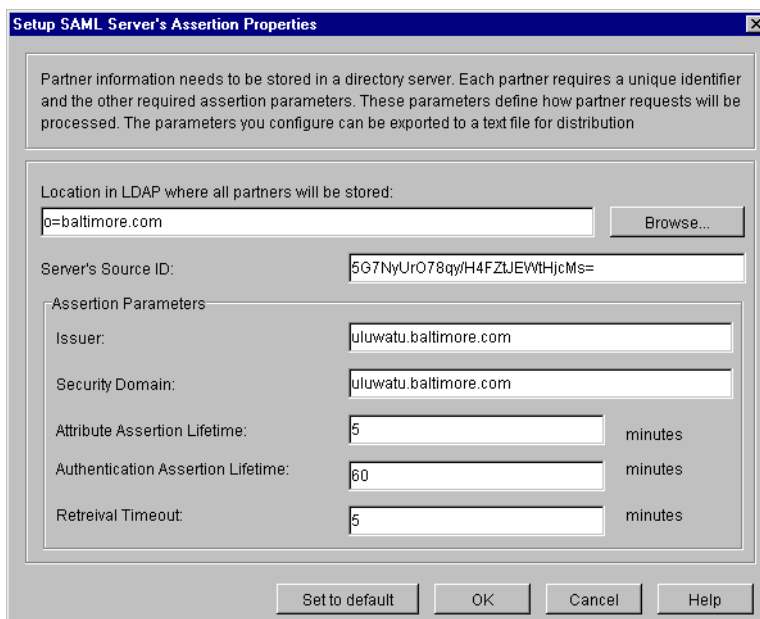


Figure 78: The Setup SAML Server's Assertion Properties dialog

4. To customize these values, modify the screen's fields as needed.
 - **Location in LDAP where all partners will be stored:** Required. Select the folder in the directory server that Select Access uses to store SAML information of all partners that you intend to send users to.
 - **Server's Source ID:** Required. A 20-byte SHA-1 hash of the server's full host name. If you enter your own ID in this field, the Setup Tool hashes it to ensure it meets the 20-byte requirement. The SAML server uses this ID to construct a SAML-specific artifact that the SAML protocol requires to redirect users to the partner's site.
 - **Issuer:** Required. Enter the unique tag for the administrator of the Select Access SAML server. The SAML server uses the value you provide to construct SAML assertions.
 - **Security Domain:** Required. Enter your security domain. Typically a security domain is the same as the domain of the Web site that transferred the user. The SAML server uses the value you provide to create a SAML subject that acts as a unique identifier for transferred users. SAML subjects are typically a user's name and the security domain the user belongs to.
 - **Attribute Assertion Lifetime:** Required. Define the how long an attribute assertion is valid for, between a range of 0 and 1576800 (3 years) minutes. Ensure the lifetime of an attribute

assertion has a longer validity period. By default, the timeout value is 7 days.



If an attribute assertion becomes invalid too frequently, user access among partner organizations is not seamless.

- **Authentication Assertion Lifetime:** Required. Define the length of time that determines how long an authentication assertion is valid for between a range of 0 and 43200 (30 days) minutes. Ensure the lifetime of an authentication assertion has a short validity period. By default, the timeout value is 5 minutes.
- **Retrieval Timeout:** Required. Define the length of time that determines how long the partner SAML server has to contact the Select Access SAML server with a request after receiving either a artifact contained in the redirect URL or a response sent to a SAML request sent earlier. The range of accepted values is 0-15 minutes. By default, the timeout value is 5 minutes.

5. Click **OK**. The **SSO to Partners** setup screen appears. See *Setting up a SAML destination partners list* on page 185.

Setting up a SAML destination partners list

The **SSO to Partners** setup screen, shown in Figure 79, enables single sign-on by allowing the Select Access SAML server to transfer users to the SAML partners you define. It also allows you to modify your own server's configuration details after you have set it up for the first time. If you need to reconfigure the Select Access SAML server's configuration, click the **Configure** button.



To ensure all partners maintain the same list of SAML configuration details, click the **Save to File** button each time your Select Access SAML server details or partnership lists change. When saving to a file, the Setup Tool prompts you to select the partner with whom you intend to share the file. This ensures your partners share the same information as you and therefore minimizes the likelihood of misconfiguration.

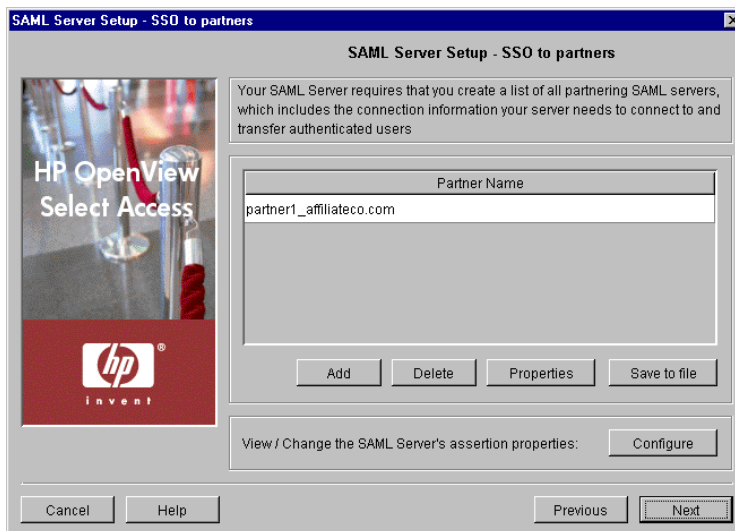


Figure 79: The SSO to Partners setup screen

To add a new SAML server to the list of SSO partners

1. Click the **Add** button. The **Setup SAML Destination Partner** dialog appears, shown in Figure 80.



If you need to delete a partner, select the corresponding entry from the list and click **Delete**. If any of your partners need the same list as you (to prevent an unauthorized user from gaining access to protected resources), share this information as well.

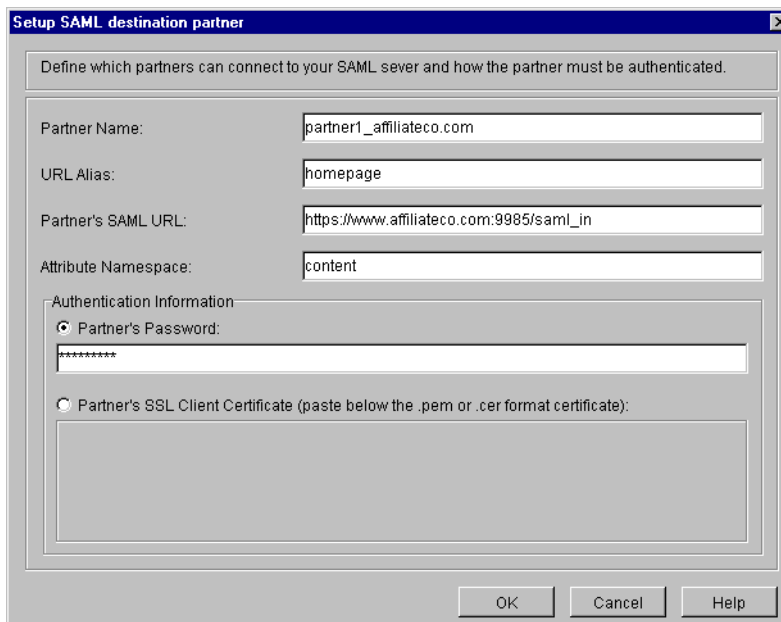


Figure 80: The Setup SAML Destination Partner dialog

2. Configure the fields of this screen as needed.



With the exception of **Partner Name**, only configure the following fields using data your partner has shared with you. You cannot assign these values independent of your partner.

- **Partner Name:** Required. Enter the name of the partner that you are transferring users to. Select Access uses this name to display the partner in the Policy Builder's Users Tree and create a CN attribute for that partner. Select Access also uses the CN to construct the DN of user entries that the Policy Builder renders on the Users Tree for the partner.
- **URL Alias:** Required. Enter a text string that the SAML server substitutes each time an authenticated user request a specific URL. This makes your SAML URL more secure as a Web server cannot accidentally expose it. For details on how the SAML server maps the alias, see *Understanding SAML's redirect syntax* on page 33 of the *HP OpenView Select Access 6.0 SAML Solution Guide*.
- **Partner's SAML URL:** Required. Enter the actual SAML URL. This is the SAML URL that you do not want to expose to third parties for security reasons.
- **Attribute Namespace:** Required. Define a namespace that the SAML server uses with attribute assertions. A namespace can be any string but is typically a Universal Resource Identifier. For example, an attribute assertion that defines a company's number of employees can be:

`www.mycompany.com:totalemployees, 1000`

In this example, `www.mycompany.com` is the namespace that was defined by this field.



When the Select Access SAML server acts as a sending party, you can only create one attribute namespace per partner.



If you are sending users who have a CN longer than 20 characters to a SAML partner that is using an Active Directory server and you do not export the UID personalization attribute, the SAML authentication fails. In this case, you always export the UID attribute to avoid this problem.

- **Partner's Password:** Optional. Choose this option if you require the Select Access SAML server to perform password-based authentication. If you select this option, you must enter the password in the corresponding field that follows.

- **Partner's SSL Client Certificate:** Optional. Choose this option if you confirm the identity of your partner with a client certificate. If you select this option, you must paste the partner's client certificate in the corresponding box that follows. The client certificates must match before you server authenticates the Select Access SAML server.



The certificate you copy must be a PEM-encoded certificate. It must also contain either a cn or uid value (which must be unique). Otherwise, the SAML server cannot accept the certificate.



If you have pasted the partner's client certificate and it contains a uid, then the SAML server uses this uid for the uid attribute of the SAML partner entry. Otherwise, the SAML server uses the **Partner Name** you define instead.

3. When you finish configuring a single partner instance, click **OK**. Repeat this step for each new partner you need to add.
4. When you finish creating a list of SAML partners, click **Next** in the **SSO to Partners** setup screen. The **SSO from Partners** setup screen appears. See *Setting up a SAML source partners list* on page 188.

Setting up a SAML source partners list

The **SSO from Partners** setup screen, shown in Figure 81, enables single sign-on by allowing the Select Access SAML server to accept users transferred from the SAML partners you define.

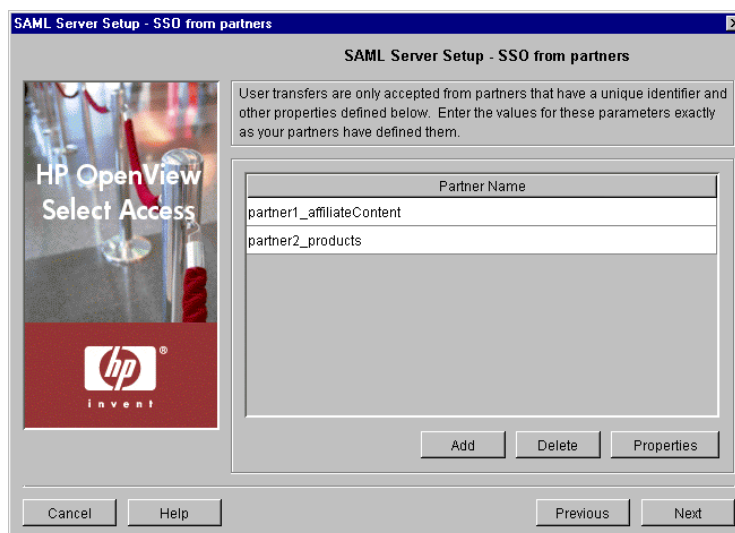


Figure 81: The SSO from Partners setup screen

To create a list of accepted SAML partners

1. To add a new SAML partner to the list of SSO partners, click the **Add** button. The **New SAML Authentication Server** dialog appears, shown in Figure 82.

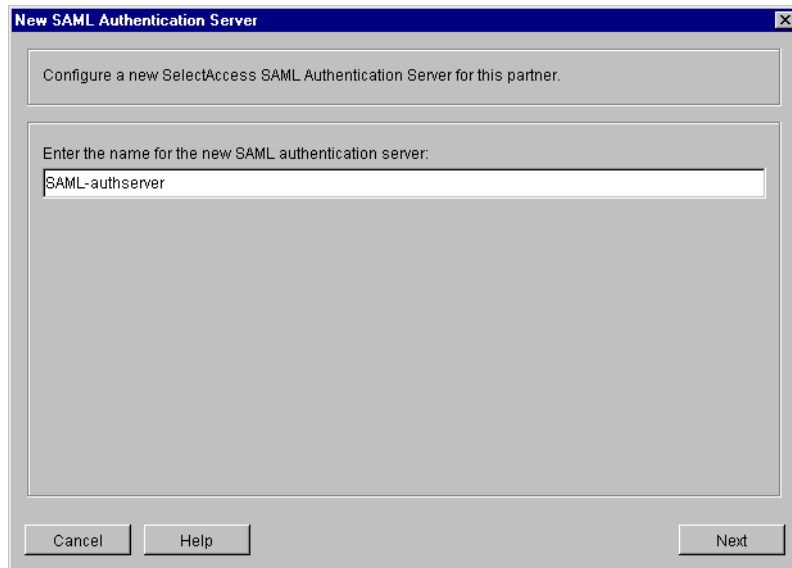


Figure 82: The New SAML Authentication Server dialog

This screen allows you to define a single instance of a partner's SAML server that receives the Select Access SAML server's transfer requests. This server effectively becomes an authentication server and Select Access includes it in your list of configured authentication methods in the Policy Builder.

2. In the **Enter a name for the new SAML authentication server** field, specify a text string used to label this instance of the SAML server that receives and authenticates your incoming transfers.
3. Click **Next**. The **SAML Partner Properties** dialog appears, shown in Figure 83, displaying the **SAML Properties** tab.

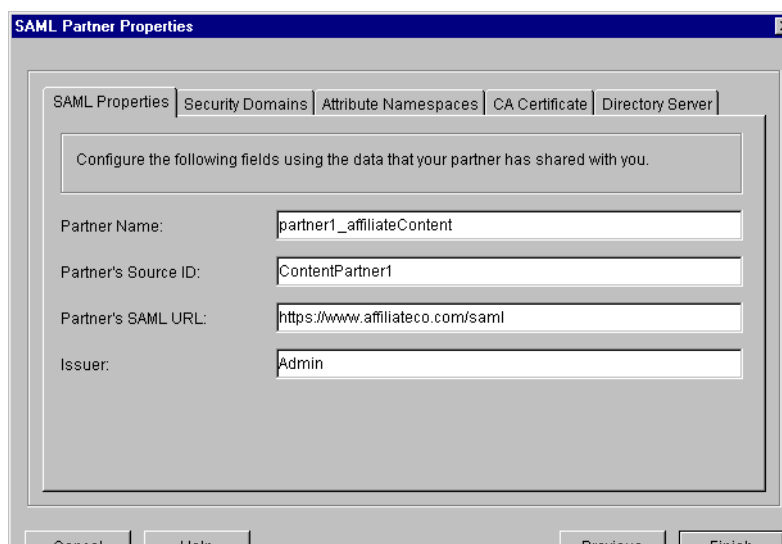


Figure 83: The SAML Partner Properties dialog – SAML Properties tab

4. Configure the fields of this tab as needed.
 - **Partner Name:** Required. Enter the name of the partner you are receiving authenticated users from. This partner's SAML server connects to your Select Access SAML server so that they can exchange data between them.
 - **Partner Source ID:** Required. Enter the exact ID your partner has given you to identify this SAML Server. The SAML server uses the partner ID to look up the address of the partnering SAML server from a local database. This ensures that a SAML server is always going to a known address to do its communications. If the IDs do not match, SAML always fails.



Ensure the partner name and ID is unique among all SAML servers.

- **Partner's SAML URL:** Required. Enter the actual SAML URL that the SAML server redirects the user to. This URL must be absolute and your partner must provide it to you. Like URL Alias, the server needs this field to complete the redirect syntax for SAML. For details on how the SAML server maps the alias, see *Understanding SAML's redirect syntax* on page 33 of the *HP OpenView Select Access 6.0 SAML Solution Guide*.
 - **Issuer:** Required. Enter the unique string the SAML server uses to identify the issuer. This string must come from your partner.
5. When you are finished, click the **Security Domains** tab.

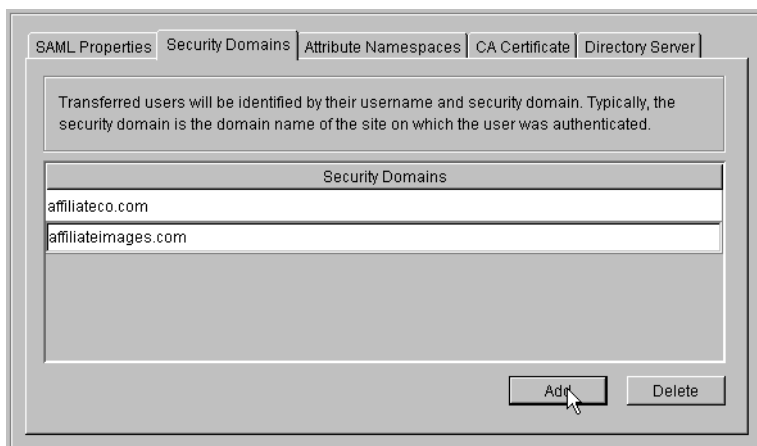


Figure 84: The SAML Partner Properties dialog – Security Domains tab

6. Click the **Add** button to create a list of security domains, provided to you by your partners. Typically, a security domain is the same as the domain of the Web site that transferred the user.
7. When you have finished creating your list, click the **Attribute Namespaces** tab.

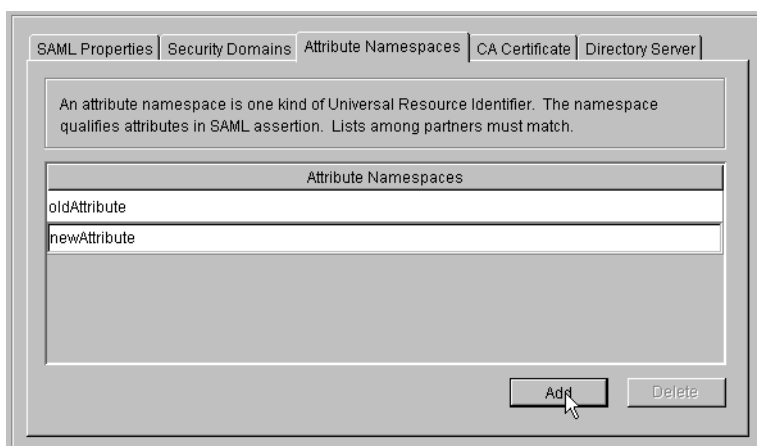


Figure 85: The SAML Partner Properties dialog – Attribute Namespaces tab

8. Click the **Add** button to create a list of attribute namespaces that your partners provide to you. A namespace can be any string but is typically a Universal Resource Identifier (URI).
9. When you have finished creating your list, click the **CA Certificate** tab.
10. In the window provided, paste your CA certificate that the SAML server uses to negotiate SSL-encrypted sessions with your

partners. The server checks signature on your partner's client certificate against the signature in this CA certificate.



Your partner must provide this certificate; otherwise, the connection between your partner's SAML server and your Select Access SAML server fails.



Because the SAML server uses CN field in the certificate as the CN value in the SAML partner entry on the Policy Matrix, ensure that no two partners have the same CN value in the client certificate.

11. Once you have pasted your certificate in the window, click the **Directory Server** tab.

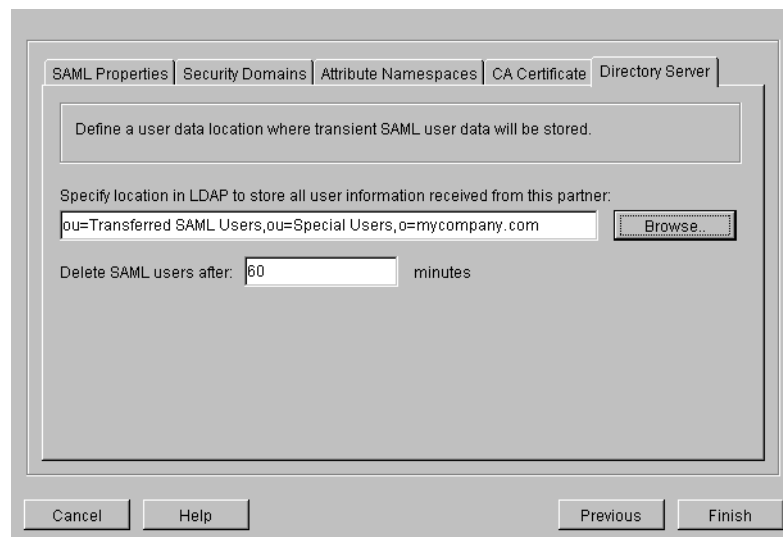


Figure 86: The SAML Partner Properties dialog – Directory Server tab

12. Define a user data location where the Policy Builder stores transient SAML users by configuring the fields of this tab.
 - **Specify location to store all user information received from this partner:** Required. Define a user location on a directory server that the Policy Builder uses to temporarily store all users from your partner's SAML server. That way, the Policy Validator can create a cookie for that user.



HP recommends you create separate folders for each partner so the Policy Builder stores users in a unique location for each.



If are configuring a partner location that requires you to browse to a folder that contains a large number of entries that exceed the Tree threshold you have set, the **Quick Search** dialog box appears. For details, see *To perform a quick search* on page 59. For details on how to change the Tree threshold, see *To set Tree thresholds* on page 63.

- **Delete SAML users after:** Required. Define the length of time that determines how long the SAML server adds a user to your directory server between a range of five and 10080 minutes (7 days). The default value is 10080 minutes. To give you more control over the lifetime of the user entry created in your directory server, Select Access compares the attribute assertion lifetime configured by your partner against this value. The SAML server uses the lesser of the two values to decide when it deletes the transferred SAML user.

13. When you have finished configuring all tabs of this screen, click **Done**.
14. In the **SSO from Partners** setup screen, click **Next**. The SAML Enforcer plugin Wizard appears displaying the **SAML Server Enforcer Plugin setup — ID** setup screen. This wizard installs and configures a SAML Enforcer plugin that enforces Policy Validator authorization decisions on the SAML server. See *Completing the SAML server setup process* on page 193.

Completing the SAML server setup process

In order to complete the SAML server setup, you must configure the SAML server Enforcer plugin and commit the changes to the Administration server.

To complete the SAML server setup process

1. Complete the setup screens of the SAML server Enforcer plugin setup process, listed in Table 29, as necessary

Table 29: Overview of the SAML server Enforcer plugin setup process


<p>General setup screen</p>	<p>Allows you to choose one of two setup types:</p> <ul style="list-style-type: none"> • Typical: Use HP’s recommended setup values. • Custom: Modify the recommended values to meet the needs of your network and/or business environment. <p>See <i>Choosing your setup type</i> on page 147 in Chapter 8, <i>Configuring the Enforcer plugins</i>.</p>	<p>Typical</p>
------------------------------------	---	----------------

Table 29: Overview of the SAML server Enforcer plugin setup process

<p>ID setup screen</p>	<p>Displayed for a Custom setup of the SAML Enforcer plugin.</p> <p>Allows you to define an enforcer ID which is used to identify the Enforcer plugin. See <i>Defining an Enforcer plugin ID</i> on page 148 in Chapter 8, <i>Configuring the Enforcer plugins</i>.</p>	<p>auto-defined</p>
<p>Single DNS domain SSO setup screen</p>	<p>Displayed for a Custom setup of the SAML Enforcer plugin.</p> <p>Allows you to allows you to identify the domain name across which users authenticate only once – even though they access resources on multiple subdomains. See <i>Setting up single domain single sign-on</i> on page 149 in Chapter 8, <i>Configuring the Enforcer plugins</i>.</p>	<p>not enabled</p>
<p>Audit Settings setup screen</p>	<p>Displayed for a Custom setup of the SAML Enforcer plugin.</p> <p>Allows you to configure audit settings specific to the SAML Enforcer plugin. See <i>Configuring enforcer-specific audit settings</i> on page 159 in Chapter 8, <i>Configuring the Enforcer plugins</i>.</p>	<p>inherit common settings defined by the Administration server</p>
<p>Validators setup screen</p>	<p>Displayed for a Custom setup of the SAML Enforcer plugin.</p> <p>Allows you to select which Policy Validators the Enforcer plugin uses to authenticate users and authorize resource requests. You can also establish whether to use round-robinning to share loads among the Policy Validators you define. See <i>Configuring Policy Validator settings</i> on page 161 in Chapter 8, <i>Configuring the Enforcer plugins</i>.</p>	<p>auto-defined to use all runtime-available Policy Validators listed in the Policy Store.</p> <p>Load sharing is enabled.</p>
<p>Tuning Parameters setup screen</p>	<p>Displayed for a Custom setup of the SAML Enforcer plugin.</p> <p>Allows you to specify tuning parameters so you can configure how the Enforcer plugin performs at runtime. See <i>Tuning your Enforcer plugin</i> on page 164 in Chapter 8, <i>Configuring the Enforcer plugins</i>.</p>	<p>auto-defined</p>

- On the final **SAML Server Enforcer Plugin - Tuning Parameters** setup screen, click **Next**. The **Finish** setup screen appears informing you that you have completed all setup tasks for the SAML server.

3. If you want to start the SAML server immediately after the Setup Tool records your configuration parameters, click the **Start now** box.
4. Click **Finish** to commit your configuration to the Policy Store. The Setup Tool then creates the following entries on the Resources Tree:
 - An HTTPS service entry for the SAML server. By default, this entry appears in the following location:
`ou=Network,nxResource=https,nxResource=
<hostname>:SAML Server`

 If you used a previous version of Select Access and installed a SAML server on your network, you will have manually created a service entry for the SAML Server on the network tree – and possibly at some other location. This entry is automatically updated in this version of Select Access with the `saml_out`, `saml_in` and `saml_responder` resources.

- The corresponding resource entries that follow the SAML server service entries (depending on whether or not you have configured the SAML server to do outbound transfers, accept inbound transfers, or both):

`saml_out` is the script that initiates the transfer to your partner's SAML server.

`saml_in` the script that receives and processes your partners transferred users.

`saml_responder` is the URL path to your partner's SAML server uses to query your SAML server for user information. The `saml_responder` communicates with your partner's `saml_in` script.

 This URL is the same URL your partner configures in the **Partner's SAML URL*** field of the **SAML Partner Properties** dialog.

Starting your SAML server

If you do not start the SAML server immediately after you configure it, you need to use an alternative method. Irrespective of the platform you are running the SAML server on, there are two startup methods:

- *Starting it automatically:* so it runs when you boot the host computer. By default, the Setup Tool configures the SAML server to start this way.
- *Starting it manually:* so it runs only when you want it to. On Windows, you can run the SAML server from the command line, whereas on Unix, you must use the `saml start` script.

You must stop and restart the SAML server if:

- You change the SAML server's configuration.
- You change the date and/or time on the computer where the SAML server's Enforcer plugin is running.
- You change configuration details for the Secure Audit Server.

Windows—starting the SAML server manually

You can start the SAML server manually on Windows by running it from the command line using the startup command with any combination of options.

To start the SAML 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:

```
netstart
```

Unix—starting the SAML server manually

You can use the `saml` script to start and stop the SAML server.

1. To start the SAML server, enter the following:

```
<install_path>/samlserver start
```

2. To stop the SAML server, enter the following:

```
<install_path>/samlserver stop
```

Uninstalling the SAML server

You can uninstall the SAML server with the uninstaller shipped with Select Access. For details, see *Uninstalling Select Access* on page 234.



For Unix users, run the uninstaller as root to ensure it removes all files.

Windows users can also uninstall the SAML server from the command line. To uninstall the SAML server from the command line, enter the following command with these parameters:

```
samlserver -U -N service_name
```

For details on these command line options, see *Windows – starting the SAML server manually* on page 196.



Close and reopen the **Services** dialog to ensure that the uninstaller has removed the service.

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 where necessary parameters are not available in a component's own setup wizard.

For example, 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 component(s) 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 staff.

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 ever 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 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 users, however, since more sophisticated Select Access users may also find it useful.



Note that 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 5, *Modifying components' central configuration parameters*, in the *HP OpenView Select Access 6.0 Policy Builder Guide*.

Predefined flags

HP has identified some common situations in which custom settings may be needed. Select Access has predefined the flags which you can set in these situations:

- **USE_BSA_PREFIX:** Prior to Select Access 5.2, the Select Access API prefixed a number of attributes with BSA. Since Select Access 5.2, however, this prefix was changed to SA. If you are using Enforcer plugins from a release previous to Select Access 5.2, you will need to select this option to ensure all components are communicating using similarly-prefixed attributes.
- **USE_OLD_P13N_TAGS:** Prior to Select Access 5.2, personalization headers were identified using the tag HTTP_BSA. In Select Access 5.2, the P13N tags were changed to HTTP_SA. If you are using Select Access's personalization feature with Enforcer plugins from a release previous to Select Access 5.2, you will need to select this option to ensure that personalization tags are handled consistently.

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.

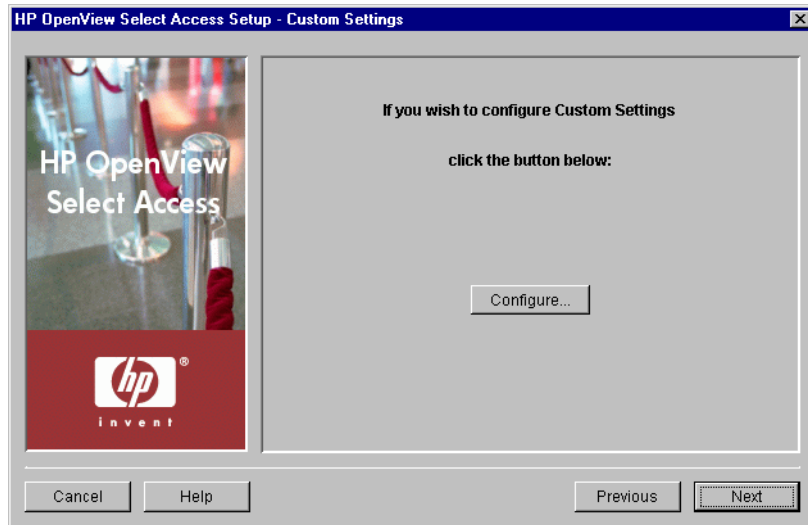


Figure 87: The Custom Settings setup screen

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 30, as necessary.

Table 30: Overview of custom settings setup process

Setup screen	Description	Default value(s)
Contact the Administration Server setup screen	Allows the Setup Tool to connect to the Administration server, so it can manage the custom settings flags. See <i>Connecting to the Administration Server</i> on page 200.	auto-defined

Table 30: Overview of custom settings setup process

Setup screen	Description	Default value(s)
Custom Settings Flags setup screen	Allows you to enable flags which override the typical behaviour of the components to which they apply. You can enable one of the predefined backwards compatibility flags or add your own custom settings. See <i>Enabling custom settings flags</i> on page 201.	not defined
Finish setup screen	The Finish setup screen allows you to commit your configurations settings to the Policy Store, and to automatically start the Policy Validator. See <i>Completing the custom settings setup process</i> on page 202.	enable Policy Validator restart

Connecting to the Administration Server

In order to configure the SAML server, 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 88, 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.

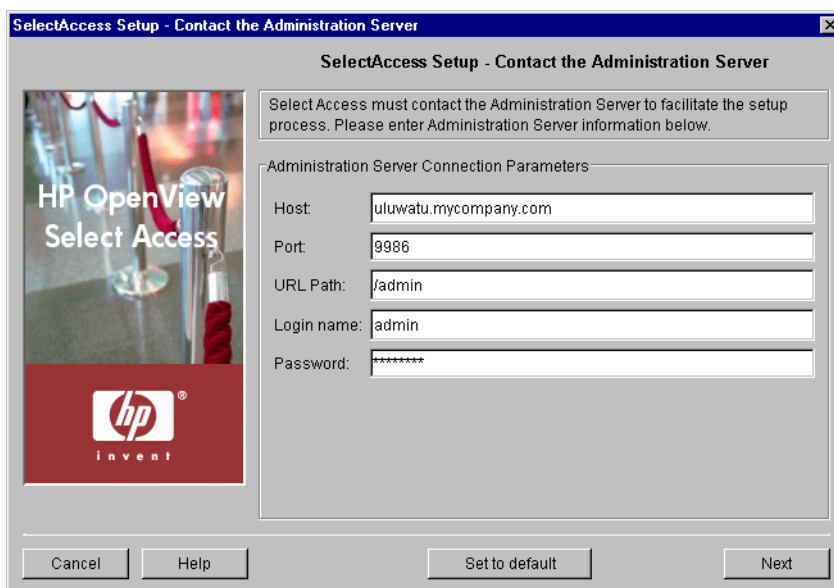


Figure 88: The Contact the Administration Server setup screen

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 user name to log into the Administration Server.
 - **Password:** Required. Enter the password to log into the Administration Server.
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 89, allows you to enable flags which override the typical behaviour of the components to which they apply. You can enable one of the predefined backwards compatibility flags, described in *Predefined flags* on page 198, or add your own custom settings. Flags set in this screen are applied globally to all applicable components.

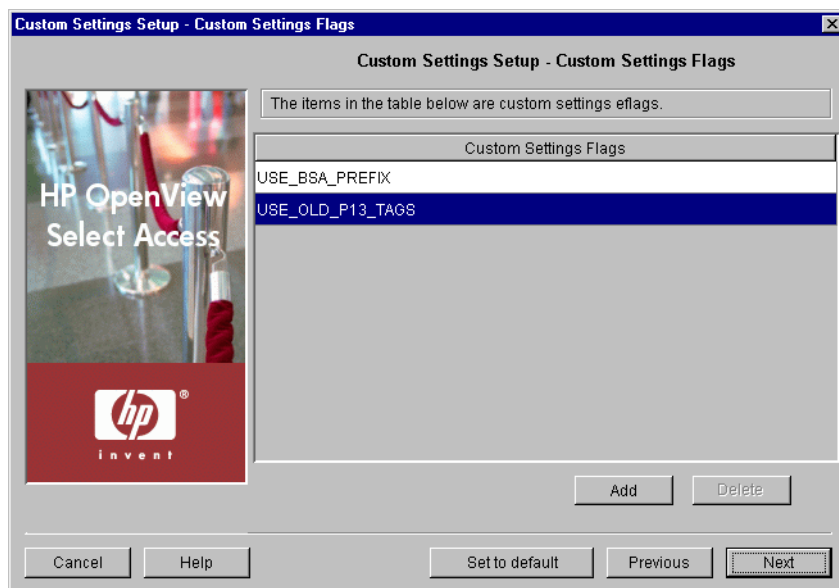


Figure 89: The Custom Settings Flags setup screen

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 and choose the necessary flag from the list. For more information, see *Predefined flags* on page 198
 - c. To add a new custom flag, select the row and type the flag name.



Users 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 users 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 Policy Validator.

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 Validator now** box.
2. Click **Finish** to commit your configuration to the Policy Store.

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.

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 LDAP 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 procedure that follows 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 a seamless one.



Always remember to update your archives each time you reconfigure your current Administration server. Otherwise, other components on your network can 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>\shared\` folder:

- `rsa.*.key`: Your Select Access component key pairs
- `ca_cert.pem`: The CA certificate used by Select Access

If you are using database reporting, you also need the `<install_path>\shared\jetty\policy_builder_driver_file(s)`. Select Access uses these driver files to log to a JDBC compliant database.

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 location 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.



Modifying certain parameters requires that you reconfigure existing Select Access components as well. See Chapter 5, *Configuring the Administration server*, for details.



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 in 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.

Maintaining Select Access

You can modify your existing installation of Select Access 6.0 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 205.
- **Modify:** Installs a new component to the existing set of components already installed. For details, see *Modifying Select Access* on page 220.
- **Uninstall:** Uninstalls some or all of Select Access components on the current host machine. For details, see *Uninstalling Select Access* on page 234.

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 behaving abnormally.
- It is under the advisement of Global Support Services.
- One or more files have been overwritten or have gone missing.

To repair detected components with Select Access's installer

1. Run the Select Access installer. The **Maintain HP OpenView Select Access 6.0** screen appears.

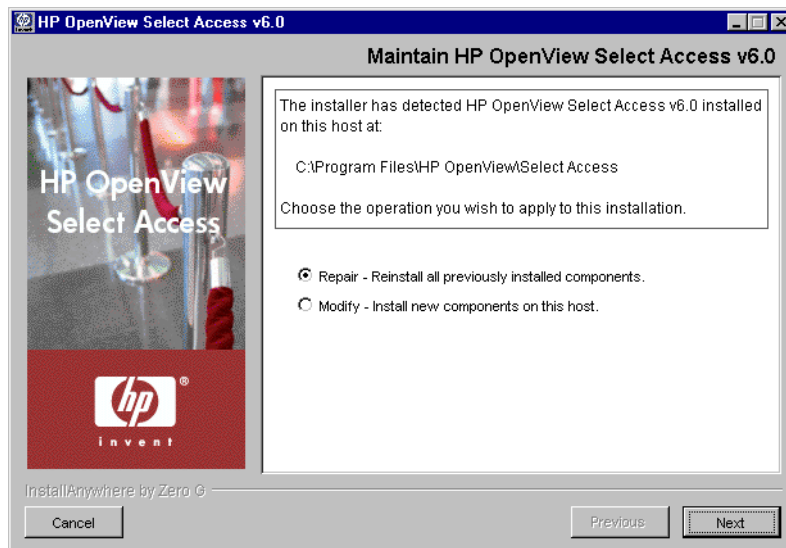


Figure 90: The Maintain HP OpenView Select Access 6.0 screen

2. Click the **Repair** option. The **Repair HP OpenView Select Access 6.0** screen appears.

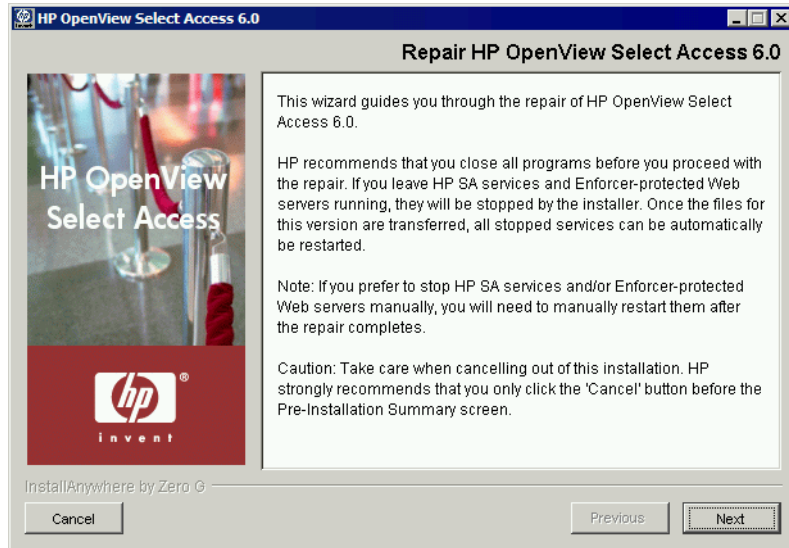


Figure 91: The Repair HP OpenView Select Access 6.0 screen

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

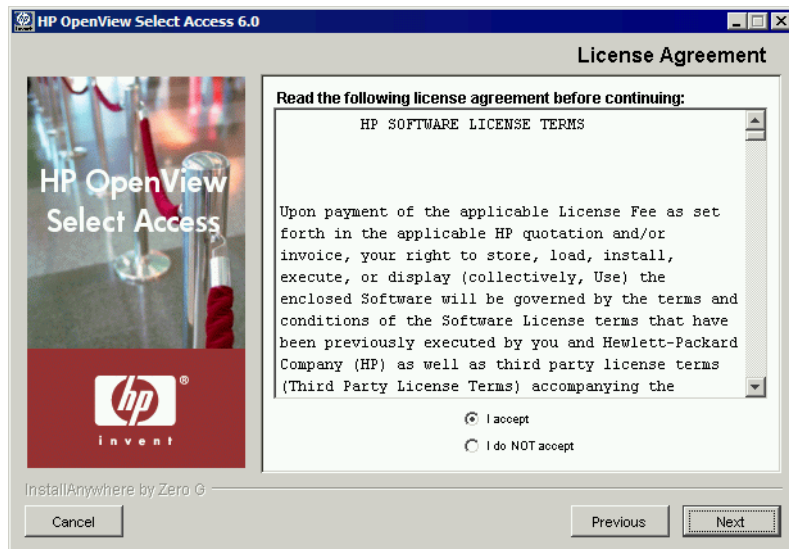


Figure 92: The License Agreement screen

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.

-
- i** 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, run the installer in modify mode. For details, see *Modifying Select Access* on page 220.
-

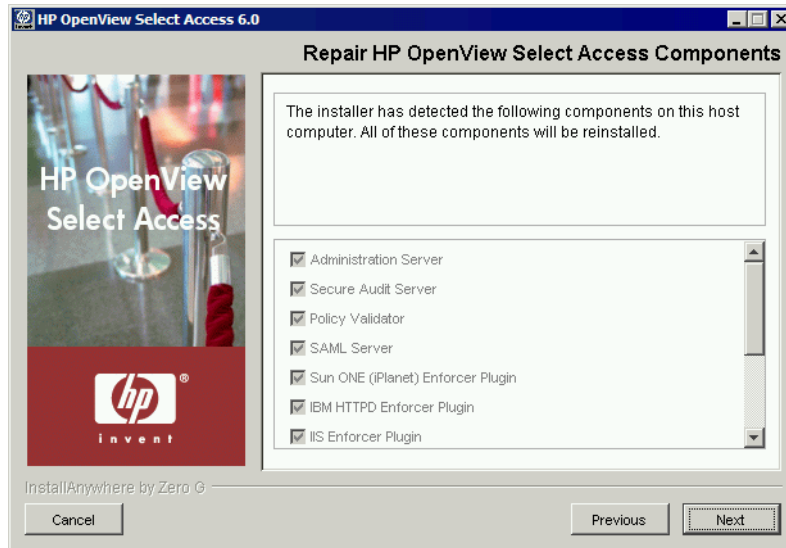


Figure 93: The Repair HP OpenView Select Access Components screen

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

! If you are running any of your Policy Validators in debug mode, the installer cannot detect that it is running. Consequently, the Policy Validator is not shut down and its files cannot be modified.

- i** 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.

The **Pre-Installation Summary** screen appears.



Figure 94: The 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 6.0)
- The install path of Select Access.

On Windows, the install path is:

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

On Unix, the install path is:

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

- The folder that holds the program shortcuts for the Select Access administration tools (for example, Policy Builder or the Setup Tool) that is installed to the Windows **Start** menu. Program shortcuts are added to the **Start>Programs>HP OpenView>Select Access** program group. As well, Select Access shortcuts also are installed to your desktop.
- 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.



Although a dialog appears with options for Internet Explorer and Netscape 6 when you install the Java plugin, the plugin (and therefore, the Policy Builder applet) also works on Netscape 4.

- 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 6.0** screen appears and outlines the installation progress of the components you selected to install.

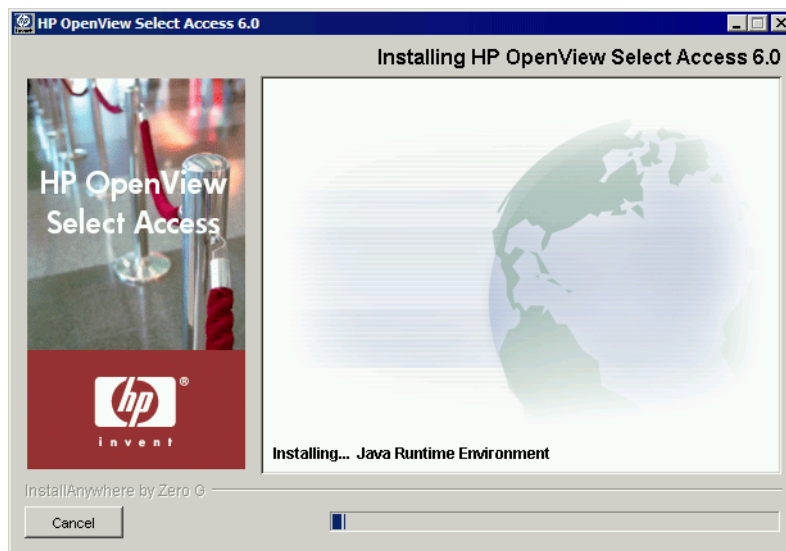


Figure 95: The Installing HP OpenView Select Access 6.0 screen

7. Upon completion, if the installer automatically stopped services for you, the **Restart HP OpenView Select Access Services** screen appears. If you stopped your own services before repairing Select Access, skip to step 11. Ensure that you restart the services that you had stopped manually after you exit this wizard.

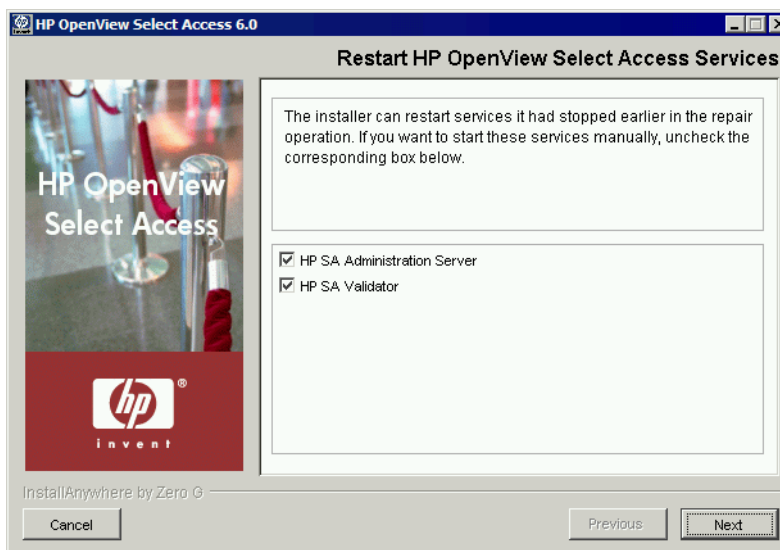


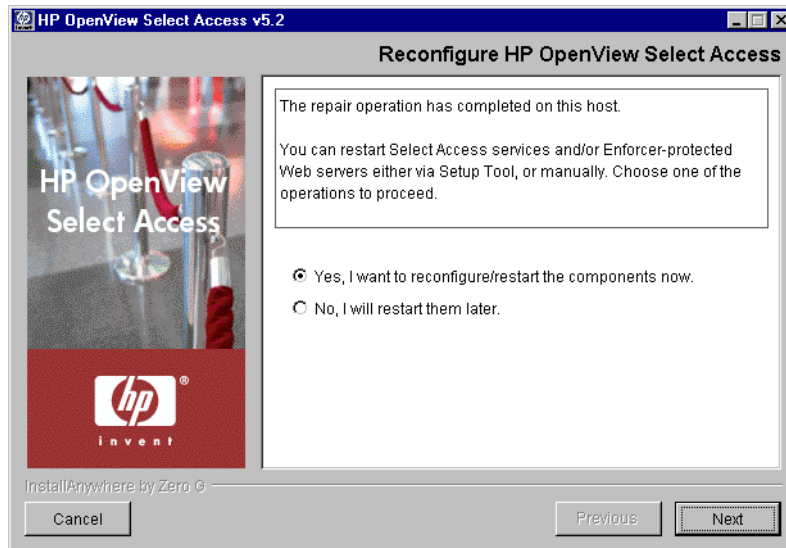
Figure 96: The Restart HP OpenView Select Access Services screen

8. 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).

9. Click **Next**. The components and services you selected are automatically restarted. When the maintenance program is finished, the **Reconfigure HP OpenView Select Access** screen appears.



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*.
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.

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. For details, see *About the selectaccess.conf file* on page 52.
 - Cleans up all temporary installation files.

To repair detected components 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 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 6.0** screen appears.



If you are maintaining Select Access with the installer, only the Repair and Modify options appear. You cannot uninstall components with the installer.



If you are running any of your Policy Validators in debug mode, the installer cannot detect that it is running. Consequently, the Policy Validator is not shut down and its files cannot be modified.

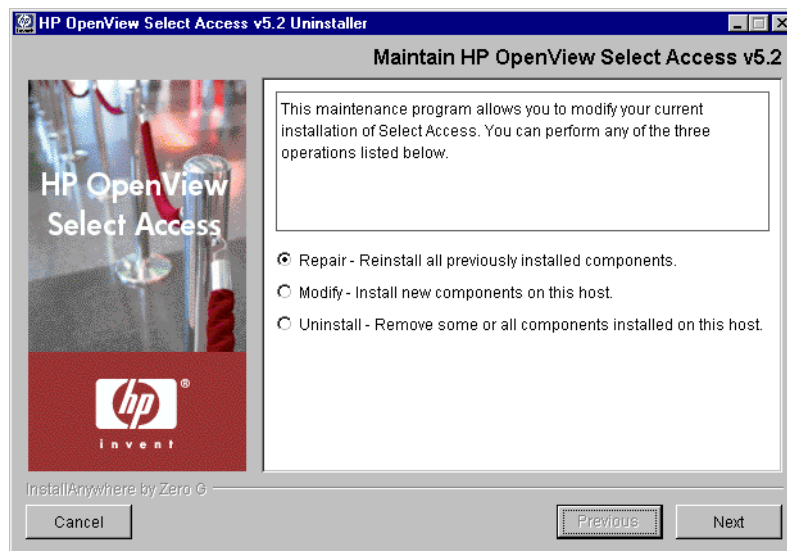


Figure 97: The Maintain HP OpenView Select Access 6.0 screen

2. To reinstall all of Select Access 6.0, click the **Repair** option and click the **Next** button. The **Run Installer in Repair Mode** screen appears.

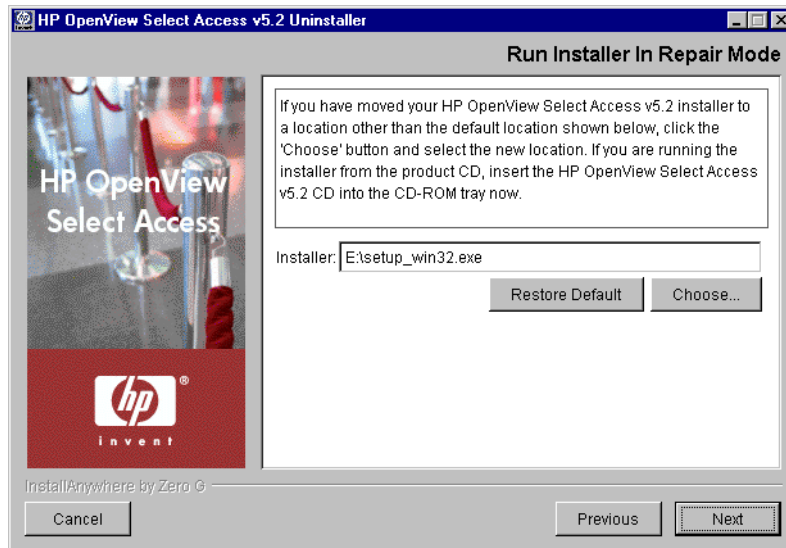


Figure 98: The Run Installer in Repair Mode screen

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, 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, it uses the path 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 avoid generating an error in the installer's log file, ensure the installer resides in the same directory as the Select Access `docs` folder. To ensure this outcome, 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 **Repair HP Select Access 6.0** screen appears.

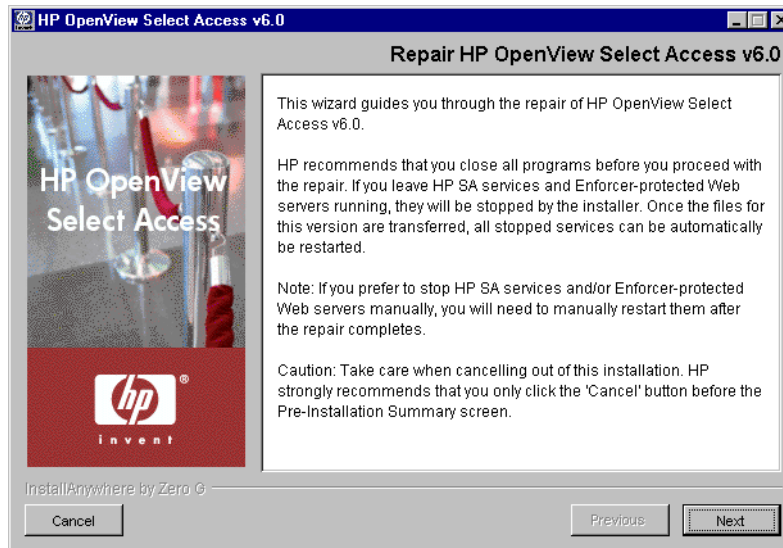


Figure 99: The Repair HP Select Access 6.0 screen

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

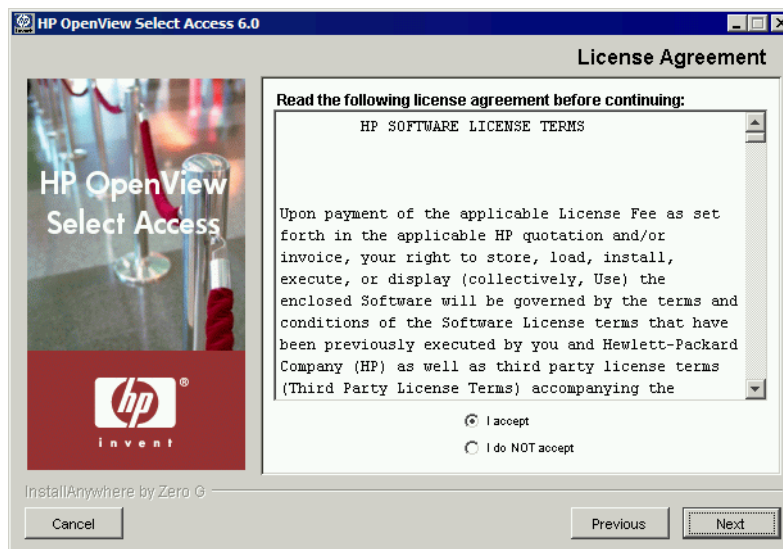



Figure 100: The License Agreement screen

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.

-
- i** 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 226.
-

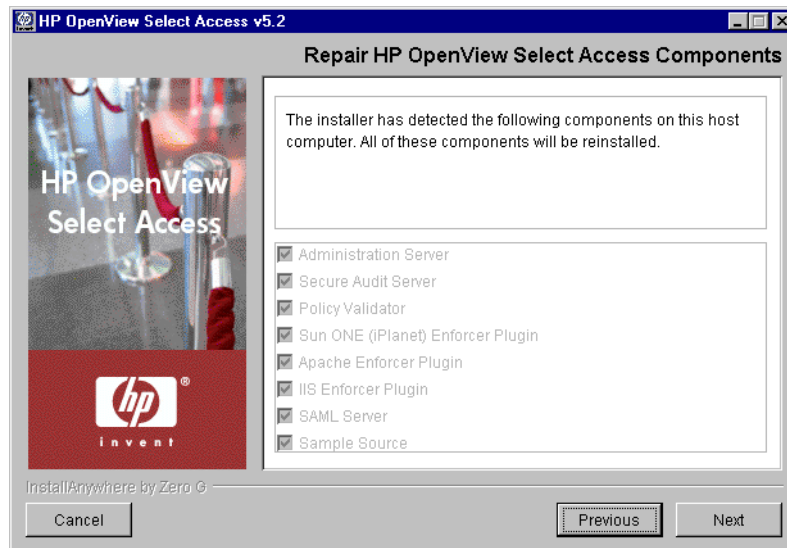


Figure 101: The Repair HP Select Access Components screen

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

! If you are running any of your Policy Validators in debug mode, the installer cannot detect that it is running. Consequently, the Policy Validator is not shut down and its files cannot be modified.

- i** On Windows, if you have any Enforcer-protected Web servers 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 can only manually stop the Web servers. The installer cannot do this automatically on these hosts.

The **Pre-Installation Summary** screen appears.



Figure 102: The 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 6.0)
- The install path of Select Access.

On Windows, the install path is:

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

On Unix, the install path is:

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

- The folder that holds the program shortcuts for the Select Access administration tools (for example, Policy Builder or the Setup Tool) that is installed to the Windows **Start** menu. Program shortcuts are added to the **Start>Programs>HP OpenView>Select Access** program group. As well, Select Access shortcuts also are installed to your desktop.
- 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.



Although a dialog appears with options for Internet Explorer and Netscape 6 when you install the Java plugin, the plugin (and therefore, the Policy Builder applet) also works on Netscape 4.

- 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 6.0** screen appears and outlines the installation progress of the components you selected to install.

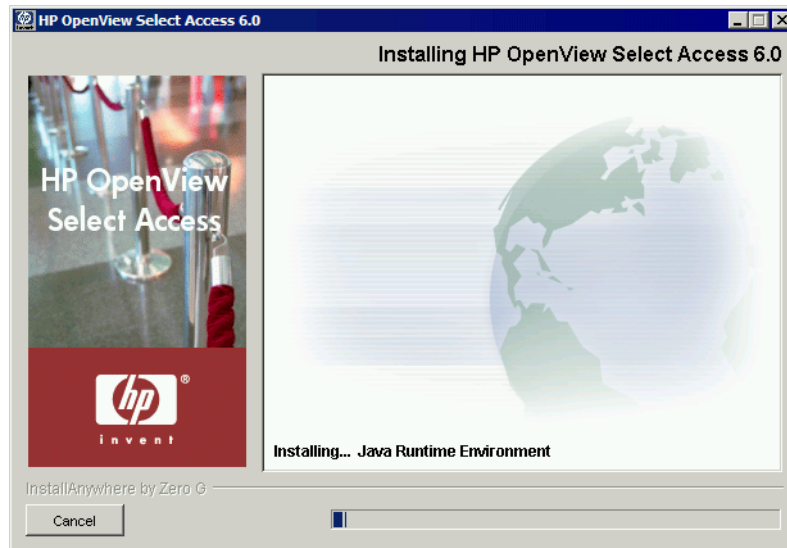


Figure 103: The Installing HP Select Access 6.0 screen

9. Upon completion, if the installer automatically stopped services for you, the **Restart HP Select Access Services** screen appears.
- If you stopped your own services before repairing Select Access, skip to step 11. Ensure that you restart the services that you had stopped manually after you exit this wizard.

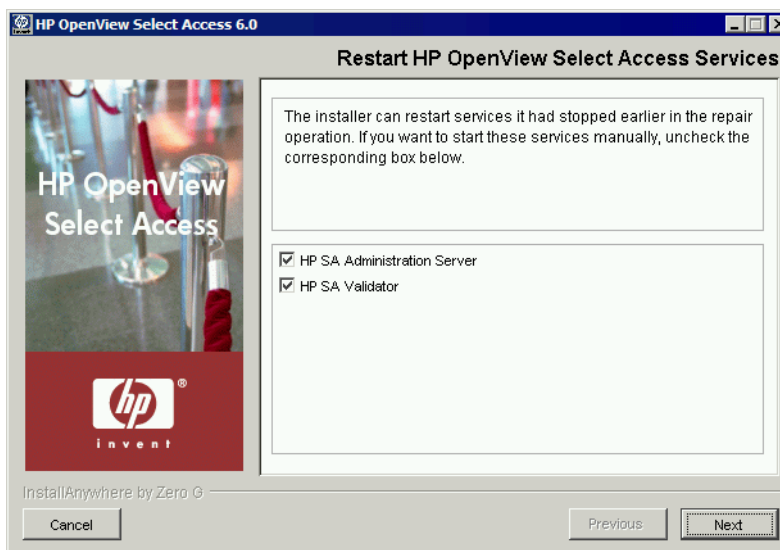


Figure 104: The Restart HP Select Access Services screen

10. 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).

11. Click **Next**. The components and services you selected are automatically restarted.
12. Click **Next**. The components and services you selected are automatically restarted. When the maintenance program is finished, the **Reconfigure HP Select Access** screen appears.

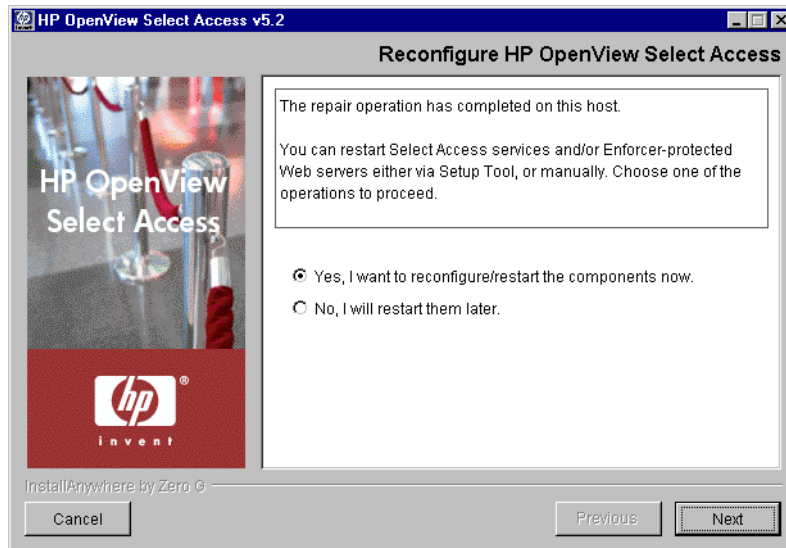


Figure 105: The Reconfigure HP OpenView Select Access screen

13. 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.**
14. 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 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 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 (if applicable) Select Access, 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. For details, see *About the selectaccess.conf file* on page 52.
 - 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 the current installation of Select Access with the installer

1. Run the Select Access installer. The **Maintain HP OpenView Select Access 6.0** screen appears.

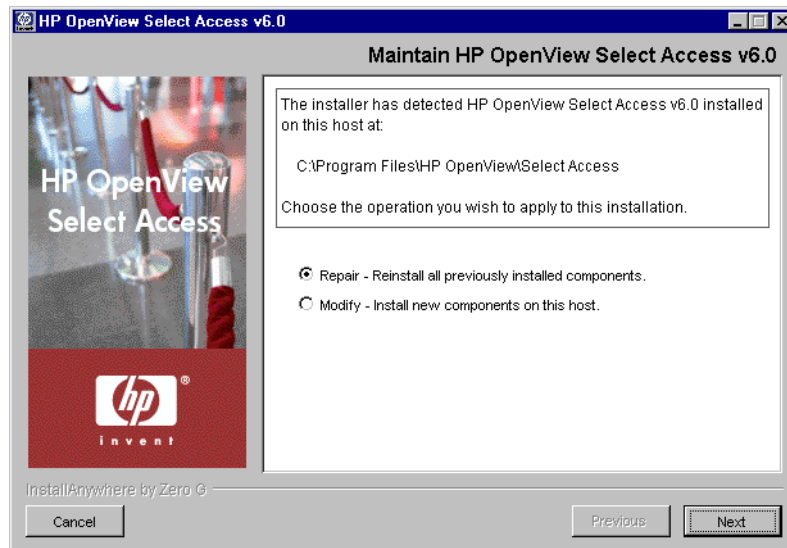


Figure 106: The Maintain HP OpenView Select Access 6.0 screen

2. Click the **Modify** option. The **Modify HP OpenView Select Access 6.0** screen appears.

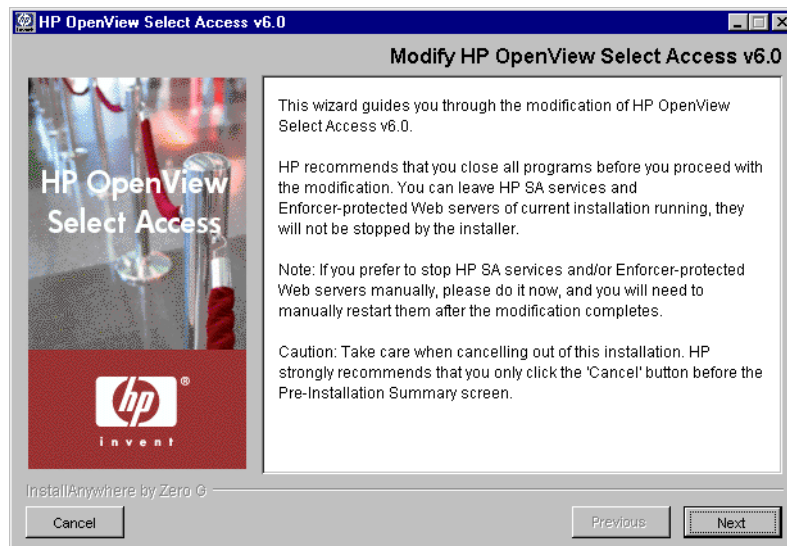


Figure 107: The Modify HP OpenView Select Access 6.0 screen

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

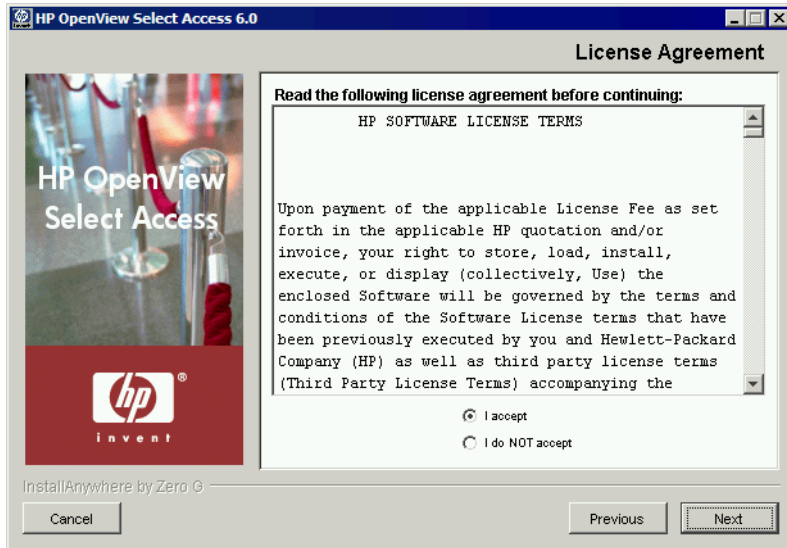


Figure 108: The License Agreement screen

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. This screen lists all components that are detected on this host computer. The maintenance program reinstalls the corresponding files for these components.

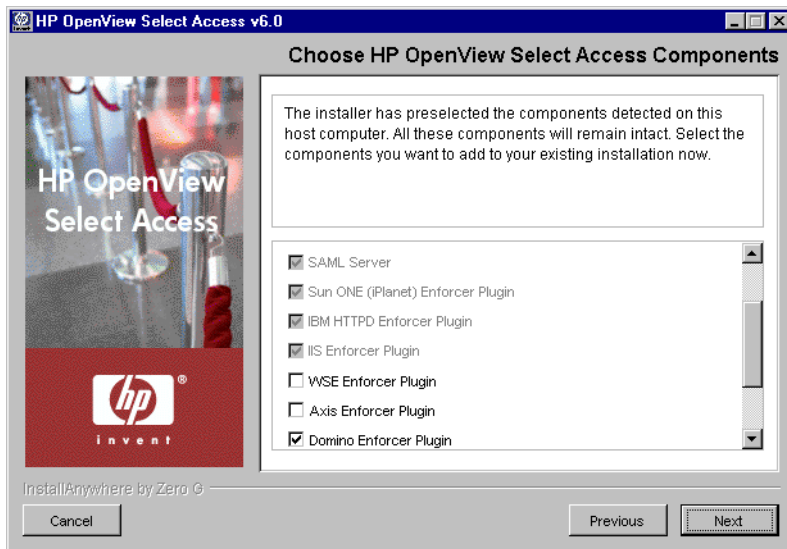


Figure 109: The Choose HP OpenView Select Access Components screen

5. Choose the additional components you wish to install together with the components that already exist on this host machine. The maintenance program installs all checked components (previously installed or new).
6. 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.



If you are running any of your Policy Validators in debug mode, the installer cannot detect that it is running. Consequently, the Policy Validator is not shut down and its files cannot be modified.



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.

The **Pre-Installation Summary** screen appears.



Figure 110: The 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 6.0)
- The install path of Select Access.


On Windows, the install path is:

C:\Program Files\HP OpenView>Select Access

On Unix, the install path is:


/opt/OV/SelectAccess

- The folder that holds the program shortcuts for the Select Access administration tools (for example, Policy Builder or the Setup Tool) that is installed to the Windows **Start** menu. Program shortcuts are added to the **Start>Programs>HP OpenView>Select Access** program group. As well, Select Access shortcuts also are installed to your desktop.
- 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.

 Although a dialog appears with options for Internet Explorer and Netscape 6 when you install the Java plugin, the plugin (and therefore, the Policy Builder applet) also works on Netscape 4.

- 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 6.0** screen appears and outlines the installation progress of the components you selected to install.

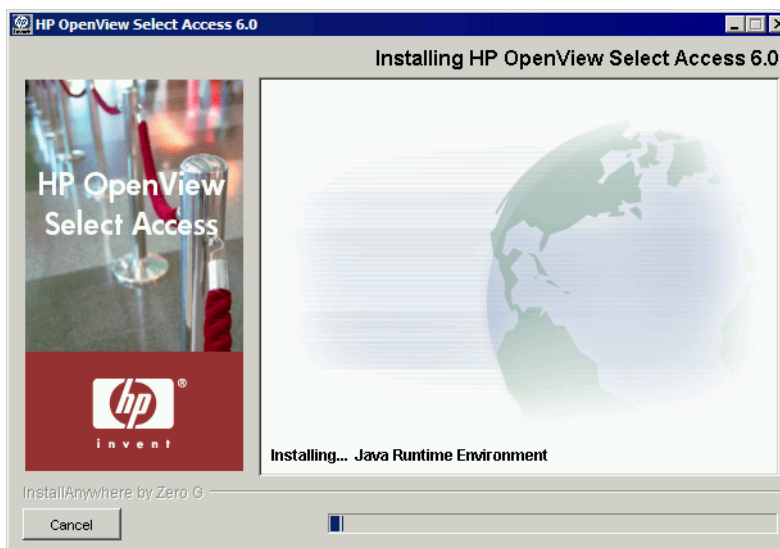


Figure 111: The Installing HP OpenView Select Access 6.0 screen

8. Upon completion, if the installer automatically stopped services for you, the **Restart HP OpenView Select Access Services** screen appears. If you stopped your own services before repairing Select Access, skip to step 11. Ensure that you restart the services that you had stopped manually after you exit this wizard.



Figure 112: The Restart HP OpenView Select Access Services screen

9. 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.

i 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).

10. Click **Next**. The components and services you selected are automatically restarted. When the maintenance program is finished, the **Reconfigure HP OpenView Select Access** screen appears.

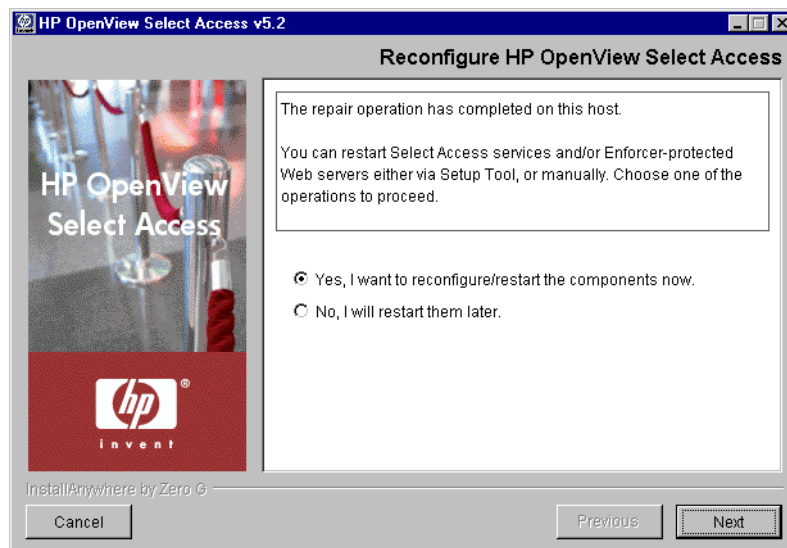


Figure 113: The Reconfigure HP OpenView Select Access screen

11. 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.**
12. When the installer is finished repairing and reconfiguring (if applicable) Select Access, the **Installation Complete** screen appears.
13. If errors were generated, click the **View install log** box to review the messages for those errors.
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 52.
- 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 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 following **Maintain HP OpenView Select Access 6.0** screen appears.



If you are running any of your Policy Validators in debug mode, the installer cannot detect them. Consequently, the Policy Validator is not shut down and its files cannot be modified.

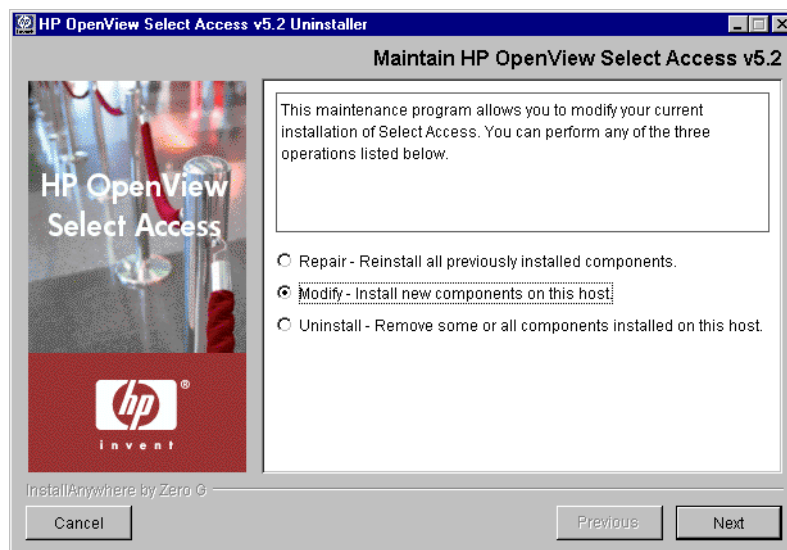


Figure 114: The Maintain HP OpenView Select Access 6.0 screen

2. To uninstall all or part of Select Access 6.0, click the **Modify** option and click the **Next** button. The **Run Installer in Modify Mode** screen appears.

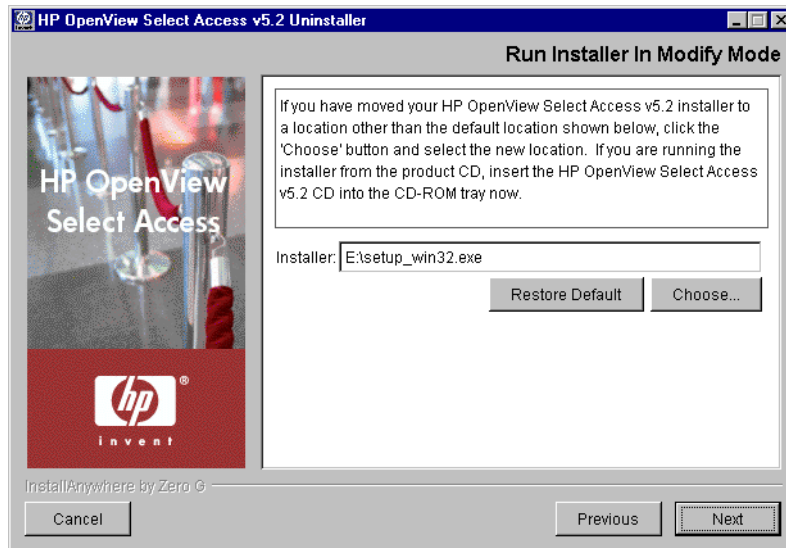


Figure 115: The Run Installer in Modify Mode screen

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, 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, it uses the path 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 avoid generating an error in the installer's log file, 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 6.0** screen appears.

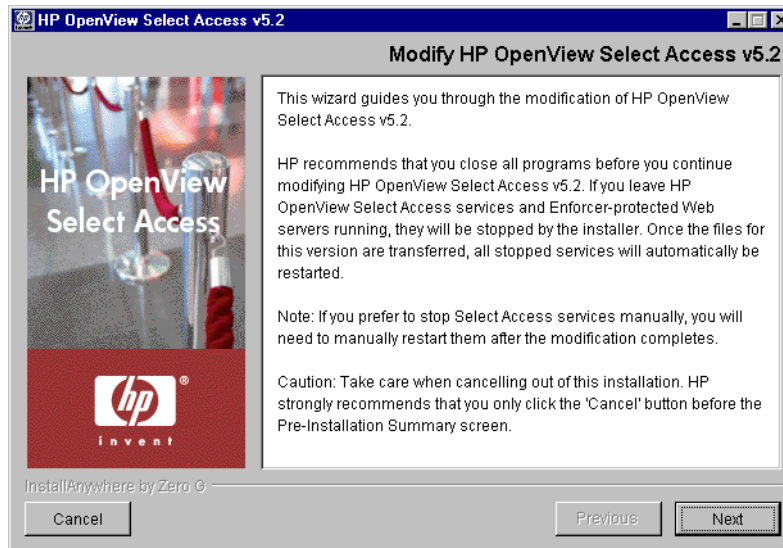


Figure 116: The Modify HP OpenView Select Access 6.0 screen

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

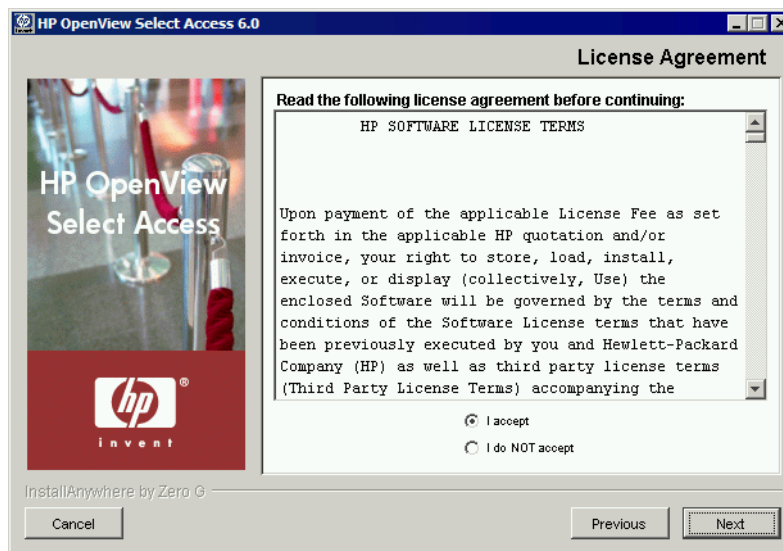


Figure 117: The License Agreement screen

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. This screen lists all components that are detected on this host computer. The maintenance program reinstalls the corresponding files for these components.

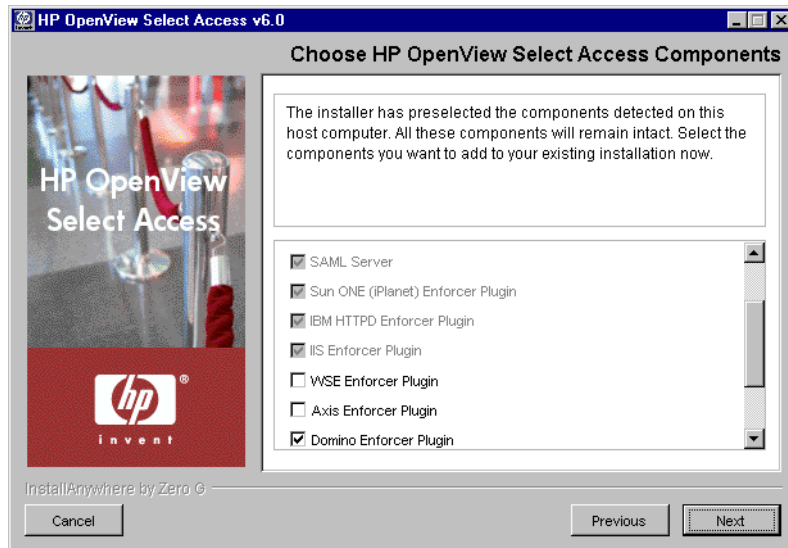


Figure 118: The Choose HP OpenView Select Access Components screen

7. Choose the additional components you wish to install together with the components that already exist on this host machine. The maintenance program installs all checked components (previously installed or new).
8. Click **Next**. If any HP services are running, the maintenance program displays a warning message. Click **OK** to let the installer automatically stop them for you. Otherwise, stop them manually now.



If you are running any of your Policy Validators in debug mode, the installer cannot detect that it is running. Consequently, the Policy Validator is not shut down and its files cannot be modified.



On Windows, if you have any Enforcer-protected Web servers 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 can only manually stop the Web servers. The installer cannot do this automatically on these hosts.

The **Pre-Installation Summary** screen appears.



Figure 119: The 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 6.0)
- The install path of Select Access.

On Windows, the install path is:

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

On Unix, the install path is:

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

- The folder that holds the program shortcuts for the Select Access administration tools (for example, Policy Builder or the Setup Tool) that is installed to the Windows **Start** menu. Program shortcuts are added to the **Start>Programs>HP OpenView>Select Access** program group. As well, Select Access shortcuts also are installed to your desktop.
- 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.



Although a dialog appears with options for Internet Explorer and Netscape 6 when you install the Java plugin, the plugin (and therefore, the Policy Builder applet) also works on Netscape 4.

- 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 6.0** screen appears and outlines the installation progress of the components you selected to install.

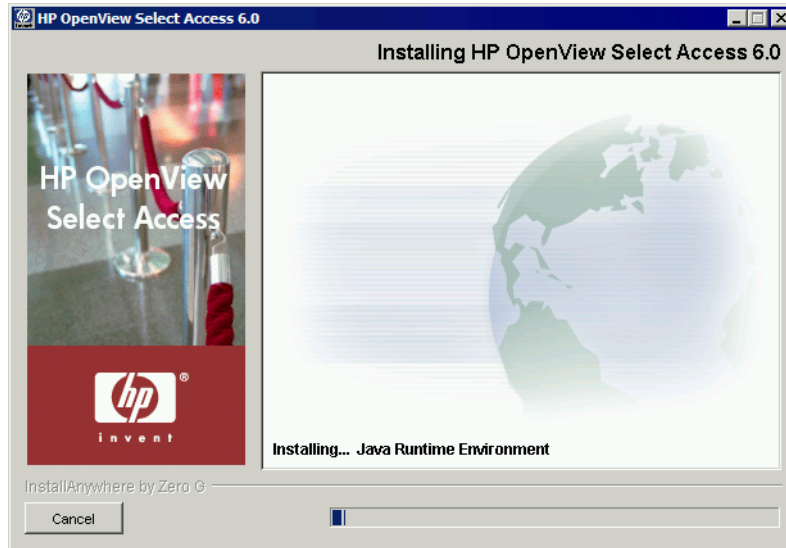


Figure 120: The Installing HP OpenView Select Access 6.0 screen

10. Upon completion, the **Restart HP OpenView Select Access Services** screen appears.

i If you stopped your own services before repairing Select Access, skip to step 12. Ensure that you restart the services that you had stopped manually after you exit this wizard.

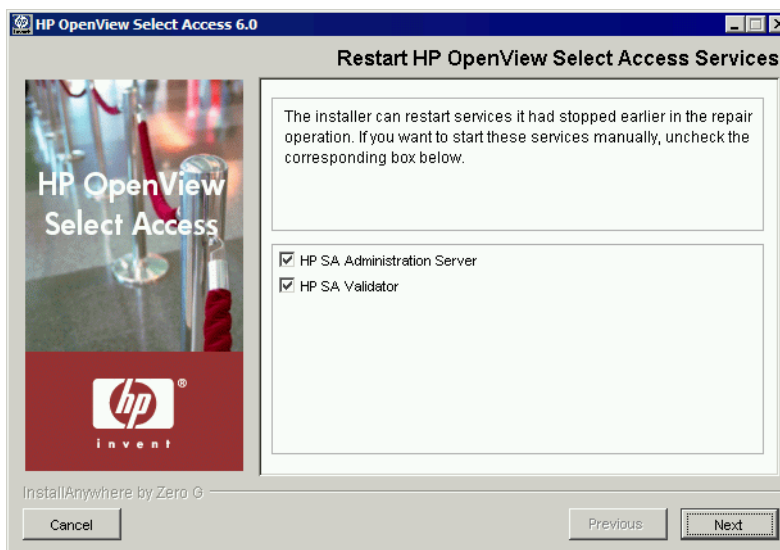


Figure 121: The Restart HP OpenView Select Access Services screen

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).

12. Click **Next**. The components and services you selected are automatically restarted. The **Configure Newly Installed Components** screen appears.

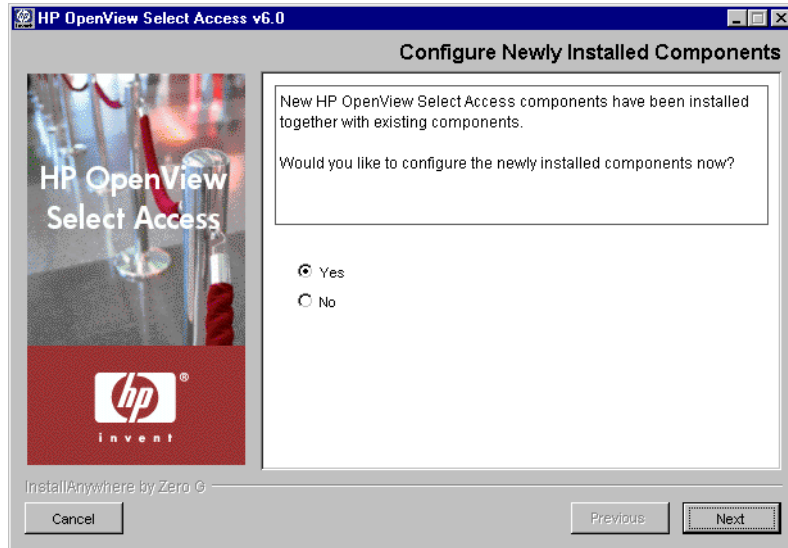


Figure 122: The Configure Newly Installed Components screen

13. Click **Next**. The components and services you selected are automatically restarted. When the maintenance program is finished, the **Reconfigure HP OpenView Select Access** screen appears.

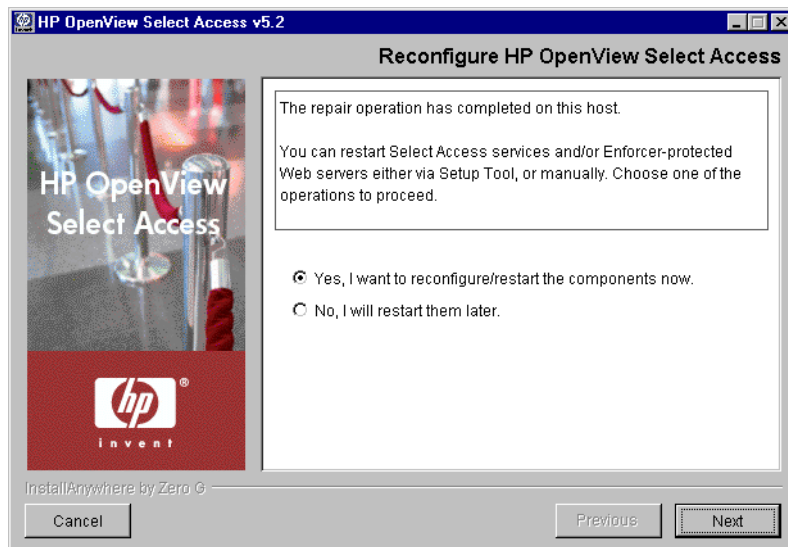


Figure 123: The Reconfigure HP OpenView Select Access screen

14. 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.**
15. 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*.

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 (if applicable) Select Access, the **Installation Complete** screen appears.

16. If errors were generated, click the **View install log** box to review the messages for those errors.
17. 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 52.
 - 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 directory server.



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.



If you are running any of your Policy Validators in debug mode, the installer cannot detect that it is running. Consequently, the Policy Validator is not shut down and its files cannot be removed.

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 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 following **Maintain HP OpenView Select Access 6.0** screen appears.

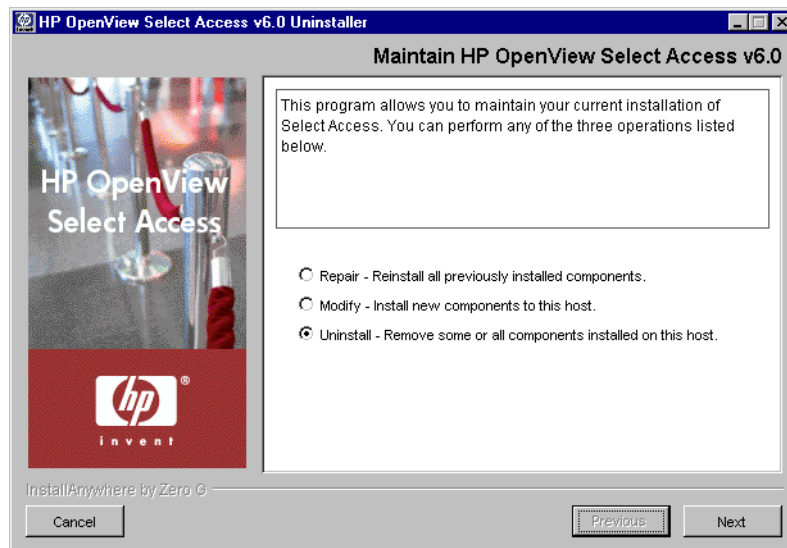


Figure 124: The Maintain HP OpenView Select Access 6.0 screen

2. To uninstall all or part of Select Access 6.0, click the **Uninstall** option and click the **Next** button. The **Choose HP OpenView Select Access Components** screen appears.

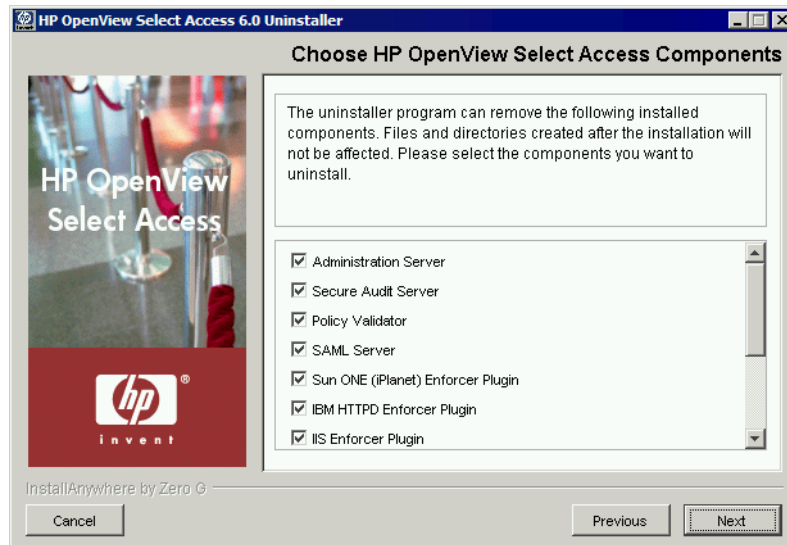


Figure 125: The Choose HP OpenView Select Access Components screen

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 appears. If you are only uninstalling some components, skip to step 6.

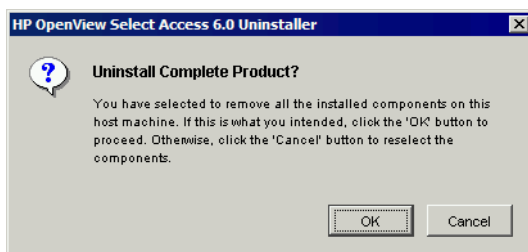


Figure 126: The Uninstall Complete Product dialog

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.

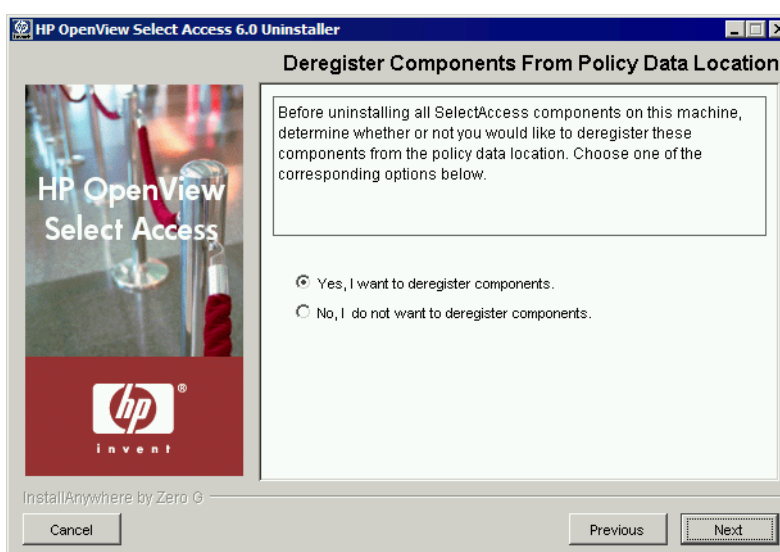


Figure 127: The Deregister Components from Policy Data Location screen

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.

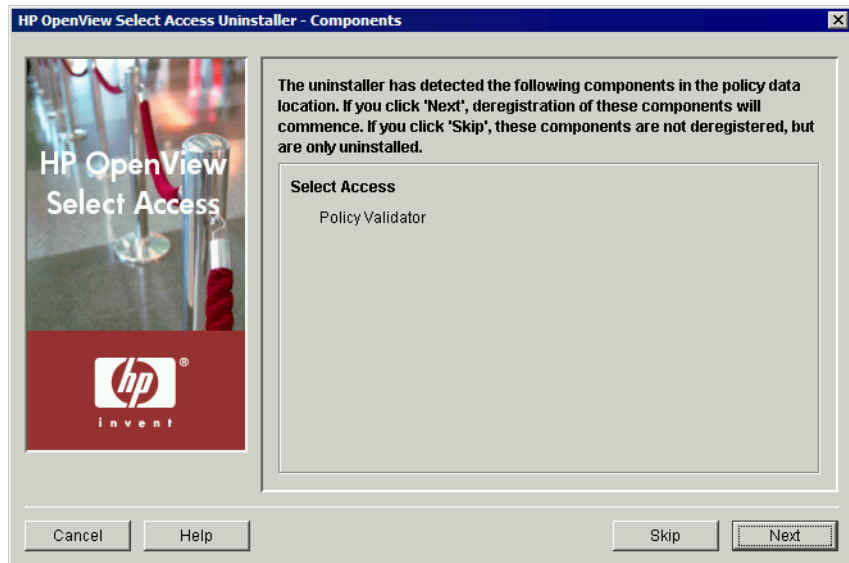


Figure 128: The Deregistration screen

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 following **HP OpenView Select Access Uninstaller - Contact the Administration Server** screen appears in Figure 129.

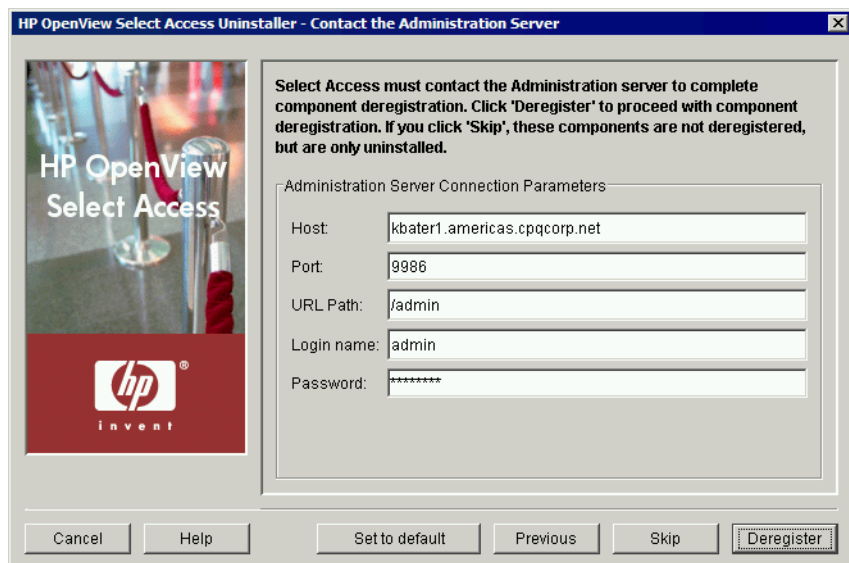


Figure 129: The Contact the Administration Server screen

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 has been installed.
 - **Port:** Required. Enter the port the administration server is running on. By default the port is 9986.
 - **Login name:** Required. Enter the user name to log into the Administration Server.
 - **Password:** Required. Enter the password to log into the Administration Server.
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.



If you are running any of your Policy Validators in debug mode, the uninstaller cannot detect that it is running. Consequently, the Policy Validator is not shut down and its files cannot be removed.



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 can only 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.

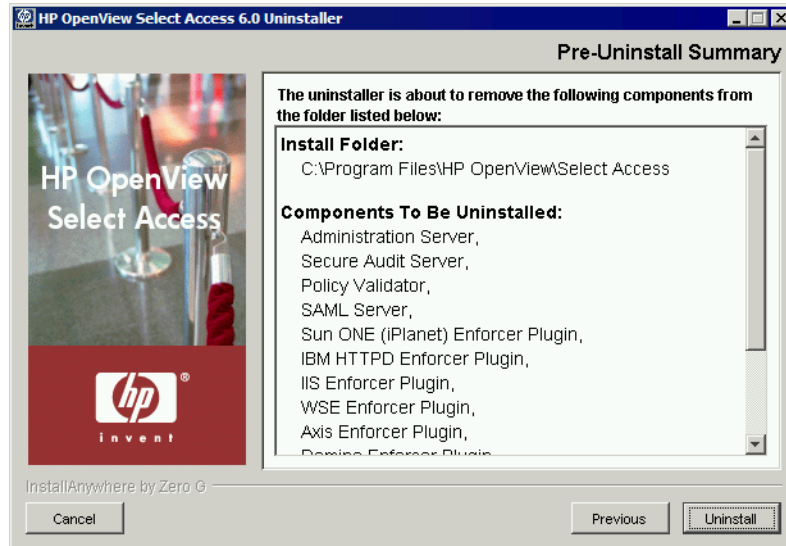


Figure 130: The Pre-Uninstall Summary screen

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 it is finished, the **Uninstall Complete** screen appears.

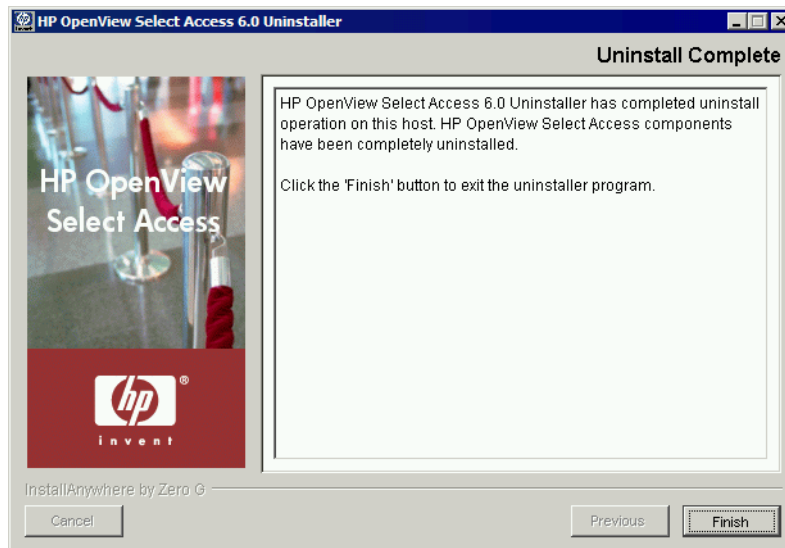


Figure 131: The Uninstall Complete screen

15. Click **Finish** to exit the uninstaller. This also removes the local files for the uninstalled components as well as the following:
 - Registry entries on Windows hosts.

- `/etc/selectaccess.conf` and the `openssl` 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 user-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.

Localizing Select Access interfaces and rendering localized data

With the release of Select Access 6.0, HP has now offers complete internationalized data support, as well as giving you the ability to localize following Select Access Java components:

- The Policy Builder
- The Setup Tool

Translating and loading localized resource bundles

You can install Select Access on an international operating system without any change. Because the Java Runtime Environment (JRE) can search the proper logical font file according to your platform setting, you simply need to use the default international characters on your system.

To localize interfaces, simply create a new resource bundle for each new language. No recompiling of code is required. However, you do need to translate the English resource bundle shipped with Select Access to support your native language. Table 31 summarizes the

procedure for customizing the native language support displayed by Select Access.

Table 31: Customizing native language support

This step...	For details, see...
1. Expand the <code>SAResourceBundle.jar</code> file.	<i>Using Select Access's resource bundle on page 242</i>
2. Translate HP's default English resource bundles to your native language. Note: You need to save each resource bundle with the corresponding Java-appropriate file name.	<i>Translating extracted resource bundles on page 243</i>
3. If necessary, convert the translated resource bundles into native Unicode before adding them to <code>SAResourceBundle.jar</code> file.	<i>Translating extracted resource bundles on page 243</i>

Using Select Access's resource bundle

All Java components' resource bundles have been archived in a single file called `SAResourceBundle.jar`. By default, you can find this file in the `<install_path>\shared\jetty\policy_builder\protected` folder. The `SAResourceBundle.jar` file includes all the resource bundles for elements of the Policy Builder's and Setup Tool's interface.

To expand the `SAResourceBundle.jar` file

1. Open the `SAResourceBundle.jar` file that contains all archived resource bundles for Select Access's interfaces. You can do this either via any archive/compression tool (for example, WinZip).
2. Expand the contents of the JAR file to Select Access's top level folder. By default, all compressed resource bundles are expanded to their corresponding `<expansion_root>\com\hp\ov\selectaccess` folder, as illustrated in Table 32. The location of this folder varies depending on where you are extracting the files to.

Table 32: Locations of expanded resource bundles

This file...	Is expanded to this folder...
<code>Util_ResBundle.properties</code>	<code><expansion_root>\com\hp\ov\selectaccess\util</code>
<code>PolicyBuilder_ResBundle.properties</code>	<code><expansion_root>\com\hp\ov\selectaccess\policybuilder</code>
<code>PolicyBuilder_Common_ResBundle.properties</code>	<code><expansion_root>\com\hp\ov\selectaccess\policybuilder\common</code>

Table 32: Locations of expanded resource bundles (Continued)

This file...	Is expanded to this folder...
PolicyBuilder_Interf_ResBundle.properties	<expansion_root>\com\hp\ov\selectaccess\policybuilder\interfaces
PolicyBuilder_Rpt_ResBundle.properties	<expansion_root>\com\hp\ov\selectaccess\policybuilder\reporting
Setup_ResBundle.properties	<expansion_root>\com\hp\ov\selectaccess\setup
Setup_Config_ResBundle.properties	<expansion_root>\com\hp\ov\selectaccess\setup\config
RuleBuilder_ResBundle.properties	<expansion_root>\com\hp\ov\selectaccess\rulebuilder
RuleBuilder_Scr_ResBundle.properties	<expansion_root>\com\hp\ov\selectaccess\rulebuilder\screens
Widgets_ResBundle.properties	<expansion_root>\com\hp\ov\selectaccess\widgets

Translating extracted resource bundles

You can translate the resource bundles you extract using any tools the translator typically uses. When translating these resource bundles, note that contents in the bundles follow this format:

```
<ID_Number>=<Translatable_string>
```

Where:

- *<ID_Number>* is the method of identification used by Select Access components to load the appropriate string on a given screen. Translators should not modify this ID number or create new IDs.
- *<Translatable_string>* is the string that is loaded.

To translate resource bundles

1. Open the resource file in any translation tool or text editor.
2. Translate the *<Translatable_string>* elements in these files to your native language.
3. Save the file using the filename syntax required by Java for the language you have translated the resource bundle to. For example, if you are translating `Util_ResBundle.properties` to Thai, you would save the file as `Util_ResBundle_th.properties`.



Do not overwrite the English file. That way, if users install Select Access on a host machine that is configured to run in English, the correct resource bundle is automatically used by default.

Converting translated files to Unicode

Once you have translated all files in one or more native languages, you need to convert them to Unicode. This is required by all languages except English. You can use the Sun's `native2ascii` converter for this purpose. The `native2ascii` converter converts a file with native-encoded characters (characters which are non-Latin 1 and non-Unicode) to one with Unicode-encoded characters. For more information on this tool, visit <http://java.sun.com/j2se/1.3/docs/tooldocs/win32/native2ascii.html>.

To use the `native2ascii` converter to convert your translated files

1. From the command line, enter the following command:

```
<path>\native2ascii -encoding <type> [inputfile  
[outputfile]]
```

Where `<type>` is the native language code you require. For example, UTF8. For details on what encodings are supported, see <http://java.sun.com/j2se/1.3/docs/guide/intl/encoding.doc.html>.

For example, `c:\jdk1.3.1_02\bin\native2ascii -encoding MS874 C:\WINNT\Profiles\myprofile\Desktop\com\hp\ov\selectaccess\utilUtil_ResBundle_th.properties C:\WINNT\Profiles\myprofile\Desktop\com\hp\ov\selectaccess\utilUtil_ResBundle_th_TH.properties`

2. Exit the `native2ascii` converter.
3. Add the converted resource bundle files to the `SAResourceBundle.jar` file.

Supporting internationalized data

Select Access supports internationalized data. That means users can enter data in their web browser in their native language and have the same characters correctly displayed in the Select Access system.

Using your own fonts

Like with localized interfaces, you can install Select Access on an international operating system without any change. Because the Java Runtime Environment (JRE) can search the proper logical font file according to your platform setting, you simply need to use the default international characters on your system.

If you want to use your own fonts rather than the system defaults, you need to manually configure the logical font files to ensure data renders in Select Access correctly. Depending on your platform, this procedure varies. For details, see *Rendering localized fonts in Select Access* on page 246.

There are two kinds of fonts with which you must familiarize yourself before localizing Select Access: physical fonts and logical fonts. The

corresponding sections that follow describe these fonts in greater detail. For details, see *Physical Fonts* on page 245 and *Logical fonts* on page 245.

Physical Fonts

Physical fonts are the font libraries that your system physically stores. They are libraries of glyphs that often include a subset of the Unicode characters your system requires. In most cases, you install physical fonts with the operating system or with third-parties (either font vendors or application providers). Typically, your system – and the applications like Select Access that run on it, use TrueType fonts.

To check the physical fonts on Windows

1. Open the **Control Panel**.
2. Click the **Fonts** icon. This displays all the font names and their associated font filenames.

To check the physical fonts on Solaris

1. Open the `/usr/openwin/lib/locale/<locale>` directory.



While you install most physical fonts in this location, you can install others to different locations (for example, `/usr/openwin/lib/locale/<locale>/X11/fonts`). Ensure you check other areas of your host computers as well.

2. Look for filenames with an `x1fd` string.

Logical fonts

Logical fonts group physical fonts under a virtual name and use a named set of formatting parameters that define the weight of a font. Logical fonts support Java Select Access by defining the fonts components needed, without having to actually install the physical font on your system. By default, there are the five font types recognized by the JRE. Table 33 defines the two properties for each logical font:


`<fonttypename>.<style>`

Table 33: Logical fonts

These logical font types...	Can have these styles...
Serif	plain
Sans-serif	bold
Monospaced	<i>italic</i>

Table 33: Logical fonts (Continued)

These logical font types...	Can have these styles...
Dialog	<i>bolditalic</i>
DialogInput	

 One logical font can use multiple physical fonts.

Rendering localized fonts in Select Access

The `font.properties` file is the JRE implementation detail that softcodes the names of one or more physical fonts to a logical name, so the font's physical presence is not required. This combination defines when and how Select Access is to use a font to display or print characters. This definition ensures that Select Access functions as a localized program using the fonts you define.

If you want to use your own fonts rather than the system defaults, you need to manually configure the logical font files. Table 34 outlines the steps required for configuring the `font.properties` files:

Table 34: Steps to localize Select Access data

Step required	For details, see...
1. Determine your regional settings. Your regional settings help you to identify your locale and consequently your language.	<i>Identifying your locale on Windows on page 247</i> or <i>Identifying your locale on Solaris on page 247</i>
2. Determine which font file you need for your locale.	<i>Supported locales for Windows on page 248</i> or <i>Supported locales for Solaris on page 248</i>
3. If you are localizing a Windows component, collect information on the physical fonts you are mapping logical names to.	<i>Identifying physical fonts on Windows on page 249</i>

Table 34: Steps to localize Select Access data (Continued)

Step required	For details, see...
4. If you are localizing a Solaris component, install and/or copy the physical fonts you are mapping logical names to.	<i>Installing the correct font on Solaris on page 250</i>
5. Open the corresponding <code>font.properties</code> file and map physical fonts to a logical name.	<i>Mapping the physical font to a logical name on Windows on page 250</i> or <i>Mapping the physical font to a logical name on Solaris on page 254</i>

Identifying your locale on Windows

In Windows, you define the locale by the regional settings that you have configured your system for. This makes identification of your locale relatively simple.

1. Click the **Regional Settings** icon in **Control Panel**. This displays the **Regional Settings Properties** dialog that defines the locale you are in.
2. Click the **Regional Settings** tab. Depending on the region you select, you need to use one of the corresponding `font.properties` file for your locale's language.



To view Japanese characters correctly while running the Policy Builder on an English version of Windows, make `font.properties.ja` the default font properties file by renaming it to `font.properties`. You will need to open the Java plugin control panel applet (from the Windows control panel) and clear its cache, then restart the Policy Builder before the changes will take effect.

Identifying your locale on Solaris

By default, Select Access installs the `font.properties` files required by most locales. The installer installs these fonts to the following directory:

```
<install_path>\jre\lib
```

You determine the locale of any operating system by using the `System.getProperty` command (`user.language`, `user.region`, and

`file.encoding` parameters respectively) to return `<language>`, `<region>` and `<encoding>` information.



Different operating system versions have different font requirements. For example, Solaris 2.5.1 does not support TrueType fonts. In these cases, `font.properties` files must necessarily be operating system-specific and are named accordingly using the following syntax:

```
font.properties.<osVersion>
```

Supported locales for Windows

By default, Select Access installs the `font.properties` files required by most locales. The installer installs these fonts (listed in Table 29) to the following directory:

```
<install_path>\jre\lib
```

For example, if the language of your regional setting (locale) is th (Thai), Java searches for the `font.properties.th` file. If the JRE cannot find the `font.properties.th` file, it searches for the `font.properties` file and uses it instead.

This language...	Requires this font file...
Arabic	<code>font.properties.ar</code>
Hebrew	<code>font.properties.iw</code>
Japanese	<code>font.properties.ja</code>
Korean	<code>font.properties.ko</code>
Russian	<code>font.properties.ru</code>
Thai	<code>font.properties.th</code>
Chinese	<code>font.properties.zh</code>
Chinese on Windows NT	<code>font.properties.zh.nt4.0</code>
Traditional Chinese	<code>font.properties.zh_TW</code>
English or default	<code>font.properties</code>

Supported locales for Solaris

Use the `font.properties` file that corresponds to your particular language environment. You identify the file you need for your language environment by the country or locale suffix that is appended to the filename, as outlined in Table 30:

```
font.properties.<locale>
```

For example, if the language of your locale is `th` (Thai), Java searches for the `font.properties.th` file. If the JRE cannot find the `font.properties.th` file, Java searches for the `font.properties` file and use it instead.



The language suffix precedes any additional suffixes, such as operating system or encoding.

This language...	Requires this font file with this suffix...
Arabic	*.ar
Hebrew	*.iw
Japanese	*.ja
Korean	*.ko
Russian	*.ru
Thai	*.th
Chinese	*.zh
Traditional Chinese	*.zh_TW
English or default	none

When you localize Select Access, it reads the `font.properties` files in the following order:

1. `font.properties.<language>_<region>_<encoding>.<osVersion>`
2. `font.properties.<language>_<region>_<encoding>`
3. `font.properties.<language>_<region>.<osVersion>`
4. `font.properties.<language>_<region>`
5. `font.properties.<language>_<encoding>.<osVersion>`
6. `font.properties.<language>_<encoding>`
7. `font.properties.<language>_<osVersion>`
8. `font.properties.<language>`
9. `font.properties.<encoding>.<osVersion>`
10. `font.properties.<encoding>`
11. `font.properties.<osVersion>`
12. `font.properties`

Identifying physical fonts on Windows

Mapping a physical font to a logical name requires that you make note of the physical font's typeface name and filename:



Make sure you have already installed the physical fonts you want to use. You must install them as a Windows system font.

1. Click the **Fonts** icon in the **Control Panel**. This displays your system's **Fonts** folder.
2. To display all details you need, click **View>Details**. This displays the names of the physical font, as well as other font properties.

Installing the correct font on Solaris

Ensure that you have already installed the physical font you want to use. The `font.properties` file requires the `xldf` string as part of the logical font definition. If you do not have the fonts you need, you can contact SunSoft to request the outline fonts for Solaris environments. You typically install these fonts to the `fonts.dir` directory.

Mapping the physical font to a logical name on Windows

Mapping a physical font to a logical name requires that you edit the `font.properties` file. You can modify the following `font.properties` sections in Table 31, depending on your business needs.

To edit this section...	For details, see...
Logical font mapping	Required. <i>Logical font mapping</i> on page 250.
Font filenames mapping	Required. <i>Physical font filename mapping</i> on page 252
Character conversion	Optional. <i>Character conversion</i> on page 253
Exclusion range	Optional. <i>Range exclusion</i> on page 253

Logical font mapping

The first section you must edit is the logical font mapping section. This section maps a logical name to its physical counterpart(s). When Select Access wants to invoke a font by using a logical name such as *Serif* or *Monospace*, the JRE looks up at the mapping information and loads that physical font into Select Access components.



You cannot create a new logical name. Only use the five names defined and the corresponding style values defined in *Logical fonts* on page 245.

The logical font mapping section uses the following syntax. Table 32 defines this section's parameters.

```
<logicalname>.<style>.<ordernumber>=<physicaltypeface>,  
<charset>, <conversioninfo>
```

Parameter	Description
<logicalname>	One of the five logical font types supported in the JRE. See <i>Logical fonts</i> on page 245 for details.
<style>	One of the four logical font weights supported in the JRE. See <i>Logical fonts</i> on page 245 for details. If you omit the style value, Java assumes the plain style by default.
<ordernumber>	A numerical or position value used to determine the search order when the JRE reads the file. For example, the JRE reads plain.0 before plain.1. Note: All the numbers for one logical font must be in sequence. That is, if you insert a font, you must increase the rest of the order numbers by 1. Also, because the system uses this index to identify the logical font in other sections of the file, you need to apply any changes made to a single entry universally throughout the document.
<physicaltypeface>	The font's typeface name. For example, "Times New Roman." Note: If the physical font uses international characters, use the Unicode value for that font.

Parameter	Description
<code><charset></code>	<p>The character set required by the locale. Possible values include:</p> <ul style="list-style-type: none"> • DEFAULT_CHARSET • ANSI_CHARSET • HANGUL_CHARSET • BALTIC_CHARSET • MAC_CHARSET • CHINESEBIG5_CHARSET • OEM_CHARSET • RUSSIAN_CHARSET • EASTEUROPE_CHARSET • SHIFTJIS_CHARSET • GB2312_CHARSET • SYMBOL_CHARSET • GREEK_CHARSET • TURKISH_CHARSET <p>Note: If you do not know which character set to use with your font, use the DEFAULT_CHARSET.</p>
<code><conversioninfo></code>	<p>An optional setting that defines a different coding index when not using Unicode. You can specify how to convert the Unicode index to this coding index, by using the <code>NEED_CONVERTED</code> parameter. When you specify this parameter, you also need to create a character set converter and specify it in the character conversion section of this file. For details, see <i>Character conversion</i> on page 253.</p>

Physical font filename mapping

The next important section you must modify is the font filename mapping section. This section establishes a mapping between the typeface name and the filename for it. By mapping the typeface name of the font to its filename, you reduce the time Select Access spends trying to find the file for a particular font name. You must map all styles of the typeface used. The syntax for this section is:

```
filename.<typeface_name>_<style>=<physical filename>
```

For example:

```
filename.garamond=gara.ttf
```



This section does not support spaces in this section. Substitute spaces in the typeface name with underscores where necessary.

Character conversion

This section specifies the converter file for fonts flagged with the `NEED_CONVERTED` tag. Most fonts use Unicode indexing. However, if you are using a non-Unicode character set, define the code indexing converter required. The syntax for this section is:

```
fontcharset.<logical name>.<ordernumber>=<converter>
```

where `<logical name>.<order>` must match the corresponding entries from the logical font mapping section of the file and `<converter>` is the name of the java class that converts the file. For example:

```
fontcharset.dialog.1=sun.awt.windows.CharToByteWingDings
```



Select Access ships sample converters. By default, the installer installs these converters in the following directory:

```
<install root>\jre\lib
```

If you find that these converters are insufficient, contact either Sun or a third-party vendor and see what converters they can provide or create your own customized converter.

Range exclusion

Certain fonts contain characters that can overlap. In these cases, perhaps you have a preference for one character in a font over those in others. If ranges or individual characters are redundant, define exclusion information or your physical font. The syntax for excluding these characters is:

```
exclusion.<logicalname>.<ordernumber>=  
<Unicode_startrange>-<Unicode_endrange>
```

For example:

```
exclusion.dialoginput.3=0100-12cd
```

To determine the Unicode value of a character

1. Click **Start>Programs>Accessories>Character Map**. This displays the **Unicode Character Map** utility.
2. Select the physical font from the **Font** list.

3. Select the character set from the **Subset** list.
4. As you select different character sets, compare the characters and see where overlap exists. Make note of those characters accordingly by clicking the glyph and reading the index code that appears in the lower right-hand display area.

Mapping the physical font to a logical name on Solaris

Mapping a physical font to a logical name requires that you edit the `font.properties` file. You can modify the following `font.properties` sections, depending on your business needs, as shown in Table 33.

To edit this section...	For details, see...
Logical font mapping	Required. <i>Logical font mapping</i> below.
Character conversion information	Required. <i>Character conversion</i> on page 256
Exclusion range	Optional. <i>Range Exclusion</i> on page 256
Fontset specification	Required. <i>Fontset specification</i> on page 257

Logical font mapping

The first section you must edit is the logical font mapping section. This section maps a logical name to its physical counterpart(s). When Select Access wants to invoke a font by using a logical name such as *Serif* or *Monospace*, the JRE looks up at the mapping information and loads that physical font into Select Access components.



You cannot create a new logical name. Only use the five names defined and the corresponding style values defined in *Logical fonts* on page 245.

The logical font mapping section uses the following syntax. Table 34 defines the parameters it uses.

```
<logicalname>.<style>.<ordernumber>=<xldfstring>
<conversioninfo>
```

Parameter	Description
<code><logicalname></code>	One of the five logical font types supported in the Java Runtime Environment. See <i>Logical fonts</i> on page 245 for details.

Parameter	Description
<code><style></code>	<p>A named set of formatting parameters that defines the weight of a font. See <i>Logical fonts</i> on page 245 for details.</p> <p>Note: If you omit the style value, Java assumes the plain style by default.</p>
<code><ordernumber></code>	<p>A numerical or position value used to determine the search order when the JRE reads the file. For example, the JRE reads <code>plain.0</code> before <code>plain.1</code>.</p> <p>All the numbers for one logical font must be in sequence. That is, if you insert a font, you must increase the rest of the order numbers by 1. Also, because they system uses this index to identify the logical font in other sections of the file, apply any changes made to a single entry universally.</p>
<code><xldfstring></code>	<p>The string copied from the font installed in your font path directory. For example, a Japanese font looks like this:</p> <pre>ricoh-hg mincho 1-medium-r-normal-0-0-0-0-m-0-jisx0208.1983-0</pre> <p>When copying this string, replace:</p> <ul style="list-style-type: none"> • The second 0 with %d. Select Access substitutes the %d with a specific point size when it uses the font. • All remaining 0 values with * <p>For example, a string Select Access copies from the serif font looks like this before Select Access uses it:</p> <pre>serif.1=-ricoh-hg mincho 1-medium-r-normal--*-%d--*-m-*-jisx0208.1983-0.</pre>

Parameter	Description
<code><conversioninfo></code>	A way of defining a different coding index for fonts on Solaris that it needs to convert to Unicode. This definition requires that you use the <code>NEED_CONVERTED</code> parameter. When you specify this parameter, you also need to create a character set converter and specify it in the character conversion section of this file. For details, see <i>Character conversion</i> below.

Character conversion

All fonts on Solaris that it needs to convert to Unicode. The syntax for this section is:

```
fontcharset.<logical name>.<order>=<converter>
```

where `<logical name>.<order>` must match the corresponding entries from the logical font mapping section of the file, and `<converter>` is the name of the java class that converts the file. For example:

```
fontcharset.dialog.1=sun.awt.windows.CharToByteWingDings
```

Select Access ships sample converters. By default Select Access installs these converters to the following directory:

```
<install root>\jre\lib
```

If these converters are not sufficient, do one of the following:

- Contact either Sun or a third-party vendor and see what converters they can provide.
- Create your own customized converter.



The JRE must see your converter. Therefore, the Select Access classpath must include the classpath to the converter. The simplest way to do this is to put this class under your `$JDK_HOME/classes/myown/package` directory.

Range Exclusion

Certain fonts contain characters that can overlap. In these cases, perhaps you have a preference for one character in a font over those in others. If this is the case, you have the option of deciding not to display character ranges in those fonts.

To determine where overlap occurs, enter the following command:

```
xfd -fn "<xlfd string>"
```

where *<xlfd string>* is the string of the physical font name.

If certain ranges or individual characters are redundant, define exclusion information on your physical font. The syntax for excluding these characters is:

```
exclusion.<logical name>.<order>=<Unicode_startrange>-  
<Unicode_startrange>
```

For example:

```
exclusion.dialoginput.3=0100-12cd
```

Fontset specification

In Solaris, you must specify a fontset for the locale, because Solaris manages the fontset at application runtime. This prevents Select Access from knowing that it is using multiple fonts. A fontset is a collection of fonts that can render all codesets represented in a locale's encoding, because a single font cannot render multicode set strings.

Fontsets delineate:

- The number of fonts
- The character-set registry of the fonts (these vary among different locales)
- Information on the locale

You specify a fontset for the locale, by adding the logical font definition to each locale-specific fontset. For example, the `en_US.UTF-8` locale supports the following set of font character sets as the FontSet:

- ISO 8859-1 (Latin-1)
- ISO 8859-2 (Latin-2)
- ISO 8859-4 (Latin-4)
- ISO 8859-5 (Latin/Cyrillic)
- ISO 8859-7 (Latin/Greek)
- ISO 8859-9 (Latin-5)
- ISO 8859-15 (Latin-9)
- BIG5 (Traditional Chinese)
- GB 2312-1980 (Simplified Chinese)
- JIS X0201-1976, JIS X0208-1983 (Japanese)
- KS C 5601-1992 Annex 3 (Korean)
- ISO 8859-6 based one (Arabic)
- ISO 8859-8 (Hebrew)
- TIS 620-2533 based one (Thai)

Querying multilingual URLs

To be able to query multilingual URLs between Web browsers and Select Access components, the Web browser and Web server must support UTF-8 characters.

Configuring Microsoft Internet Explorer v4 and v5 to send URLs in UTF-8 format to IIS Web servers:

1. Click **Tools>Internet Options**. The **Internet Options** dialog appears.
2. Click the **Advanced** tab and click the **Always send URLs as UTF-8** option. This enables multilingual URLs and allows Policy Validator to match the URL name with a resource name stored in LDAP that is already in UTF-8 format.
3. Click **OK**.

Appendix B

Character set listing

Select Access supports the character sets listed in Table 35. You can define a specific character set 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 user character set is iso8859-1.

Table 35: 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

Table 35: Supported character sets (Continued)

cp1004	cp1008	cp1025	CP1026	cp1027
cp1046	cp1089	cp1112	cp1114	cp1122
cp1123	cp1125	cp1130	cp1131	cp1200
cp1208	cp1250	cp1251	cp1252	cp1253
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
csAdobeStandardEncoding	csASCII	csBig5	csEUCKR	cseucpkdfmtjapanese
csGB2312	csHPRoman8	csIBM037	csIBM1026	csIBM273
csIBM277	csIBM278	csIBM280	csIBM284	csIBM285
csIBM290	csIBM297	csIBM420	csIBM424	csIBM500

Table 35: Supported character sets (Continued)

csIBM855	csIBM857	csIBM860	csIBM861	csIBM863
csIBM864	csIBM865	csIBM866	csIBM868	csIBM869
csIBM870	csIBM871	csIBM918	csISO2022CN	csISO2022JP
csISO2022JP2	csISO2022KR	csISO58GB231280	csisolatin0	csisolatin1
csisolatin2	csisolatin3	csisolatin4	csisolatin5	csisolatin9
csisolatinarabic	csisolatincyrllic	csisolatingreek	csisolatinhebrew	csJISEncoding
cskoi8r	csKSC56011987	csMacintosh	csPC850Multilingual	csPC851
cspc862latinhebrew	csPC8CodePage437	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-roecee	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_VPUA	ibm-1098_X100-2000

Table 35: Supported character sets (Continued)

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
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

Table 35: Supported character sets (Continued)

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
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

Table 35: Supported character sets (Continued)

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
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

Table 35: Supported character sets (Continued)

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_BigEndi an	UTF16_LittleEn dian	UTF16_Opposite Endian
UTF16_Platform Endian	UTF-16BE	UTF-16LE	UTF-32	UTF32_BigEndi an
UTF32_LittleEn dian	UTF32_Opposite Endian	UTF32_Platform Endian	UTF-32BE	UTF-32LE
UTF-7	UTF-8	windows-1250	windows-1251	windows-1252
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

This appendix provides solutions to possible problems you may be experiencing.

Policy Builder errors

HP has documented the following error:

- *Network Discovery not detecting redirects* on page 267

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 Validator errors

HP has documented the following errors:

- *Policy Validator generates error when installing* on page 267
- *Policy Validator failing at startup* on page 268
- *iPlanet 4.0 and Sun ONE 6.0: cookies not refreshed on IE* on page 269
- *Policy Validator looping* on page 269
- *Policy Validator short circuits* on page 269

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 pop 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:


```
<install_path>\bin
```
- f. Run the following command to install the Policy Validator as a service:


```
validator -I
```
- g. 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 users 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 6.0 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 users.

A Certificate chain verification is a very expensive operation that 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 270
- *Restricted IBM HTTP server resources* on page 270
- *Virtual Web server support problems with IIS* on page 271
- *Caching problems with IIS* on page 271
- *Integrated Windows authentication issues on IIS* on page 272

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 Users and an allow policy to Known Users. However, when a user enters their credentials with the Password server I configured, they are denied access. The Policy Validator then prompts the 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, users 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, users 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 6.0 Installation Guide*. For details on the Component Configuration tool, see Chapter 5, *Modifying components' central configuration parameters* in the *HP OpenView Select Access 6.0 Policy Builder Guide*.

Integrated Windows authentication issues on IIS

- Q I am having problems with my Integrated Windows authentication server 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:
- Open an MS-DOS command prompt session.
 - Navigate to the `Inetpub\AdminScripts` folder.
 - At the command prompt, run the following utility with the following command:
 - `adsutil get w3svc/NTAuthenticationProviders`
 - This command tests your Integrated Windows authentication system. If your deployment is problematic, you receive an error message.
 - If you receive an error message, enter the following command from the same location:
 - `cscript adsutil.vbs get w3svc/NTAuthenticationProviders`
 - 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 272*
- *Denied access on default page on page 273*
- *Browser gets deny yet Policy Validator gives allow on page 273*

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 users 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 gives 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 permissions. 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:

- *iPlanet and iPlanet Unicode problems on page 273*
- *Critical Path and Siemens over SSL problems on page 273*
- *Browsing for OCSP certificates on Critical Path on page 274*

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 and 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 274
- *Generic problems* on page 274
- *Microsoft certificates and failed signing* on page 275
- *Problems specific to IIS* on page 276
- *Problems specific to Apache* on page 276

Browsing for OCSP certificates on Critical Path

Q Why does the Policy Validator have problems locating the OCSP certificate authentication server'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 a user:

- a. The Subject DN of the certificate must meet one of the following conditions:
 - Exactly match the DN of the user's directory entry.

- Contain a `uid` attribute that exactly matches the `uid` attribute in the user's directory entry.
- Contain a `cn` attribute that exactly matches the `cn` attribute in the user's directory entry.
- b. The user's directory 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 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 277*

SSO failing on Internet Explorer

Q Why does Single sign-on (SSO) fail on IE sometimes?

A SSO always fails on IE when users 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 277*

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 role attribute values on page 277*

Empty role attribute values

Q I have set up personalization so that it returns role and group information and some attributes in the roles. Why do I get

“attribute=”, with nothing appearing after the equals symbol for those attributes?

- A** The attribute is not an attribute of the role or group. As a result, the value appears empty. For details on which attributes you can use, see *About directory attributes* on page 276 of the *HP OpenView Select Access 6.0 Policy Builder Guide*.

Glossary

A

Access control

The restriction of access to resources to prevent unauthorized use or use in an unauthorized manner.

Access policy

An access policy consists of authentication methods used to identify users and authorization rules that determine the user's level of access for the requested resource.

Administration server

This server administers Select Access' configuration information, as well as its certificate and policy data and then writes it to the Policy Store.

Administrator

See Security Administrator.

Alias

A pointer (or shortcut) to the actual user entry. An alias to the user entry is also shown under any groups or roles to which the user belongs.

Allow policy

A policy that allows a user access to a resource.

API (Application Program Interface)

The interface through which application programs communicate with the operating system and other services.

Application server

A server program in a computer that is usually part of a three-tier configuration: a client, an application server, and a database.

ASCII

ASCII is the most common format for text files in computers and on the Internet. In an ASCII file, each alphabetic, numeric, or special character is represented with a 7-bit binary number. 128 possible characters are defined.

ASN.1 (Abstract Syntax Notation)

An internationally accepted method for formatting information in machine-independent form.

Attributes

The required and optional characteristics used to describe an LDAP directory entry. An attribute has a type and a value in the format type=value, for example, uid=ksmith.

Audit policy

A policy that defines which events are logged for a given Select Access component.

Audit trail

A time-based log that shows which users have accessed a network resource and what operations have been performed using those resources. Audit trails monitor stability, ensure data integrity, and maintain corporate security.

Authentication

The act of proving an individual's identity and guaranteeing that a message really has come from the person who claims to have sent it. In many cases, authentication takes place via a username and password.

Authenticator

Select Access has five types of authenticators: password, certificate, registration, challenge/response (SecurID and RADIUS), and SAML. Each authenticator contains information about a particular authentication server. To determine whether it should return true or false when evaluating a query, the Policy Validator gives the query to each of its authenticators in turn.

Authorization

The process of giving users access rights to network resources based on their identity.

B**BER (Basic Encoding Rules)**

The set of rules for encoding ASN.1 defined data to produce self-identifying and self-delimiting transfer syntax for data structures described in ASN.1 notations. BER is used in a wide range of applications, such as Simple Network Management Protocol (SNMP) and LDAP.

Block cipher

A symmetric algorithm that encrypts a message by breaking it down into blocks and encrypting each block.

Branches (true/false)

The connections between the decision points of a rule created in the Rule Builder.

C

CA (Certification Authority)

A CA is a third party that registers users and certifies their identities by signing their public-key certificate.

Caching

Retaining a previously retrieved copy of something to enable quicker access. For Web servers, this is either performed at the browser client or at the proxy. The Policy Validator stores the information it has obtained from the directory server in a cache. The Policy Validator will not be aware of any changes until the cache is cleared, at which point it looks up information in the directory server.

CAO (Certification Authority Operator)

The interface through which the elements of a public-key infrastructure (PKI) are defined and configured. The CAO processes CA-signed certificates for these elements, defines registration policies, and administers certificates.

Certificate

A block of data containing your public key and basic identification details, signed with the CA's private key to verify that it is authentic.

Certificate template

A certificate template creates a profile for certificates based on their intended use. A certificate template is defined as part of the registration policy (RP).

Challenge/response server

One of four types of authentication servers the Select Access Policy Builder supports. For example, SecurID requires users to enter a passcode to authenticate themselves, whereas RADIUS requires users to enter a secret.

Ciphertext

A term used to describe text or data that has been encrypted. The encrypted data is undecipherable until it is converted into plaintext using a key.

Cleartext

See *Plaintext*.

COM (Component Object Module)

An object-oriented programming model for binary code developed by Microsoft. COM objects can be accessed by any COM-compliant application.

Component pool profile

Includes the configuration parameters shared by Enforcer plugins or Policy Validator pools.

Conditional policy

A policy that allows a user to access a particular resource if he meets certain criteria, which are defined in rules.

Confidentiality

Evidence that the contents of the message have not been disclosed to third parties.

Cookie

A text string used to identify users and possibly prepare personalized Web pages for them. Cookies are saved by browsers and are often used to authenticate users to a Web server without requiring further user interaction.

CRL (Certificate Revocation List)

A list of the serial numbers of all certificates that are no longer valid and should not be trusted.

D**Data signing**

A valid CA certificate attests to an entry's validity. The security benefits of policy data signing are data integrity and data authenticity. You need to configure Policy Validator to handle data signing, but you monitor signing status in Policy Builder.

Decider

A Policy Validator decider plug-in makes the decision at the various rule decision points. Policy Validator deciders are used to make decisions based on information contained in queries and an LDAP database.

Decision end point

The nodes available in the Rule Builder toolbar (Allow, Deny, logout user) that are placed at the end points of a decision tree.

Decision point

A point in a rule where an access decision is made. Decision points appear as icons in the Rule Builder and correspond to deciders in the Policy Validator.

Decryption

The process of transforming ciphertext back into plaintext so that it can be understood. It is the reverse of encryption.

Delegated mode

A scaled-back version of the Policy Builder that limits functions to the application of access policy to restricted sets of user and resource combinations. The appearance of delegated administration mode is the same as that of full administration mode, although functions and features that are not available to a delegated administrator are grayed out.

Delegated administration matrix

A grid from which delegated administrators can delegate administration privileges to users. Display the Delegated Administration view to access the Delegated administration matrix.

Delegation

The act of assigning management responsibility to selected security administrators who use the Delegated Administration Matrix to manage users and create authorization rules.

Denial-of-service

An attack that prevents a server from servicing its clients/customers.

Deny policy

A policy that denies a user access to a resource.

DES (Data Encryption Standard)

A symmetric algorithm that encrypts blocks of binary data using a 56-bit key.

Diffie-Hellman

Originally invented in 1974, Diffie and Hellman reinvented this key-agreement algorithm in 1976. It is used to create a shared secret random number that can then be used as a symmetric algorithm's session key.

Digest

The result of passing a file through a one-way hash algorithm, a digest is a representation of text in the form a single string of digits. It is nearly impossible to derive the original text from the string. Encrypting a message digest with a private key creates a digital signature.

Digital signature

A block of data created by hashing a file and encrypting the resulting digest using the sender's private key. Digital signatures ensure the integrity and origin of the data.

Directory entry

An entry in the directory server similar to a database record that contains information for a specific item, such as a folder, user, group, or role.

Directory server

A directory server is typically used to store information, such as a company directory, in a central repository and to provide quick and easy access to this information. LDAP is a standard protocol for accessing directory servers.

Directory tree

A hierarchical directory structure used by the directory server for locating resources.

DMZ (Demilitarized zone)

In computer networks, a DMZ is a computer host or small network inserted as a “neutral zone” between a company’s private network and the external public network. It prevents outside users from gaining direct access to a server with sensitive information.

DN (Distinguished name)

A sequence of attributes that uniquely identifies an entity and traces its path up the directory tree. The DN provides the necessary information about the owner of a certificate. The certificate contains both the DN of the owner and the DN of the issuer of the certificate.

DOM (Document Object Model)

The outline for how objects in a Web page, such as text, images, and links, appear. DOM supports both HTML pages and XML documents.

Domain name

Part of the Internet Protocol (IP) address used to identify the organization or local network to which a local host is connected. For example, the host name `www.mycompany.com` contains the domain name `mycompany.com`.

E**EJB (Enterprise Java Beans)**

A Java framework developed by Sun Microsystems that uses program components to build an application based on the client/server model.

Encryption

The conversion of data into an indecipherable form, known as ciphertext, to protect it from unauthorized viewing or use, especially during transmission or when it is stored. Encryption is typically based on a key, required in order to decrypt the information.

Enforcer API

A set of routines and protocols that pass queries from a resource server to the Policy Validator.

Enforcer plugin

An Enforcer plugin is installed in each server that manages access to network resources. The Enforcer plugin intercepts user requests, then sends queries to the Policy Validator to enforce access control.

Entropy

This is a routine that measures system activity, file system information, and the latency when the system switches from one process to another, creating a pool of information that would be very difficult for any attacker to reproduce exactly.

Entry

See Directory Entry.

Envelope

An enveloped message is one that has been encrypted with a session key, which is then encrypted in turn using the recipient's public key.

Event log

An event log is a track record of activities that range in level of severity. It comprises an audit trail and an audit policy.

Extranet

An intranet that authorized outsiders can access with a valid username or password, or by some other means of authentication. Depending on a user's identity, an extranet provides various levels of accessibility to different external users.

Failover

A backup mode for when a component is unavailable. In Select Access, you can enable failover for instances when a particular directory server is not available to process a request. You can set up your Policy Validator and your Enforcer plugins to use failover by configuring them to do so using the Setup Tool.

False branch

Created using the Rule Builder. The false branch defines the outcome if the decision point is evaluated as false, meaning that the user does not meet the decision criteria. False branches can lead to another decision point containing criteria, an allow decision point, or a deny decision point.

Folder

The Policy Builder interface displays two types of folders. One type is a means of organizing users, groups, and roles on the Users Tree. Another type of folder is a means of organizing services on the Resources Tree.

Full mode

The default version of the Policy Builder that includes all policy creation features. Running the Policy Builder in this mode allows the administrator unrestricted access to add, modify, or delete users, resources, rules, user access policies, or user delegation privileges from the Policy Matrix.

G**Gateway**

A combination of hardware and software that links two different types of networks and acts as an entrance point from one network to another.

Group

A named collection of users and possibly other groups. A user can be directly made 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 rule, unless you override it.

H**Hash**

A hash value is a number generated from a string of text, which is then used to compare versions of a calculated piece of data. If the hash results match, you can draw the assurance that the data has not been tampered with.

Hash algorithm

An algorithm used to create a digest of the data.

HMAC algorithm

Message authentication using hash functions. This key-hashed method uses a shared secret key and hash function to hash data and appends the hash to the data.

Host name

A fully qualified domain name that identifies one specific host computer within the Internet. For example, `www.hp.com` is the host name of Hewlett-Packard's Web server.

HTTP header

HyperText Transfer Protocol (HTTP) is the protocol for exchanging information between Web servers and browsers that consists of two types of HTTP header variables: request header variables and reply header variables.

HTTPS (Secure Hypertext Transfer Protocol)

A variation of the HTTP protocol that provides SSL security for online transactions using the World Wide Web.

I

IETF (Internet Engineering Task Force)

A large international community of network designers, operators, vendors, and researchers who are concerned with the evolution of Internet architecture and its smooth operation.

IIS (Internet Information Server)

Microsoft IIS is an extensible Internet server that runs on Windows NT Server 4.0 and Windows 2000.

Inheritance

Occurs when the authorization policies of a defined group or folder are applied to each constituent (users or resources) within that group.

Integrated Windows Authentication

An authentication server that uses NTLM or Kerberos authentication methods. This authentication method is also known as Windows NT challenge/response authentication.

Integrity

Proof that the message contents have not been altered, deliberately or accidentally, during transmission.

Internetworking

The process of connecting individual local area networks (LANs) to create wide area networks (WANs), and connecting WANs to form even larger WANs.

Intranet

A private network within an enterprise consisting of LANs or WANs. An intranet allows employees to access company information and computing resources.

IP (Internet Protocol)

The method by which data is sent from one computer to another on the Internet. See also *TCP/IP*.

IP address

A 32-bit numeric address written as four clusters of numbers separated by periods, such as 216.27.61.137. These number clusters are used to identify a device, such as a computer or printer, on a TCP/IP network. A single digit cluster cannot exceed 255.

I

IPSec

IPSec is a simple version of the emerging Internet IP security protocol. It includes the Encapsulated Security Payload (ESP) protocol for encryption and the Authentication Header (AH) protocol for authenticating TCP/IP packets. IPSec is typically used for creating VPNs across untrusted Internet links and is appropriate for data that has a short lifetime.

J

JAAS (Java Authentication and Authorization Service)

JAAS is a Java package that supports authentication and access control protocols. JAAS implements a Java version of the Pluggable Authentication Module (PAM) framework.

J2EE (Java 2 Platform, Enterprise Edition)

The J2EE adds Enterprise Java Beans, servlets, and related technologies to the standard Java libraries to create a platform for developing multi-tier enterprise applications.

JDBC (Java Database Connectivity)

JDBC is an application program interface (API) specification for connecting programs written in Java to the data in common databases.

K

Key

See PKI.

Kerberos

An authentication method that uses an electronic ticket that gives authenticated users access to restricted services. This option is available to Windows 2000 Domain Controllers only.

L

LAN (local area network)

A geographically limited data communications network, allowing easy interconnection of terminals, microprocessors, and computers in adjacent buildings.

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 user can access any resource without knowing where or how it is physically connected.

LDAP query

A request about users and resources made to an LDAP server.

Load balancing

Distributing the amount of work a computer has to do evenly across a network so that no single device is overwhelmed by requests.

Login

The act of identifying a user before allowing access to resources on a system. Typically, a login process requires a username and a password.

M

MAC (Media Access Control) address

A hardware address that uniquely identifies each node of a network.

MAC (Message Authentication Code) algorithm

A MAC is a mechanism that provides an integrity check, or authentication, of messages. It is based on a shared secret key.

Manifest

A list of all entries in the Policy Store that have been signed. Because the Policy Builder checks the manifest when determining whether or not a violation has taken place, the manifest is used to essentially protect the data in your Policy Store.

MD5 (Message Digest algorithm 5)

MD5 can be used for digital signature applications where a large message has to be compressed in a secure manner prior to be signed with the private key. MD5 takes a message of arbitrary length and produces a 128-bit message digest.

Message digest

See *Digest*.

N

Network discovery

The process through which services and resources are scanned or discovered on a network. A network resource plug-in is any tool that scans a network service and generates a list of resources available through the service. You can either use the HTTP or HTTPS Policy Builder plug-in, or you can use your own plug-in to discover different types of services.

Network resource

See *Resource*.

Network service

See Service.

Node

A network entity with a unique address that does some sort of processing. Every node has its own separate IP address.

Non-repudiation

Provides evidence of the message's origin so that the sender of the message cannot later deny having sent it. Also provides evidence that the message was received so the recipient cannot deny receiving it.

Nonce

An opaque piece of data. A nonce may simply be a large random number or it may contain encrypted or digitally signed data, such as an expiry date. Examples of a nonce are a timestamp, a counter on a Web page, or a marker to prevent unauthorized reproduction of a file. Cookies also function like nonces but are specific to Web servers.

NTLM

An authentication method that uses a domain authentication service on the domain controller to issue a token that gives authenticated users access to restricted services. This option is available to both Windows NT and Windows 2000 Domain Controllers.

O**OCSP (Online Certificate Status Protocol)**

A protocol that allows applications to verify whether a certificate is valid or has been revoked. OCSP can be either a replacement or a supplement to checking against a CRL. It attempts to overcome some of the distribution limitations of CRLs. OCSP specifies a request-response message syntax between a client application that requires certificate revocation status information and a server application that has knowledge of the revocation status. The OCSP server (or OCSP responder) can also provide additional status information beyond that available through a CRL.

OPSEC (Open Platform for Secure Enterprise Connectivity)

An initiative launched by Check Point Software Technologies to create a standardized environment of compliant security technologies.

Operational policy

Operational policies govern your entire PKI. They set up operational rules, explicitly defining required tasks and how each entity performs its functions on a daily basis. For example, the CA's operational policy defines how often the CA generates a CRL and whether it generates a new CRL each time a certificate is revoked. The RA's operational policy defines the time period

during which the RA processes certificate requests and how often it polls the database for new requests.

Override

Unique setting that takes precedence over shared component pool settings.

P

Padding algorithms

Used with encryption algorithms that process data in fixed amounts. If the actual input data does not fill an encryption block, it must be padded up to the correct length.

Passcode

A password generated by SecurID servers that authenticates users through an exchange using tokens that act as passcodes. These passcodes expire after a set amount of time (usually 60 seconds).

Passphrase/password

A series of characters that enables a user to access a file, computer, or device on a multi-user computer network. You can store passphrases in encrypted form using a one-way algorithm that prevents them from being decrypted.

Password policy

A set of rules that allow administrators to set robust password policies for the entire organization, as well as for individual users. Password policy can involve the age, size, uniqueness and expiry of passwords.

PEM (Privacy Enhanced Mail)

An Internet protocol that provides data confidentiality, data integrity, and data origin authentication for electronic mail.

PKCS (Public-Key Cryptography Standards)

This set of standards has been developed to aid compatibility between different cryptographic products.

PKI (Public-key infrastructure)

A PKI system provides a framework by which users and entities can communicate securely. Public-key cryptography uses a combination of public and private keys, digital signatures, digital certificates, and trusted third party Certification Authorities (CAs), to meet the major requirements of e-security. The X.509 standard defines a PKI as "The set of hardware, software, people and procedures needed to create, manage, store, distribute and revoke certificates based on public-key cryptography."

Plaintext

Data in its original unencrypted form.

Plugin

Plugin applications are programs that can easily be installed and used as part of your Web browser. Select Access supplies Enforcer plugins (Apache, Axis, Domino, IBM HTTPD, IIS, iPlanet, Oracle, TCP, and WSE), Policy Validator plugins, and authorization server plug-ins. Select Access supplies APIs so that clients can create their own plugins.

Policy

A set of defined practices or a formal statement of operational rules. See *Access policy*, *Registration policy* and *Operational policy*.

Policy Builder

A central administration tool to create authorization policies that authorize or deny users access to network resources.

Policy Matrix

A grid in the Policy Builder that displays users, resources, and the access policy assigned to each user-resource pair.

Policy query

A request for a resource made by an enforcer plug-in to the Policy Validator. The Policy Validator evaluates the user's authorization policy to determine whether the user is allowed access to the network resource. The access decision is sent to the enforcer plug-in.

Policy reply

A decision to a resource request made by the Policy Validator via an Enforcer plugin. Based on the user's authorization policy, the Policy Validator replies with an allow, deny or conditional decision.

Policy signing

See Data signing

Policy Store

A directory server that acts as a repository for policy data and configuration information.

Policy Validator

A component that evaluates enforcer plug-in queries to determine if a user is allowed or denied access.

Policy Validator plug-in

A plug-in component used in the Policy Validator to make an access decision.

Port

An endpoint to a logical connection on a TCP/IP network. A port is defined by its port number. For example, port 80 is generally reserved for HTTP traffic.

Portal server

A server that centralizes access to information and applications for employees and customers. It has a directory of links to Web pages, documents and reports.

Private key

A secret cryptographic key that enables you to decrypt files that have been encrypted using your public key.

Protocol

An established format for transmitting data between two devices in order to allow users to access a service. Examples of protocols are FTP, HTTP, DNS, and LDAP.

Proxy server

A server that interacts with another server on a client's behalf. Proxies are sometimes used to provide local caching to improve performance. Often, they are implemented in firewalls to give access control based on user authentication.

Public key

In public-key cryptography, this key is made public to all. It is primarily used for encryption but can also be used for verifying signatures. It can be published without revealing the owner's corresponding private key.

Public-key certificate

A packet of data consisting of your public key and your basic identification details, all signed with the CA's private key to verify that it is authentic.

Q**Query**

See Policy Query.

Query utility

The Query utility is a command line application that sends queries to a Policy Validator. This utility can be used to verify communication between Enforcer plugins and the Policy Validator.

R

RADIUS (Remote Authentication Dial-In User Service)

An Internet Engineering Task Force (IETF) protocol for protecting networks and resources against remote or dial-in access by unauthorized users. RADIUS consists of both server-side authentication algorithms and client-side access software.

RDN (Relative distinguished name)

A DN is made up of a sequence of one or more RDNs. Each RDN comprises an attribute identifier and its corresponding value, for example, c=US. Whereas a DN identifies entities in a directory tree, an RDN is the path from one node to a subordinate node. See also *DN (Distinguished name)*.

Referral

A response that redirects the Select Access component to the directory server that holds the data it requires.

Registration policy

A registration policy (RP) provides a set of rules and criteria for certificate requests that must be met before the CA can issue a certificate. An RP governs what data must be collected for the certificate applicant to register and determines the content of the certificate(s) generated.

Replication

The method of making copies of user or policy data (some or all) to enhance the fault tolerance of your directory system.

Report Viewer

The Report Viewer is a dialog box that displays your report content in several pertinent columns that can help the administrator understand why certain events are being logged and what users are triggering events.

Reporting

A Select Access function that extracts information from the Secure Audit server's audit trail regarding runtime transactions and events involving Select Access components that act as clients to the Secure Audit server. A report is issued to administrators regarding who has accessed or tried to access what resources, who has changed which policies at any given time, and the current state of policy.

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.

Resource Plugin

An application used to gather resource URLs and add them to the Resources Tree in the Policy Builder.

Resource Server

A server managing access to network resources (for example, a web server or FTP server).

Resources Tree

A hierarchical tree in the Policy Builder that contains folders, services, and resources.

Role

A role contains users whose membership is based on attributes configured in the user entry. As a result, a role is dynamic and users are added and removed automatically as their attributes change.

Root certificate

The self-signed public-key certificate at the top of the certification hierarchy.

Round robin

A way to manage server congestion by using different servers in turn. With Select Access, we install multiple Policy Validators for the purpose of load-balancing by distributing queries among a list of Policy Validators.

RSA

An asymmetric algorithm used primarily to create digital signatures, and more rarely for encryption. It is named after its creators: Rivest, Shamir, and Adleman. It provides security by factorization and discrete logarithm intractability.

Rule

A decision tree constructed in the Rule Builder that specifies whether a user is allowed access, denied access, or given conditional access to a resource.

Rule Builder

A component of Select Access that security administrators use to create the conditional rules that determine users' access rights.

S**SAML (Security Assertions Markup Language)**

In Select Access, SAML provides a vendor-independent way of doing cross-domain single sign-on and conveys user profile information between Web applications.

Schema

The structure of a database system, including the layout of fields in tables, and the relationships (if any) between different tables.

Secret

The encrypted password string generated by the RADIUS server. A matching Secret indicates that a user is authenticated. The maximum number of characters is limited to 1000.

Secure Audit Server

A server that centralizes logs across a distributed network. It uses SOAP, which allows the Secure Audit server to communicate with other Select Access components over the Internet regardless of what operating system the component is running on. The Secure Audit server is useful for monitoring stability, ensuring data integrity, and maintaining corporate security.

SecurID

A user authentication system developed by RSA Security Inc. that combines two factors: something the user possesses (token) and something the user knows (PIN). This combination is used to produce a passcode or temporary password.

Security administrator

The administrator(s) responsible for creating security policies, using the Policy Builder.

Seed

A bit sequence, which is typically random, used to generate a longer pseudo-random bit sequence.

Server plugin

See Enforcer Plugin.

Service

A service provides access to a resource via one or more protocols, for example, HTTP or FTP. Examples of services include file servers, databases, an NT domain, and a CA service. 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.

Servlet

A small program that runs on a server. For example, the Administration server runs a single servlet to run the Policy Builder.

Single sign-on

An authentication process that only prompts users for their username and password at the beginning of their session, but gives them access to multiple sites and applications without having to reauthenticate.

Smart card

A card with an embedded integrated circuit for storing information, typically used for authenticating a computer user or banking services, providing access control, storing value applications, and/or carrying private keys in a security system.

S/MIME (Secure Multipurpose Internet Mail Extension)

An addition to the MIME protocol that supports the exchange of encrypted email via the Internet.

SMTP (Simple Mail Transport Protocol)

A TCP/IP protocol that governs the transmission of email over computer networks.

SOAP (Simple Object Access Protocol)

A platform-independent communications protocol based on XML and HTTP. SOAP allows components to communicate over the Internet, irrespective of whether they are installed on Windows or Unix.

Socket

A software object that connects an application to a network protocol.

SSL (Secure Sockets Layer)

A protocol commonly used for securing the transmission of messages over the Internet, SSL is used by Web clients and servers to set up authenticated and encrypted sessions. SSL uses X.509 certificates. It has recently been succeeded by Transport Layer Security (TLS), which is based on SSL.

Stream cipher

A symmetric encryption algorithm that operates one bit at a time.

Subnet

A subnetwork that is an identifiably separate part of an organization's network. It shares the same network address as other parts of the network but has a unique subnet number.

T**TCP (Transmission Control Protocol)**

TCP is a communications protocol used with the Internet Protocol to send data, in the form of message units called packets, from one computer to another.

TCP/IP

TCP/IP is a two layered communications protocol made up of TCP and IP. It is built into many operating systems and is the basic communications language of the Internet. It is also used in

I

intranets and extranets, making it the de facto standard for transmitting data over networks. See also *IP (Internet Protocol)* and *TCP (Transmission Control Protocol)*.

Terminal point

The nodes available in the Rule Builder toolbar (Allow, Deny, Custom response, User logout, Redirect, Profile self-management) that are placed at the end points of a decision tree.

Threshold value

An amount that limits the number of entries to be displayed when performing a Find in Policy Builder.

Tree

See *Directory Tree, Resources Tree, Users Tree*.

Triple DES

Encrypts using the symmetric algorithm DES three times, normally with three different keys. This block cipher is equivalent to using Select Access's triple mode with the DES algorithm.

Tree

See *Directory tree*.

True branch

Defines the outcome if the decision point is evaluated to be true, meaning the query meets the decision end point criteria. True branches can lead to other decision points containing criteria, to an allow decision point, or to deny a decision end point.

U

UDP (User Datagram Protocol)

UDP is a communications method that uses the Internet Protocol to actually get a unit data (called a datagram) from one computer to another.

Unauthorized access

Occurs when an unknown user without the proper credentials accesses a protected resource.

Unauthorized tampering

Occurs when an attacker intercepts data communications and modifies their content.

Unknown user

A column in the Policy Matrix that contains rules to authenticate users who have not been or cannot be identified. It specifies what to do if a user's identity cannot be determined.

User

A directory server entry containing information about a single user. Users can be discrete entries or added to one or more groups. Also refers to any individual attempting to access a network resource.

User location

Contains your user information in one or more locations on one or more directory servers.

Users Tree

A hierarchical tree in the Users Tree that contains folders, groups, and users.

V

Validator

See *Policy Validator*.

Verification

The process of ensuring that the sender of an electronic document is who she claims to be.

VPN (Virtual private network)

A private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures.

W

WAN (wide area network)

A geographically dispersed telecommunications network.

X

X.500

An internationalized standard for developing electronic directories. Certificates and other information can be published to these directories using the X.500 standard.

X.509

The X.509 standard defines what information can be included in a certificate and describes the data format of the information.

XML (Extensible Markup Language)

XML is a markup language for documents that contain structured information, where structured information refers to both the content and some indication of the role that this

content performs. It was created so that richly structured documents could be served, received, and processed over the Internet.

Index

A

Addresses

- Administration server, 71
- IP, directory server, 65
- replicated directory server, 80

Administration server

- address, 71
- address definition, 70
- auditing settings, 80
- certificates, 71
- configuration, setup tasks, 61
- configuring, 59
- custom setup, 60
- data signing, 76
- multiple installations of, scenarios for, 84, 203
- platform availability, 12
- Policy store configuration, 65, 127, 180, 201
- Port definition, 70
- recovering, 84, 203
- setting up, 60, 64, 94, 124, 178
- setup tasks, 60, 123, 139
- typical setup, 60

Alerts

- configuring, 108

Alerts, emailing, 7

Apache

- Enforcer plugin, 13
- Enforcer plugin, operating systems, 11

Apache Enforcer plugin, 141

Apache Web Server

- configuring with enforcer, 170
- restarting, 171

Application servers, supported, 15

Attributes

- assertion lifetime, SAML, 184
- defining as part of profile, 6
- namespace, SAML, 187
- troubleshooting, 277

Audit

- common settings, 53
- entry, 81, 97, 131, 160
- overview, 93
- policy, creating, 111
- policy, specifying, 100
- settings setup screen, 96
- settings, Administration server, 80
- settings, Enforcer plugin, 130, 159

- stream, signing, 97
- trail, 81, 97, 131, 160
- trail, specifying, 100
- troubleshooting, 277

Audit policy

- configuring component streams, 111

Authentication, SAML server, 189

Authorization policies See Access policies

Axis Enforcer plugin, 141

Axis Host Application

- configuring with enforcer, 170
- restarting, 173

B

Backing up, data, Administration server, 84, 203

Browsers

- character sets, 259
- errors, 277
- multilingual URLs, 258

C

Cache

- cleanup percent, 135
- cleanup, command line options, 137
- fast cache response, 270
- refresh interval, Policy Validator, 134
- Web pages, 167

CD drive, mounting on HP-UX, 25

Certificates

- data signing setup screen, 76
- directory server, 71
- for directory servers, 75
- SSL, 75
- troubleshooting, 269, 274, 276
- uploading for delegated administration, 84
- verify intervals, 76, 79

CGI, troubleshooting, 277

Changes, tracking See Audit

Character Map, 253

Client, Secure Audit server setup, 80

Code

- examples, platform availability, 14

Components

- configuring log output streams, 111

Components, installing specific, 31, 40

- Configuring
 - alerts, 108
 - components when using, 54
 - Enforcer plugins, 139–??
 - in console mode, 49, 54
 - Policy Validator, 121, 138, 175
 - Secure Audit server, 91–120
 - SelectAccess, parameter types, 52
 - SelectAccess, selectaccess.conf, 52
 - SelectAccess, Setup Tool, 53
- Connection timeouts, Secure Audit server, 99
- Console mode
 - configuring SelectAccess in, 49, 54
 - installing SelectAccess in, 47
- Content folder, defining location of, 38, 47, 211, 219, 226, 234
- Control Panel, adding and removing components, 212, 226, 234
- Cookies
 - domain, 150
 - secure user credentials, 131
 - troubleshooting, 269, 277
 - Web session, 167
- Corporate boundaries, navigating See SSO
- CRLs, Administration server, 76
- Custom setup
 - administration server, 60
 - Enforcer plugins, 62, 125, 139, 143, 193
 - Policy Validator, 123
- D**
- Daemons
 - entropy gathering, 27
 - for mounting CD drive, 25
- Data
 - multiple user location, 24
 - policy location, 66
 - policy location setup screen, 67
 - rendering internationalized, 244
 - signing, 76
 - signing, setting up, 76
- Databases
 - creating tables, 105
 - JDBC, 101, 103
 - JDBC compliant, 7
 - reporting, 81
 - SSO, 6
 - using with Secure Audit server, 101
- Debugging, 112
 - command line options, 137
 - mode, Secure Audit server, 112
- Defaults, configuration parameters, 59
- Delegated Administration
 - benefits, 7
 - CA certificates for, 84
 - definition of, 7
- Digital signatures
 - signing audit stream, 97
 - troubleshooting, 275
- Digital signatures, used with the Secure Audit server
- Directory servers
 - certificates, 71
 - compliance of LDAP. See Directory servers
 - protecting data of, 76
 - replicated, setup screen, 79
 - setting up, 65
 - setting up Policy Store, 66
 - supported LDAP servers, 14
 - troubleshooting, 273
- Disk space
 - needed for SelectAccess, 11
- Domains
 - navigating across See SSO
 - setup of multiple, 151
 - single setup, 149
- Domino Enforcer plugin, 141
- E**
- Email. See Alerts
- Enforcer API library
 - operating systems available for, 11
 - platform availability, 14
- Enforcer plugins
 - balancing queries using round-robin, 163
 - configuring, 139–??
 - custom setup, 62, 125, 139, 143, 193
 - how to configure, 139, 198
 - platform availability, 12
 - Policy Validator, quit attempt to open connection, 165
 - See Apache Enforcer plugin, iPlanet Enforcer plugin, IIS Enforcer plugin, Sun ONE Enforcer plugin, TCP Enforcer plugin
 - troubleshooting, 271, 272, 277
 - typical setup, 62, 125, 139, 143, 193
- Entropy gathering daemon, 27
- Errors
 - browser, 277
 - configuring to a standard stream, 110
 - denied access, to service, 272
 - denied access, Web page, 273
 - logging, 113, 277

- Policy Builder, 267
- runtime, system log, 81
- Secure Audit server, 101
- XML, 277

Events, logs, 81, 97, 131, 160

F

Failover

- of the Administration server, 84, 203
- support, Enforcer plugins, 161

Fatal exceptions, 113

Files, ignored by Enforcer, 152, 155

Filtering, events, 110, 112

Firewalls, NAT mapping, 145, 163

Folders

- fonts, internationalization, 250
- installing SelectAccess, 31, 39
- Policy Store, 67
- SelectAccess defaults, 31, 34, 40, 213, 227

Font names, logical and physical, 245

Forms

- defining location of content folder, 38, 47, 211, 219, 226, 234
- login, 270

G

Guide, contents of, 1

H

Hardware requirements, 11

HP-UX, mounting CD drive, 25

HTTP

- basic authentication, 270
- GET request, 277
- headers, 277
- tags, troubleshooting, 267

HTTPS

- selecting as protocol, 195
- service, adding, 195

HTTPS, See SSL

I

IBM HTTPD Enforcer plugin, 141

Ignored filenames, 152, 155

IIS Enforcer plugin, 13, 141

- operating systems available for, 11

IIS Web Server

- configuring with enforcer, 168, 170

- restarting, 172

Installing

- in console mode, 47
- operating systems, 11
- Select Access, 29, 30, 38, 39, 206, 214, 221, 228
- Select Access Linux and Solaris components, 29, 38
- SelectAccess, 29, 36, 45, 208, 209, 222, 223
- steps of, 29
- system requirements, 11
- TCP Enforcer plugin, 174
- uninstalling components, 205, 234, 235, 237, 238, 239

Installing SelectAccess, 45, 209, 224

Integrated Windows authentication
troubleshooting, 272

Internationalization, 241

Internationalizing data, 244

Internet Information Service. See IIS

iPlanet

- Enforcer plugin, 13

ISAPI, 277

J

JDBC, 7, 101

- configuring database, 103
- databases, logsetup utility, 105
- databases, requirements for, 105
- reporting, 82
- using with SAS, 101

L

Level, logging hierarchy, 110, 112

License agreement, 30, 39, 206, 214, 220, 228

Linux Select Access components, installing, 29, 38

Lists

- available Policy Validators, 163
- character sets, 259
- Pass-through domains, 159
- protected Web sites, 151
- virtual Web sites, 158

Load balancing, 132

Locale

- identifying, 247
- SelectAccess, 57

Lockout, user, 6

Log files See Audit

Logical font names, 245

Looping queries, 269

M

Mapping fonts, 246

Memory

needed for SelectAccess, 11

Modes

console, installer, 47

console, setting up, 49, 54

Modifying components, 205, 220

N

NAT mapping, 145, 163

Network

discovery, 7

discovery, plugins used, 7

discovery, troubleshooting, 267

NT service, Secure Audit server, starting, 119

O

OCSP, 79

server URL, 76

timeout, 76

timeouts, 269

timeouts with, 165

troubleshooting, 269, 274

Operating systems

needed for SelectAccess, 11

supported, 11

Oracle Enforcer plugin, 141

P

Parameters

common parameters, 53

default group parameters, 53

ignored filenames, 152, 155

override parameters, 53

pass-through domains, 158

Partner, properties of server, 195

Passwords

history lists, 6

minimizing number of, 6

self-managing, 6

PDFs, troubleshooting, 271

Personalization

troubleshooting, 277

PFS mount, 25

Physical font names, 244

Platforms. See Operating systems

Policies, audit, 110

Policy Builder, 12

default port, 73, 74

errors, 267

operating systems available for, 11

password dictionary, 133

platform availability, 12

troubleshooting, 272

Policy data location. See Policy Store

Policy Matrix

adding services, 195

saml_in, 195

saml_out, 195

saml_responder, 195

Policy signing, 23

Policy Store

Policy Data Location setup screen, 66

setting up policy data location, 66

Policy Validator

cache refresh interval, 134

Configuration Editor, 11

configuring, 121, 138, 175

custom setup, 123

Enforcer plugin, 165

Enforcer plugin, quit attempt to open

connection, 165

logging, 112, 270

operating systems available for, 11

platform availability, 12

port, 130, 182

server pool, 162

starting, 136

starting manually, 136

startup script, running manually, 138

troubleshooting, 267, 268, 269, 270, 272, 274,

275, 277

typical setup, 123

uninstalling, 138, 175, 196

Portal servers, supported, 15

Port, Policy Validator, 130, 182

Port, Secure Audit server, 96

Processor

needed for SelectAccess, 11

Profiles

attributes in, 6

locking out user access, 6

re-activation, 6

self-managing, 6

Protocols

HTTPS, 195

Q

Queries

- looping, 269
- troubleshooting, 270
- user information, 195
- XML, maximum size, 135
- XML, Policy Validator, 121

Query program

- platform availability, 13

R

Recovering, the Administration server, 84, 203

Red Hat Linux. See Linux, 11

Regional settings, 247

Rendering internationalized data, 244

Repairing components, 205

Reports

- JDBC database, 103
- setup screen, 81

Requirements

- needed to run SelectAccess, 11

Resource bundle

- locating, 242
- translating, 241

Resources. See Resources Tree

Resources Tree. See Policy Matrix

Resources Tree, discovering network assets, See Network discovery

Resources, adding, 195

Roles

- troubleshooting, 277

Roles, attributes used for membership, 6

Round robin

- definition of, 161
- publishing keys, 132

S

SAML server

- authentication, 189
- available log channels for, 112
- definition, 177
- starting automatically, 195
- starting manually, 196
- startup script, running manually, 196
- uninstalling, 196

SAML, to partner URL, 195

saml_out, adding to Policy Matrix, 195

saml_responder, adding to Policy Matrix, 195

Schemas

- uploading, 66

Script

- saml_out. See saml_out

Secure Audit server

- configuring databases for, 101
- creating reports from See Reports
- debugging, 112
- digitally-signing output, 7
- outputting logs to, 7
- platform availability, 12
- port, 96
- setting up clients of, 80
- signing data digitally, 97
- SOAP, 96
- starting, 119
- startup script, running manually, 120
- timeouts for, 99

Select Access

- Administration server, 8
- auditing See Audit, 7
- Enforcer plugin See Enforcer plugin
- installing, 29, 30, 38, 39, 206, 214, 221, 228
- Linux, installing, 29, 38
- overview, 5
- Policy Builder See Policy Builder
- Policy Validator See Policy Validator
- SAML server See SAML server
- Secure Audit server, 9
- Solaris, installing, 29, 38

SelectAccess

- Administration Server, 12
- Enforcer plugins, 12
- installing, 26, 29, 36, 45, 208, 209, 222, 223, 224
- modifying installed components, 205, 220
- operating systems available for, 11
- platform availability, 11
- Policy Builder, 12
- query program, 13
- repairing installed components, 205
- Secure Audit Server, 12
- Setup Tool, 12
- startup script, running manually, 120, 138, 196
- system requirements, 11
- uninstalling installed components, 205, 234, 235, 237, 238, 239

selectaccess.conf, 38, 47, 211, 219, 226, 234

Self-servicing

- passwords, 6
- profiles, 6

Server pool, Policy Validators used by Enforcer plugin, 162

- Services
 - adding resources to, 195
 - adding to Resources Tree, 195
 - HTTPS, 195
 - servlet Enforcer plugin, 141
 - Servlet, saml_responder. See saml_responder
 - Settings, regional, 247
 - Setup Tool, 60, 94, 124, 142, 178, 199
 - platform availability, 12
 - Signatures, digital, troubleshooting, 275
 - Signing
 - stream, messages of, 111
 - Signing, of audit stream, 97
 - Single sign-on
 - See SSO
 - SOAP messages
 - encrypting, 154
 - signing, 152
 - SOAP protocol, 96
 - Software requirements, 11
 - Solaris, 11
 - localizing SelectAccess on, 57
 - Select Access components, installing, 29, 38
 - SQL, scripts for database tables, 105
 - SSL
 - certificates, 75
 - certificates needed, 71
 - directory server setup, 75
 - gathering random data, 27
 - port to disable, 65
 - regenerate, 70, 128, 148
 - troubleshooting, 270, 273
 - SSO
 - how used by Select Access, 5
 - SAML server, 32, 41
 - troubleshooting cookies, 269, 277
 - Startup script
 - Policy Validator, starting manually, 138
 - SAML server, starting manually, 196
 - Secure Audit server, starting manually, 120
 - Sun ONE
 - Enforcer plugin, 13
 - Enforcer plugin, operating systems available for, 11
 - Sun ONE (iPlanet) Enforcer plugin, 141
 - Sun ONE (iPlanet) Web Server
 - configuring with enforcer, 169
 - Sun ONE Web Server
 - restarting, 170
 - Synthetic users See Transient user entries, 112
 - System defaults, configuration parameters, 59
 - System requirements for SelectAccess installation, 11
- T**
- Tables, creating for SQL databases, 105
 - TCP Enforcer plugin, 141
 - installing, 174
 - operating systems available for, 11
 - Telnet, accessing resources, 270
 - Templates
 - HTML forms, 270
 - Timeouts
 - OCSP, 165, 269
 - Tracking changes, See Audit
 - Transient user entries, certificates, 112
 - Translating resource bundles, 241
 - Troubleshooting
 - attributes, 277
 - browser errors, 277
 - certificates, 269, 274, 276
 - CGI, 277
 - denied access, to service, 272
 - denied access, to Web page, 273
 - digital signatures, 275
 - directory servers, 273
 - Enforcer plugin, 271
 - forms, 270
 - HTTP basic authentication, 270
 - HTTP headers, 277
 - integrated Windows authentication, 272
 - ISAPI, 277
 - logging, 277
 - network discovery, 267
 - network services, 272
 - OCSP, 274
 - PDFs, 271
 - personalization, 277
 - Policy Builder, 267, 272
 - Policy Validator, 267, 268, 269, 270, 274, 275
 - referer headers, 277
 - roles, 277
 - SSL, 270, 273
 - SSO cookies, 269, 277
 - URLs, 267
 - virtual servers, 271
 - Web servers, 270
 - XML, 277
 - Typical setup, administration server, 60

U

Unicode, 253

Uninstalling

components, 205, 234, 235, 238, 239

Policy Validator, 138, 175, 196

Policy Validator manually, 137

SAML server, 196

Uninstalling components, 237

Unix

console mode, 49, 54

Unix, console mode, 47

Upgrading

issues, 20

removing files, 24

URLs

troubleshooting, 267

URL, for in-bound SAML server, 195

User credentials, troubleshooting, 270

Utility programs

query utility, 13

V

Virtual Web sites, 158

VNC, 29

W**Web sites**

denied access to, 273

troubleshooting, 270

virtual, 271

Windows, 11

WSE Enforcer plugin, 141

X**XML**

signing, troubleshooting, 275

troubleshooting, 277

X-Windows, 29

