

HP OpenView Select Access

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

Software Version: 6.2

Policy Builder User's Guide

Document Release Date: September 2006

Software Release Date: September 2006



Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notices

© Copyright 2001-2006 Hewlett-Packard Development Company, L.P.

Trademark Notices

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

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

For expanded copyright notices, see HP OpenView Select Access <install_path>/3rd_party_license directory.

Documentation Updates

This manual's title page contains the following identifying information:

- Software version number, which indicates the software version
- Document release date, which changes each time the document is updated
- Software release date, which indicates the release date of this version of the software

To check for recent updates, or to verify that you are using the most recent edition of a document, go to:

http://ovweb.external.hp.com/lpe/doc_serv/

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

You can visit the HP OpenView Support web site at:

www.hp.com/managementsoftware/support

HP OpenView online support provides an efficient way to access interactive technical support tools. As a valued support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract.

To find more information about access levels, go to:

www.hp.com/managementsoftware/access_level

To register for an HP Passport ID, go to:

www.managementsoftware.hp.com/passport-registration.html

Contents

1	Introducing the Policy Builder	15
	Audience	15
	The Select Access Documentation Set	15
	Chapter Summary	16
2	Getting Started With the Policy Builder	19
	Chapter Overview	19
	The Policy Builder: A Mode Overview	19
	Running the Policy Builder in a Specific Mode	20
	To run the Policy Builder for the first time	21
	To force Policy Builder to launch in a new IE Browser	24
	Using Policy Builder with Firefox 1.5	24
	To Use Policy Builder with Firefox 1.5	24
3	Building Your Identities and Resources Trees	25
	Chapter Overview	25
	Using the Policy Builder: An Introduction	25
	Before You Begin	27
	Setting Up Your Policy Matrix	27
	About the Identities Tree	28
	Web Services	30
	Building the Identities Tree	31
	Sample scenario: a large multinational	31
	To create a global identities location list	33
	To add or modify an identity location	33
	To set the identity location's general parameters	34
	To create a list of replicated servers	36
	To select the preferred identity attributes	37
	To specify how identities will be identified in the Policy Builder	38
	To select an identity location	39
	To import a CA certificate for a new identity location	39
	Manually Adding or Modifying an Identity Profile	40
	To create or modify an identity profile	40
	To refresh data	42
	Deleting an Identity	42
	To delete an identity	43
	About the Resources Tree	43
	Building the Resources Tree	44
	Updating the Resources Tree	45

Adding Network Resource Services to the Resources Tree	45
To create a new network service	45
Entering information for a non-server-specific resource service	47
Entering information for a server-specific network resource service	47
To add a server-specific resource service	48
To discover your network resource services	48
To modify a network resource server	51
To delete a network resource service	52
Adding Network Resources to the Resources Tree	52
Manually Adding a Network Resource to a Resource Server	52
To create a new network resource or edit an existing one	53
Automatically Generating a List with a Discovery Plugin	54
Plugin requirements	54
To create a global Resource Discovery plugins list	55
To configure a new or existing Resource Discovery plugin	56
Running a Network Resource Plugin	58
Before you run resource discovery	58
To run a discovery plugin for network resources	58
Importing a Resource List	61
Resource list requirements	61
To import resource URLs	61
Deleting a Resource	62
To delete a resource	62
Terminating a Network Discovery	63
4 Organizing Identities and Resources	65
Chapter Overview	65
Before You Begin	65
Understanding the Differences Between Organizational Units	66
What Are Groups?	66
What Are Dynamic Groups?	66
What Are Folders?	67
Identity scenario	67
Resource scenario	67
Working with Identities, Groups, Dynamic Groups, and Folders	68
Understanding How to Organize Entries	68
Creating and Modifying a Group	69
To create or modify a group	69
Assigning Group Membership	70
To change an identity's group membership	71
To change a group's members	71
Creating and Modifying a Dynamic Group	73
To create or modify a dynamic group	73
To view dynamic group membership	75
Creating and Modifying a Folder	75
To create or modify a folder to categorize your identities	76
To create or modify a folder to categorize your resources	77

Deleting a Group, Dynamic Group or Folder.	77
To delete a group, dynamic group, or folder	77
Expanding, Searching, and Hiding a Group, Dynamic Group, or Folder	77
Finding a Tree Entry	77
To perform a quick search	78
Expanding a Collapsed Entry	79
To perform a quick search by expanding a collapsed entry	79
To perform an advanced search	80
Understanding Post-Search Results	81
To determine which search results to display	82
To hide a tree entry	82
To unhide a tree entry	83
Setting Tree Threshold Values.	83
To set tree thresholds	83
5 Authentication Basics: Select Auth & Personalization	85
Chapter Overview	85
Authentication Criteria	85
Elements of Select Access Authentication	86
Using Select Auth to Authenticate Identities	87
When an Identity Cannot be Authenticated by Policy Validator	87
About the Select Auth Column.	87
Setting a Select Auth Policy	88
To set a Select Auth policy	88
To disable Select Auth	89
To enable Select Auth	89
To inherit Select Auth	90
To choose from a list of available authentication services.	90
To change Select Auth properties	91
Enabling Personalization.	92
How Personalization Works	92
How Select Access Processes Identity Data for Personalization	92
When to Enable Personalization	93
To enable personalization	93
To determine which directory-specific attributes to use for identities and groups	95
6 Setting Up Authentication Services.	97
Chapter Overview	97
Understanding the Mechanics of Authentication Services	97
Configuring Your Authentication Services	97
Validating Identities When Profiles Are Not on the Directory Server	99
Why Transient Identity Profiles Are Created	99
Where Transient Identities Are Stored	100
Setting Up Your List of Authentication Services	100
Supported Authentication Services Types	100
To configure authentication services	101
To define an authentication method for a new service	102

Integrated Windows Authentication Service	103
Sequence of integrated authentication.	104
To configure a new or existing Integrated Windows authentication service	104
NTLM Authentication Service	105
To configure a new or existing NTLM service	105
Registration Authentication Service	107
To configure a new or existing registration service	107
Trusted Servers Authentication Service	112
How does the Trusted Server Policy Validator plugin work?	112
To configure a new or existing trusted authentication service	113
RADIUS Authentication Service	114
To configure a new or existing RADIUS service	114
SecurID Authentication Service.	117
To configure a new or existing SecurID service	117
To configure advanced SecurID properties	119
Certificate Authentication Service.	120
To configure a new or existing certificate service	120
To configure advanced certificate properties	122
Password Authentication Service	124
To configure a new or existing password service	124
Kerberos Authentication Service	125
To configure a new or existing Kerberos service	126
Avoiding Incorrect Service Setup for Groups and Dynamic Groups	127
Symptoms of an Incorrect Setup	127
To correctly set up authentication in the Policy Builder	127
Setting Up Authentication Forms Used by Authentication Services	128
7 Controlling Network Access	129
Chapter Overview	129
Understanding Authorization	129
Using the Policy Matrix to Set Policy	130
Administering Access Policies For Known or Unknown Identities	130
To apply an access policy to a known or unknown identity.	131
About the Access Policy Icons.	132
About Access Policy Inheritance	133
Increasing Scalability	133
Inheriting Access Policies	133
To determine policy inheritance	136
Priority Given to Access Policies	136
Overriding an Inherited Access Policy.	137
When a Pairing Inherits Multiple Access Policies	137
Tips for Administering Access Policies	139
8 Managing Identity Profiles	141
Chapter Overview	141
Introducing Select Access Management Features	141
Managing Identities Profiles	142

To activate the identity's profile and specify password preferences	142
To disable an identity's profile	144
Managing End User Passwords	144
Setting Up and Maintaining Password Management.	145
Configuring Password Policies	145
To enable a company-wide password policy	146
To configure password strength.	147
To configure password expiry	149
To configure password failure	150
To set password policy forms.	151
To disable company-wide password policies.	152
Enabling Password Resets	152
To configure the password reset policy.	154
Understanding End Users' Answer Requirements	155
9 Creating Conditional Access Rules with the Rule Builder.	157
Chapter Overview	157
Introducing the Rule Builder	157
What Can Conditional Policy Rules Do?.	158
How Do Conditional Policy Rules Work?	158
What is a Decision Point?.	159
What is a Terminal Point?	160
Before You Begin	161
Creating a Rule	161
Working with Rules	162
To create a new policy rule	163
To copy an existing rule.	163
To modify a rule	163
To delete a rule.	164
To save a rule	164
To print a rule	164
Working with Decision Points	164
To create a decision point	164
To copy and paste decision points	165
To modify a decision point.	165
To delete a decision point	165
The Networks and Domains Decision Point	165
To configure a networks and domains decision point	166
The Time of Day Decision Point.	167
To configure a Time of Day decision point	168
The Encryption Level Decision Point.	169
To configure an Encryption Level decision point.	169
The Directory Attributes Decision Point	170
To configure a Directory Attributes decision point	171
The Authentication Properties Decision Point	173
To configure an Authentication Properties decision point	173
The Ports Properties Decision Point	174

To configure a Ports Properties decision point	175
The Query Attributes Decision Point	176
To configure a Query Attributes decision point	177
Available Query Attributes	179
The XPath Decision Point	180
To configure an XPath decision point	180
To write a valid XPath Expression	183
The Alert Notification Decision Point	183
To configure an Alert Notification decision point	184
The Insert Subrule Decision Point	184
To configure an Insert Subrule decision point	185
The Citrix Decision Point	186
To configure a Citrix decision point	186
The Workflow Decision Point	187
To configure a Workflow decision point	187
The Custom Response Terminal Point	189
To configure a Custom Response terminal point	189
The Logout Identity Terminal Point	190
The Redirect Terminal Point	191
To configure a Redirect terminal point	192
The Profile Self-Management Terminal Point	193
To configure a Profile Self-Management terminal point	193
The Allow and Deny Terminal Points	195

10 Controlling Administrative Access 197

Chapter Overview	197
Levels of Administrative Access	197
Root Administration Access	197
Delegated Administration Access	198
Web Administration Access	198
Self Administration Access	198
Enabling Administration Server Resources	199
To enable Select Auth on an Administration server resource	199
Using the Administration Matrix to Delegate Entitlements	202
About Administration Entitlements: Delegation and Workflow	203
How Administration Policies are Represented	203

11 Managing Delegation Policies 205

Chapter Overview	205
Enabling Delegation	205
How Views Are Customized	206
To enable delegation	206
About the Delegated Administration Enforcer plugin	206
Assigning Administration Entitlements	207
Administration Resources You Can Delegate	207
To set a specific delegation entitlement	209
About Delegation Entitlement Inheritance	213
Inheritance Restrictions on Groups and Dynamic Groups	213

Disinheritance Prevention	214
12 Using Administration Workflow	217
Chapter Overview	217
How Does Administration Workflow Work?	217
Setting Up Administration Workflow	218
Configuring Email Options	218
Setting Mail Server Properties	219
To configure mail server properties for administration workflow	219
Specifying Custom Workflow Alert Templates	220
To change which templates will be used for workflow alerts	220
Creating Workflow Rules	221
To create a new workflow rule	221
Setting Workflow Conditions	222
Applying a Workflow Condition	222
To apply workflow conditions	222
Applying Workflow to the Creation of New Identity Profiles	223
About Administration Workflow Inheritance	224
When a Pairing Inherits Multiple Workflow Conditions	224
Workflow Inheritance and Delegation	224
Using Inheritance to Set Workflow Conditions with Delegation Entitlements	224
Administering Change Requests	225
Managing Change Requests as a Submitter	226
To check the status of a pending change request	226
Managing Change Requests as an Approver	227
To view change requests awaiting your response	228
To check the approval status	229
13 Changing Audit Settings	231
Chapter Overview	231
Understanding Audits	231
Configuring Audit Settings from the Policy Builder	231
How You Can Configure Audit Settings	232
To change common and/or group default audit settings	232
Configuring an Audit Trail	233
To choose an audit trail	233
Configuring Select Audit	235
To configure Select Audit:	235
Configuring a Log File	235
To configure a log file	236
Configuring System Logging	237
To configure system logging	237
Configuring a Standard Error Stream	237
To log to standard error	237
Configuring an Audit Policy	237
To create an Audit Policy	238
Supported Audit Policy Combinations	240

14 Managing Your Policy Data	245
Chapter Overview	245
What is a Policy Store?	245
What Data Gets Recorded to the Policy Store	245
Updating Policy Data Cached by the Policy Validator	246
To update the Policy Validator cache	246
To enable warnings when policy data affects the Policy Validator	246
Updating Policy Data Displayed by the Policy Builder	246
To refresh policy data	247
Protecting Policy Data Recorded in Your Policy Store	247
Setting Up Data Signing	247
Understanding Signing States	248
Losing Your Key	248
Locating and Validating Entry Violations	248
To validate an entry violation	249
To disable warnings	250
15 Modifying Components' Central Configuration Parameters	251
Chapter Overview	251
What Parameters You Can Update	251
Configuring Central Parameters from the Policy Builder	251
Changing Configuration for a Group	252
To change the group defaults shared by multiple components	253
Changing Override Parameters	253
To create or change an override value for a single component	254
Modifying Group and Override Parameters for the Enforcer Plugin	255
What You Need to Do to Change Enforcer Plugin Settings	255
To configure central Enforcer plugin parameters	256
Modifying Group and Override Parameters for the Policy Validator	267
What You Need to Do to Change Policy Validator Settings	267
To configure central Policy Validator parameters	267
Refreshing Configuration Changes	271
Deleting a Component's Configuration	271
Displaying Warning Messages	271
To enable warning messages	271
A Invalid Characters	273
B Using Web Administration	275
Before You Begin	275
About Web Administration Security	275
Setting Up Access to the Web Administration Application	276
Getting Started with Web Administration	276
Running Web Administration	276
To run the Web Administration application	277
Locating Identities	278
To search for an identity	279

To browse for an identity.	279
To display all the visible identities.	279
Managing Identities, Groups, and Folder.	280
Managing Identities	280
To add, modify or rename a new identity profile	280
To assign the current identity to a group.	282
To delete an identity profile	282
Managing Groups	282
To add, modify, or rename a group	282
To add a new member to the current group.	283
To delete a group	284
Creating and Modifying a Folder.	284
To add, modify, or rename a folder	284
C Writing LDAP Expressions	287
When Search Expressions Are Used.	287
Understanding Comparison Operators.	287
Nesting Filters	288
D Uploading Custom Plugins.	289
What is a Custom Plugin?	289
Uploading Different Policy Plugin Types	289
To upload a custom Decision Point or Authentication plugin.	289
To upload a Subject Editor plugin	290
E Troubleshooting	291
Appendix Overview	291
Installer Errors	291
Out of Memory Error when Installing on HP-UX.	291
Policy Builder Errors	292
Policy Builder Does Not Initialize	292
Network Discovery Not Detecting Redirects.	292
Policy Builder and Critical Path Index Node Values	292
Running Policy Builder in Delegated Administration Mode	293
Running Two Sessions on the Same Machine.	293
X11 Display Error with Delegated Mode on Solaris	293
Policy Validator Errors	294
Policy Validator Registers with Wrong Address on Linux	294
Policy Validator Generates Error When Installing.	294
Policy Validator Failing at Startup	295
Policy Validator and Hostnames	295
iPlanet and Sun ONE 6.0: Cookies Not Refreshed on IE	295
Policy Validator Looping	296
Policy Validator Short Circuits.	296
Policy Validator Missing SSL session Information	296
Web server/Application Server Errors	297
HTTP Basic Authentication Problematic	297
Restricted IBM HTTP Server Resources.	297

Virtual Web Server Support Problems with IIS	298
Caching Problems with IIS	298
Integrated Windows authentication issues on IIS	298
Denied Access Errors	299
Denied Access to Service	299
Denied Access on Default Page	299
Browser Gets Deny yet Policy Validator Returns Allow	300
Directory Server Errors	300
Active Directory 2003 and Profile Password Setup Problems	300
iPlanet and iPlanet Unicode Problems	301
Critical Path Over SSL Problems	301
Certificate Errors	301
Browsing for OCSP certificates on Critical Path	301
Generic Problems	302
Microsoft Certificates and Failed Signing	302
Problems Specific to IIS	303
Problems Specific to Apache	303
Browser Errors	304
SSO Failing on Internet Explorer	304
Personalization Problems	304
Empty Dynamic Group Attribute Values	304
Password Management Problems	304
Glossary	305
Index	313

1 Introducing the Policy Builder

As the administrative hub of Select Access, the Policy Builder is a Java-based user interface that gives administrators (full or delegated) a policy-driven approach for administering identity entitlements and transaction security.

Via the Policy Matrix and its grid-based representation of identities and resources, the Policy Builder simplifies the complicated and often time-consuming process of creating and applying access policies. With simple visual icons and inheritance rules, the Policy Builder allows you to quickly understand policy logic and thereby reduce the number of errors typically incurred by other list-based access management systems. The result is a single administration point where authentication management information (who you are), and entitlement management data (what you are entitled to access) are easily controlled.

Audience

This guide is intended for individuals or teams responsible for creating enterprise-level network security with a specific mandate to manage how access to valuable corporate resources is controlled. This guide assumes a working knowledge of:

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

The Select Access Documentation Set

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

- *HP OpenView Select Access 6.2 Installation Guide*, © Copyright 2000-2006 Hewlett-Packard Development Company, L.P. (`installation_guide.pdf`)
- *HP OpenView Select Access 6.2 Policy Builder Guide*, Copyright 2000-2006 Hewlett-Packard Development Company, L.P. (`policy_builder_guide.pdf`)
- *HP OpenView Select Access 6.2 Network Integration Guide*, © Copyright 2002-2006 Hewlett-Packard Development Company, L.P. (`integration_guide.pdf`)
- *HP OpenView Select Access 6.2 Concepts Guide*, © Copyright 2005 - 2006 Hewlett-Packard Development Company, L.P. (`concepts_guide.pdf`)

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

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

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

- *HP OpenView Select Access 6.2 Developer's Tutorial Guide*, © Copyright 2004-2006 Hewlett-Packard Development Company, L.P. ([dev_tut_guide.pdf](#))
- *HP OpenView Select Access 6.2 Developer's Reference Guide*, © Copyright 2004-2006 Hewlett-Packard Development Company, L.P. ([dev_ref_guide.pdf](#))

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

Chapter Summary

This guide includes the chapters listed in [Table 1](#).



See the *HP OpenView Select Access 6.2 Release Notes* ([relnotes.pdf](#)) on the Select Access installation CDs for known installation issues at the time of this release.

Table 1 Chapter Summary

Chapter	Description
Chapter 2, Getting Started With the Policy Builder	This chapter introduces you to the Policy Builder. The Policy Builder is a digitally-signed Java applet that the Administration server always serves over SSL. The Policy Builder allows administrators to define the authentication methods and authorization policies with an easy-to-use administration grid.
Chapter 3, Building Your Identities and Resources Trees	This chapter describes the two axes of the Policy Builder: the Identities Tree and the Resources Tree. Together the Identities Tree and Resources Tree visually illustrate the connection between identities, resources, and the policies you administer.
Chapter 4, Organizing Identities and Resources	This chapter describes the ongoing maintenance of your identities and resources, which includes organizing them into logical and/or discrete units.
Chapter 5, Authentication Basics: Select Auth & Personalization	This chapter introduces you to the fundamentals of authentication and personalization. Authentication is the process by which an unknown user is identified as a known user. Once the identity is known to the Select Access system, content can be personalized for a given user.
Chapter 6, Setting Up Authentication Services	This chapter is the counterpart to Chapter 5, Authentication Basics: SelectAuth & Personalization. It continues the explanation of how Select Access authenticates identities using the supported authentication services.

Table 1 Chapter Summary (cont'd)

Chapter	Description
Chapter 7, Controlling Network Access	This chapter describes the concept of access management. How you control identity access to sensitive resources depends on how you apply a correct combination of allow/deny/conditional policies against specific identity/resource combinations.
Chapter 8, Managing Identity Profiles	Keeping identity data current is not necessarily the domain of identity administrators alone. Select Access allows end users to manage their own profile data via its profile self-management features.
Chapter 9, Creating Conditional Access Rules with the Rule Builder	A conditional access rule is a way of graphically describing the logic flow of evaluation criteria or behavior. This chapter describes how you can use the Rule Builder to create these conditional rules.
Chapter 10, Controlling Administrative Access	This chapter introduces the levels of administration access an identity can have. It is an overview topic to the more detailed subjects of Delegated Administration management and workflow management described in subsequent chapters of this guide.
Chapter 11, Managing Delegation Policies	This chapter advances the subject of administrative access first discussed in Chapter 10, Controlling Administrative Access. It gives you the implementation details you need to set specific entitlements for identities, thereby granting them administrative responsibilities.
Chapter 12, Using Administration Workflow	Administration workflow allows you to restrict user or policy changes from taking effect until they have been authorized by selected managers or administrators. This chapter describes how to use workflow to protect corporate data.
Chapter 13, Changing Audit Settings	This chapter introduces you to the term “audit.” It also describes how you use the Policy Builder to change those parameters initially configured when Select Access components were installed.
Chapter 14, Managing Your Policy Data	This chapter describes the policy data you create, how it is stored, and how you can better manage that data.
Chapter 15, Modifying Components' Central Configuration Parameters	You can modify the Policy Validators' and Enforcer plugins' configuration from the Policy Builder. This chapter describes how to manage and update the parameters that were originally set after they were installed with the Setup Tool.

Table 1 Chapter Summary (cont'd)

Chapter	Description
Appendix A, Invalid Characters	The characters listed in this appendix are characters that are invalid on specific directory servers.
Appendix B, Using Web Administration	The Web Administration application is a customizable, form-based application that allows you to access the Administration server through your corporate portal. Using Web Administration, administrators with the appropriate entitlement can remotely manage your Select Access identities.
Appendix C, Writing LDAP Expressions	LDAP requires you to make requests for information in the form of a stylized search expression that acts as an attribute filter.
Appendix D, Uploading Custom Plugins	Select Access includes several software modules that add specific features or services to an existing server. However, depending on your environment, you can upload your own plugins to customize Select Access' functionality. This appendix describes how to upload the GUI interfaces for the custom plugins you have created.
Appendix E, Troubleshooting	This appendix includes topics that troubleshoot a Select Access-protected system.

2 Getting Started With the Policy Builder

This chapter introduces you to the Policy Builder. The Policy Builder is a digitally-signed Java applet that the Administration server always serves over SSL. The Policy Builder allows administrators to define the authentication methods and authorization policies with an easy-to-use administration grid.

The grid is divided into two parts.

- The Resource Access branch allows authorized administrators to set authentication and authorization policies against specific identity (on the horizontal axis) and resource (on the vertical axis) combinations.
- The Administrative Access branch allows authorized administrators to set delegation policies against specific identity and administration function combinations. This allows you to set the level of administration privilege granularity, which can range from managing data (identity or resource) to setting policy.

Chapter Overview

The following topics describe how to run the Policy Builder according to the administrative entitlements assigned to you:

- [The Policy Builder: A Mode Overview](#) on page 19
- [Running the Policy Builder in a Specific Mode](#) on page 20
- [Using Policy Builder with Firefox 1.5](#) on page 24

The Policy Builder: A Mode Overview

You can access full or restricted Policy Builder features and administrative functionality depending on the mode you choose to run the Policy Builder in:

- **Root Administration:** Runs the default version of the Policy Builder, which includes all policy creation features. In this mode, the Policy Builder allows you unrestricted access to add, modify, or delete identities, resources, rules, access policies, or delegation entitlements from the Policy Matrix.
- **Delegated Administration:** Runs the Policy Builder with only the features and functions enabled for that administrator, according to the entitlements assigned to the administrator's profile. If a function has not been delegated, administration entitlements for that feature are not assigned; therefore the feature in question is dynamically disabled at run time.



If a delegated administrator tries to use a function that was not assigned to her, the Policy Builder notifies her that she is not authorized to use that function.

- **Web Administration:** Runs a pared-down, form-based version of Policy Builder functionality.

Running the Policy Builder in a Specific Mode

The Administration server identifies the mode you wish to run the Policy Builder in, depending on the port provided. Ports for different modes are defined when you configure the Administration server. As shown by [Figure 1](#), when the configuration of the Administration server is registered in the directory server, a message appears outlining the URL and port number combinations for each mode.



Figure 1 URL and Port Combinations Message Box

For details on setting up unique port values, see [Chapter 5, Configuring the Administration Server](#), in the *HP OpenView Select Access 6.2 Installation Guide*.

To run the Policy Builder for the first time

- 1 Initialize the mode of the Policy Builder you want to run. [Table 2](#) lists these options for you.

Table 2 Initializing the Policy Builder

Mode	Procedure
Root Administration	<ul style="list-style-type: none">• On Windows, click the Policy Builder shortcut located on your desktop or in your HP OpenView Select Access 6.2 program group.• On UNIX, type the URL and port configured for this mode in your browser's Address box. The default syntax is: <code>https://<admin_server_host>. <domain>:9986/admin</code>
Delegated Administration	<ul style="list-style-type: none">• Type the URL and port configured for this mode in your browser's Address box. The default syntax is: <code>https://<admin_server_host>. <domain>:9987/admin</code>
Web Administration	<ul style="list-style-type: none">• Type the URL and port configured for this mode in your browser's Address box. The default syntax is: <code>https://<admin_server_host>. <domain>:9991</code>

- HP recommends running the Policy Builder over Firefox 1.5 or later and Microsoft Internet Explorer 5.5 or later. You can run the Policy Builder over other browsers, but HP cannot attest to their stability or security.
- You can also substitute <admin_server_host>.<domain>> with your host's IP address.

If you configured the Administration server to allow Select Access to handle SSL certificates and connections, a security alert similar to the one shown below appears.

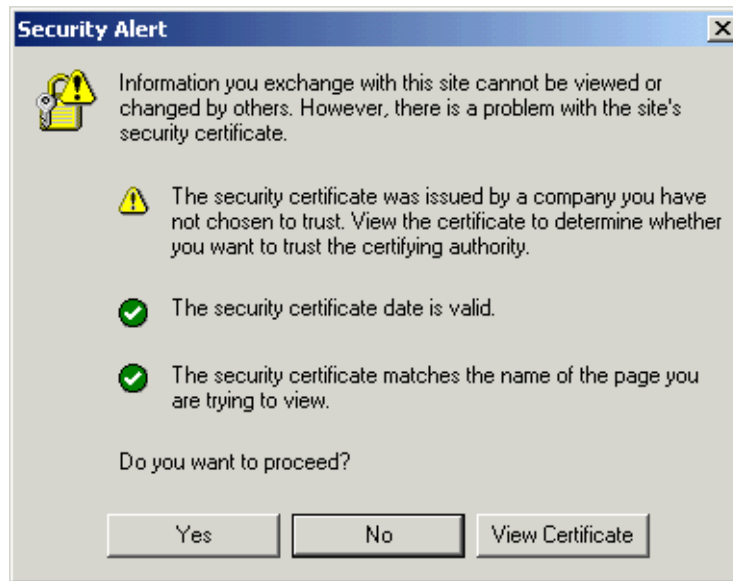


Figure 2 Example Certificate Security Alert

- 2 Click **View Certificate**. The **Certificate** dialog box appears.
- 3 Click the **Certification** tab.
- 4 Select the CA root and click **View Certificate**. A second **Certificate** dialog box appears.
- 5 On the **General** tab, click **Install Certificate**, and follow the Certificate Manager Import wizard's prompts to add this certificate to your Root Store.
- 6 The **Import Successful** message box appears. Click **OK** to close this message box.
- 7 Click **OK**.
- 8 Click **Yes** on the **Security Alert** message box. The Select Access Administration login page that is used to access the Policy Builder appears. If you are running the Policy Builder in delegated mode, you may be required to authenticate with additional methods (for example, certificate or token), depending on what authentication policy has been configured for you.



Select Access Administration

Please Login

Login Name

Password

First-time users:

You may need to [download the Java Plug-In](#) and read about the [Select Access code-signing certificate](#) before logging in.

Figure 3 Policy Builder Login Page: Root Administration Mode

- 9 Enter the login information required to access the Policy Builder in Root Administration mode (that is, the login information required to log into the Administration server), and click **Login now**.

The Administration server compares the credentials with the login information in its configuration file. It then generates a cookie for this administrator and starts the corresponding client's applet. This cookie is used to store session preferences. To restore Policy Builder to its system defaults, delete this cookie.

► If the Policy Builder starts before your directory server starts, it retries connecting to these components, which can take some time.

- 10 Because Select Access 6.2 upgrades the version of the Sun Microsystems Java Plugin, you are prompted to install a new plugin. Follow the installer prompts. If you are not automatically prompted, click the download link on the login page and download the corresponding installer first.
- 11 Once the plugin has been installed, a Java plugin security warning appears. For details on this warning message, click the corresponding Select Access code-signing link on the login page.

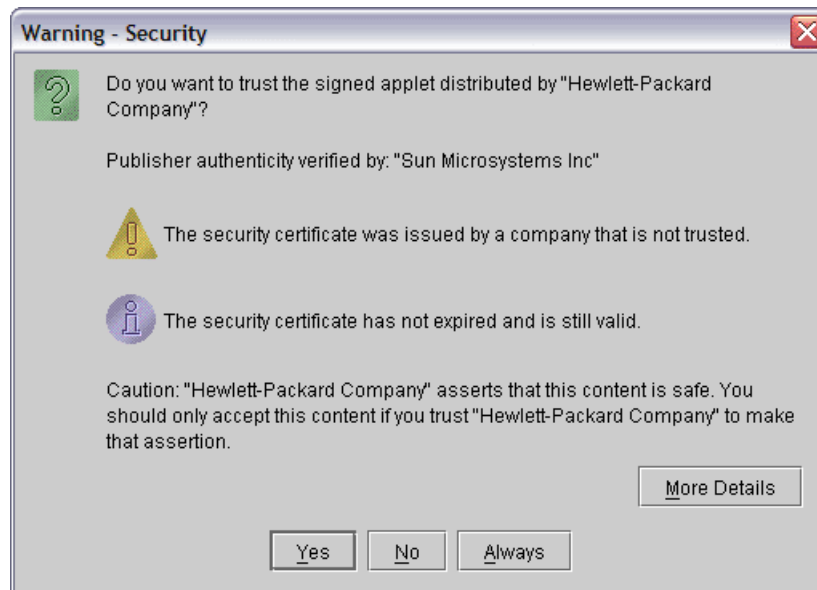


Figure 4 Java Plugin Security Warning Message Box: Sun Microsystems

- 12 To run the Policy Builder without future alerts, click **Grant Always**.

By default, the Policy Builder applet loads in an open browser window. If one is not open, the applet launches a window for you. If you are using Internet Explorer as your default browser, you can configure it to force the Policy Builder into a new window each time you start it with one of the desktop shortcuts. For details, see [To force Policy Builder to launch in a new IE Browser](#).

- 13 Once the Policy Builder applet appears, set it up as needed. For details, see [Setting Up Your Policy Matrix](#) on page 27.

► If you leave the Policy Builder idle for 30 minutes or more, the Administration server requires that you log in again so that your administration credentials can be renewed.

To force Policy Builder to launch in a new IE Browser

- 1 In a browser window, click **Tools** → **Internet Options**. The **Internet Options** dialog box appears.
- 2 Click the **Advanced** tab.
- 3 Under the **Browsing** category, uncheck the **Reuse windows for launching shortcuts** box.
- 4 Click **OK**. The next time you run the Policy Builder with one of the desktop shortcuts, it opens a new window rather than launching in one you are already using.

Using Policy Builder with Firefox 1.5

Policy Builder will work with Firefox in the Windows or Linux environments if you install the JRE in the following ways:

- **Windows:** To use the Policy Builder in the Windows environment, you must install the Java 1.4.2_10 JRE **after** you have installed Firefox. The installer for the JRE will automatically install the Java plugin into the Firefox environment.
- **Linux:** To use the Policy Builder on Linux, you must install the Java 1.4.2_10 JRE plugin manually into the Firefox environment.

➤ More information about installing the JRE on Linux can be found at <http://plugindoc.mozdev.org/linux.html#Java>.

➤ Do not use the feature in Firefox to “Install Missing Plugins” as it will install the wrong version of the JRE.

To Use Policy Builder with Firefox 1.5

- 1 Verify that you do not have any existing Java plugins installed by typing in the following URL in the Firefox browser:
`about:plugins`
If there are existing JRE plugins installed you need to remove those versions of the JRE.
- 2 Install the Java Runtime Environment.
- 3 Make a **symbolic link** to `libjavaplugin_oji.so` in your Firefox Plugins directory. Use the copy located in the `plugin/i386/ns610-gcc32` directory in the JRE 1.4.2.
- 4 Run the `about:plugins` command again to verify that you only have the 1.4.2_10 plug-in installed.

3 Building Your Identities and Resources Trees

This chapter describes the two axes of the Policy Builder: the Identities Tree and the Resources Tree. Together the Identities Tree and Resources Tree visually illustrate the connection between identities, resources, and the policies you administer.

Chapter Overview

This chapter consist of the following topics:

- [Using the Policy Builder: An Introduction](#) on page 25
- [Before You Begin](#) on page 27
- [Setting Up Your Policy Matrix](#) on page 27
- [About the Identities Tree](#) on page 28
- [About the Resources Tree](#) on page 43

Using the Policy Builder: An Introduction

To set up a policy, create two sets of data that form the vertical and horizontal axes of the grid:

- **Resource data:** There are two kinds of resources that can be found on the vertical axis of the grid:

- **Network resources:** In the Resource Access tree. Resources from any number of Enforcer-protected content servers (typically web and application servers) form the Resources Tree.

Automatically included among these resources in the Policy Builder's Root Administration mode are the Administration server's network resources, which allow you to enable and disable Delegated, Web, and Self Administration. For more information on the Administration server network resources, see [Chapter 10, Controlling Administrative Access](#).

- **Administrative resources:** In the Administrative Access tree. Automatically created and uneditable, these resources allow administrators to delegate access to certain aspects of the Policy Builder to selected administrators. You can also set workflow conditions for any delegated resource or function.

The Administrative Access tree is only displayed in the Policy Builder's Root Administration mode, or in Delegated Administration mode when the Delegated Administrator has been granted subdelegation entitlements. For more information on the Administrative resources, see [Controlling Administrative Access](#). This resource data is part of the Policy Store.

- **Identity data:** Profiles from any number of directory locations form the Identities Tree. The Identities Tree also includes Unknown Identities that have yet to be authenticated.

The grid allows you to quickly and easily identify user and resource pairs, and assign an access policy for this combination. **Figure 5** illustrates an example Policy Matrix populated by data along both the Identities and Resources Trees.

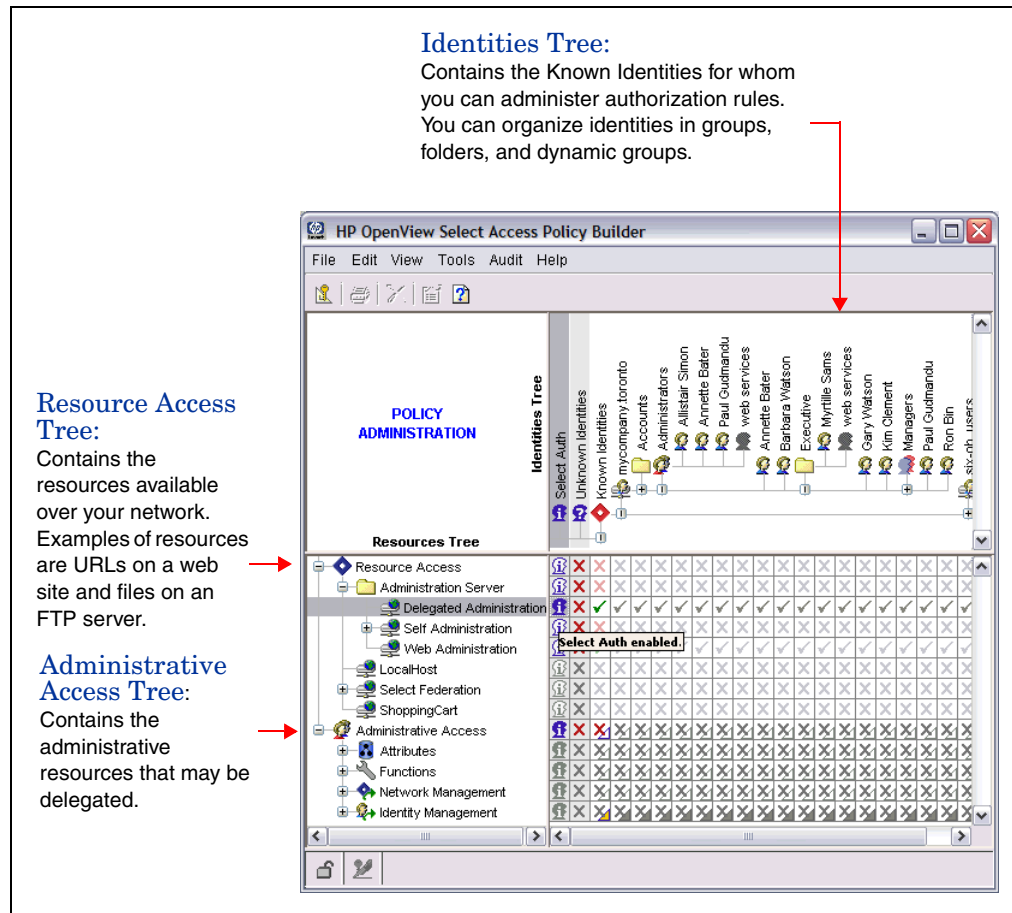


Figure 5 Policy Matrix: Identities and Resources Tree Defined

▶ Select Access will be adding the capability for defining privacy policies within Select Access' Rule Builder via the Privacy Manager, in the near future. In preparation for the addition of this new capability, this version of Select Access has a new entry under the **Tools** menu: **Data Source Configuration**. This menu item is currently greyed out. It will be activated if the Privacy Manager plugin is installed, once available.

Before You Begin

Before you set up your Policy Matrix, think about your existing directory structure, as well as your corporate resources, and answer the following questions:

- IdentitiesTree-specific questions:
 - Will user data be centrally located or will it be distributed among multiple identity locations?
 - How will you set up identities so that they can take advantage of policy inheritance? This enables you to ultimately create access policies more quickly.
 - How do you intend to maintain this tree as the number of known identities shifts over time?
- Resources Tree-specific questions:
 - Which method of building the Resources Tree best meets the need of your organization and best suits the size of your network?
 - How do you intend to maintain this tree as the number of services and/or resources shift over time?

Setting Up Your Policy Matrix

To set up the Policy Builder, follow the steps outlined in [Table 3](#).

Table 3 Setting Up the Policy Matrix

Setup Task	Details
1 Add your user data, which can be stored across one or more network identity locations. Each identity location becomes a top-level branch on your Identities Tree.	About the Identities Tree on page 28
2 Build the branches of your Resources Tree by adding your corporate services to the vertical axis of the Policy Matrix. Once you have added your branches, you can populate them with the content these services serve.	About the Resources Tree on page 43

About the Identities Tree

Your user information is shown in the Identities Tree to the right of the **Known Identities** column. The Identities Tree can contain any combination of identities, groups, dynamic groups, and folders, as shown in [Figure 6](#). You can store these elements in any number of identity locations, depending on how your directory system is architected.

- Identities that are members of groups and dynamic groups must be in the same identity location as that group or dynamic group. You may need to create mirror groups and dynamic groups across all identity locations to ensure they work correctly.
- You cannot move identities from one folder to another. Therefore, ensure you carefully think through your directory structure from the onset.

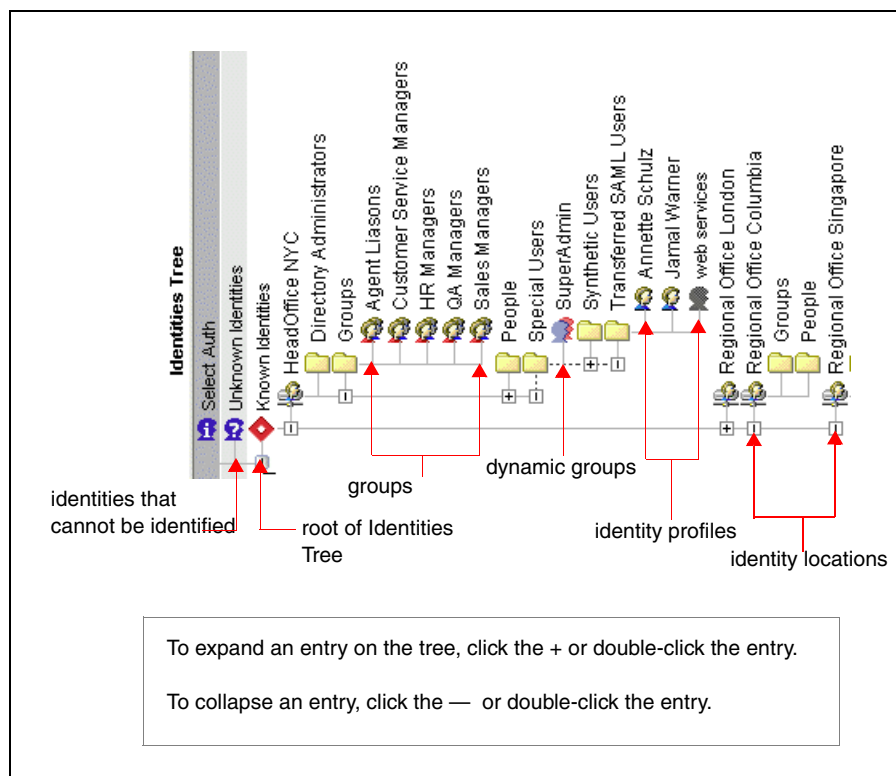


Figure 6 Identities Tree Overview

Data is represented by a graphic element or icon on the Identities Tree. Each graphic element that appears in the preceding figure is described in greater detail in [Table 4](#).

Table 4 Graphic Elements in the Identities Tree










Element	Description
Identity 	<p>A human identity profile. You can add an identity to the Policy Builder with the directory server.</p> <p>Note: If you delete an identity from the Identities Tree, it is also permanently deleted from the directory server it is stored in.</p>
Non-human Identity 	<p>A non-human identity profile. You can add a non-human identity to the Policy Builder with the directory server. You create and protect non-human identities the same way you would human identities in the Policy Builder.</p> <p>Note: If you delete an identity from the Identities Tree, it is also permanently deleted from the directory server it is stored in.</p>
Group 	<p>A collection of identities who usually share the same access 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.</p>
Dynamic Group 	<p>A collection of identities whose membership is based on attributes configured in the identity profile. As a result, a dynamic group is dynamic, and identities are added and removed automatically if user attributes change over time.</p>
Folder 	<p>Usually represents a department, division, or other discrete business unit. You can use folders to organize your identities and groups. When you create an access policy for a folder, all identities and groups in the folder inherit the access policy, unless you override it.</p>
Identity location 	<p>An identity location in any directory server where your user information is stored. When you create an access policy for the root of the tree, all items in the tree inherit the access policy, unless you override it.</p> <p>Note: Identity location distinguished names (DNs) cannot overlap.</p>

Table 4 Graphic Elements in the Identities Tree (cont'd)

Element	Description
Unknown Identities 	A way of creating rules for those identities who have not been or cannot be identified. Enable Select Auth for the given resource if you want to authenticate unknown identities who request access to that resource. Unknown identities are described in more detail in Administering Access Policies For Known or Unknown Identities on page 130.
Known Identities 	The root of one or more identity locations. Adding identity locations to the Known Identities column is described in more detail in Building the Identities Tree on page 31.
Select Auth 	The Select Access native authentication method. Select Auth allows you to pick the authentication services used to authenticate any identities who try to access a network's resources. For details, see Avoiding Incorrect Service Setup for Groups and Dynamic Groups on page 127.

Web Services

Select Access supports both Microsoft .NET (WS-Security) and AXIS 1.1 Java-based web services. The WSE Enforcer plugin is Select Access' decision-enforcement component for .NET web services. It secures .NET web services.

You can secure SOAP messages sent by your web service by configuring the WSE Enforcer plugin to sign and encrypt all SOAP messages.



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 (`gac_util.exe`). For information on installing these components, refer to your .NET documentation.

For added security, you can encrypt outgoing SOAP messages. Outgoing messages are encrypted using the same certificates used to sign incoming SOAP requests. Therefore encryption relies on the incoming message to be signed by a valid certificate which supports digital signatures.

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

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

- Password
- Certificate

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

Building the Identities Tree

Unless you have worked with a previous version of Select Access, your Identities Tree is empty by default. You build the branches of the Identities Tree by defining the location of your user data on the network. Depending on your directory and how dispersed it is, you can have all user data centrally located on one computer, or you can divide it among many. If you have multiple user data sources, you need to configure an identity location for each one.



When you add an identity location, you can replicate it across one or more directory servers. For more information on how to set up replication and referrals for a Select Access-protected system, see [Chapter 2, Directory Server Integrations](#), in the *HP OpenView Select Access 6.2 Network Integration Guide*.

Each identity location you require is added to a global identity location list. This list of identity locations:

- Creates the top-level branches on the Identities Tree. Each branch point contains its own set of identity profiles.
- Determines the identity profile search order used by the authentication services configured for all Known Identities. In this case, when an authentication service performs a search for an identity profile, it looks for it in the first identity location you define, before proceeding to subsequent locations in the order they appear.

Once you have added all the identity locations needed to build a complete Identities Tree, you can organize the identity profiles further with a combination of folders, groups, and dynamic groups. For details, see [Working with Identities, Groups, Dynamic Groups, and Folders](#) on page 68.

Sample scenario: a large multinational

For example, suppose we have a multinational organization with regional offices in New York, London, Columbia, and Singapore. Each of these offices has its own directory server with identity profiles for each employee in the region. In this case, the administrator creates a global list like the one shown in [Figure 7](#).

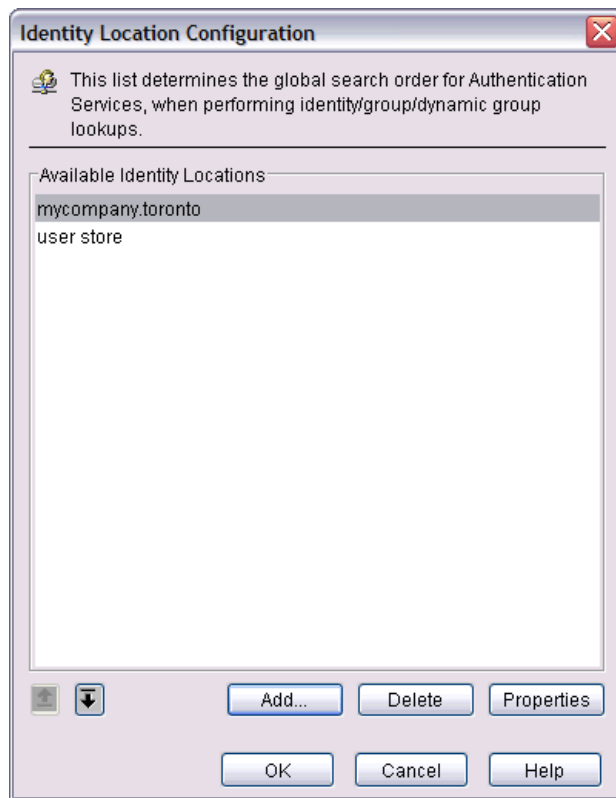


Figure 7 Example Identity Location List

The order of this global list determines the order the Policy Builder replicates when the identity locations are rendered as branches of the Identities Tree like the one shown in [Figure 8](#).



Figure 8 Example Identities Tree Rendered



Profile lookups also take place in the order they appear in the global list, and therefore in the Identities Tree. This means the Policy Validator checks for credentials in the first identity location. Only if the identity is not found does it try subsequent locations.

To create a global identities location list

- 1 Click **Tools** → **Identity Location Configuration**. The **Identity Location Configuration** dialog box appears.

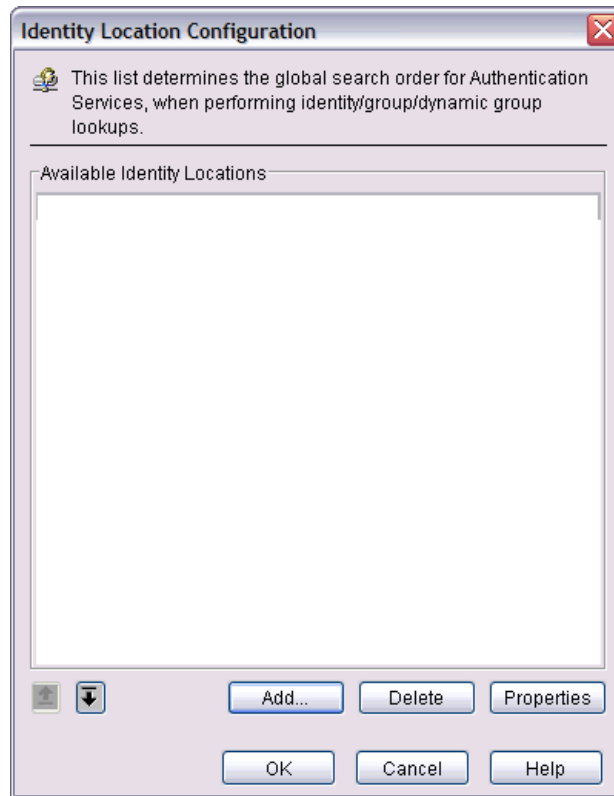



Figure 9 Identity Location Configuration Dialog Box

- 2 To add a new identity location to this list, click **Add**. This displays the **New Identity Location** dialog box, which allows you to define a new location.
- 3 To modify an identity location that already exists in this list, select the corresponding profile and click **Properties**. This displays the **Identity Location Properties** dialog box, which allows you to change the properties you configured for this location.
 For details on adding or modifying an identity location, see [To add or modify an identity location](#) on page 33.
- 4 To determine the priority of the search order used by authentication services, select an identity location in the list and click the corresponding **Up** or **Down** button. Repeat this step as needed.
- 5 Click **OK**. The Identities Tree displays your identity locations as they appear in your list. Policy Validator also performs identity lookups based on this order.

To add or modify an identity location

- 1 Do one of the following:
 - From the **Identity Location Configuration** dialog box, click **Add** to create a new identity location, or select an identity location and click **Properties** to modify an existing one.
 - Right-click the **Known Identities** column and select **New** → **Identity location**.

The corresponding **New Identity Location Configuration** or **Identity Location Properties** dialog box appears, displaying four tabs you can configure, as outlined in [Table 5](#):

- 2 Select any combination of these tabs and configure your preferences for these settings.

Table 5 Password Policy Configuration Overview

Password policy tab	For details, see...
General: This tab allows you set the general identity location parameters.	To set the identity location's general parameters on page 34
Replicated Servers: This tab allows you to define a list of replicated directory servers which will be used if your current user store is unavailable.	To create a list of replicated servers on page 36
Preferred Attributes: This tab allows you to define the list of attributes that Policy Validator uses to test permissions of selected identity profiles.	To select the preferred identity attributes on page 37
Identity: This tab allows you to define how the identities added to this location will be identified in the Identities Tree.	To specify how identities will be identified in the Policy Builder on page 38

- 3 When you have finished configuring all four tabs that combine to define the new identity location, click **OK** to add this location to the global list. For details, see [To create a global identities location list](#) on page 33.

To set the identity location's general parameters

- 1 In the **New Identity Location** dialog box, select the **General** tab, as shown in [Figure 10](#).

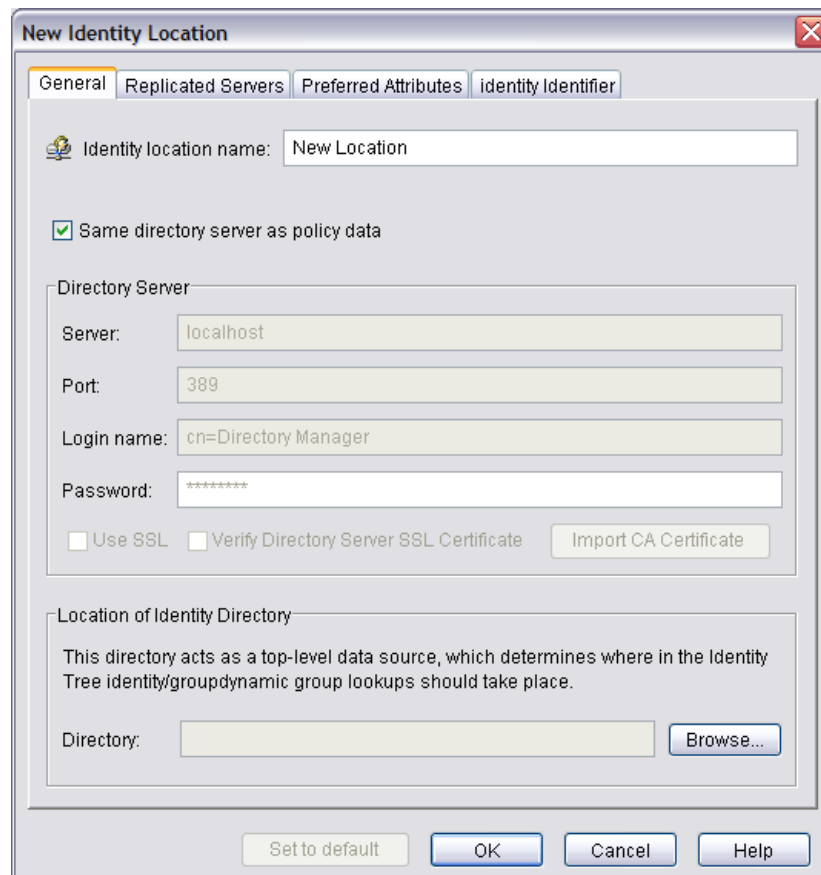


Figure 10 New Identity Location Dialog General Tab

- 2 Enter a name in the **Identity location name** field. Ensure it accurately describes this identity location. This name identifies the identity location on the Identities Tree. A descriptive name is particularly important when you have multiple directories.
- 3 If the identity location is the same as the location of your policy data, select the **Same directory server as policy data** check box, and skip to [step 5](#).
- 4 If the identity location is not the same as the location of your policy data, configure the following fields in the **Directory Server** group:
 - **Server:** Enter the host name or IP address of the computer hosting the directory server.
 - **Port:** Enter the port number for the directory server.
 - **Login Name:** Enter the administration login name that gives you access to read/write data on this directory server.
 - **Password:** Enter the administration password that gives you access to read/write data on this directory server.
 - **Use SSL:** Check this box if you want to encrypt the session that the Policy Builder opens with this directory server with SSL.
 - **Verify Directory Server SSL Certificate:** Check this box if you want the Policy Builder and Policy Validators to verify the certificate before opening an SSL session with it.
 - **Import CA Certificate:** Click this button to upload the certificate required to verify the directory server SSL certificate. For details, see [To import a CA certificate for a new identity location](#) on page 39.

- 5 Click **Browse** and select the area of the directory where the identity data is stored. For details, see [To select an identity location](#) on page 39. The DN of this location appears in the **Directory** field.



It is imperative that the DNs for different identity locations be unique, even if the directory servers are on different computers. Choosing a unique DN for each identity location prevents user authentication ambiguities from occurring when the Policy Validator caches identity profiles. You cannot use an identity location that is a child or parent of an existing identity location. You also cannot use a location in a different directory that shares the same name as an existing identity location.

For example, if you have an identity location called `Users` under `mycompany.com`, you cannot use `mycompany.com` or `Users/London` as new identity locations. You also cannot use `Users` if you have a directory on `london.mycompany.com`.

For examples of how this affects your directory topology, see [Chapter 2, Directory Server Integrations](#), in the *HP OpenView Select Access 6.2 Network Integration Guide*.

To create a list of replicated servers

- 1 If the identity location has been replicated to other directory servers, in the **New Identity Location** dialog box, select the **Replicated Servers** tab, as shown in [Figure 11](#).

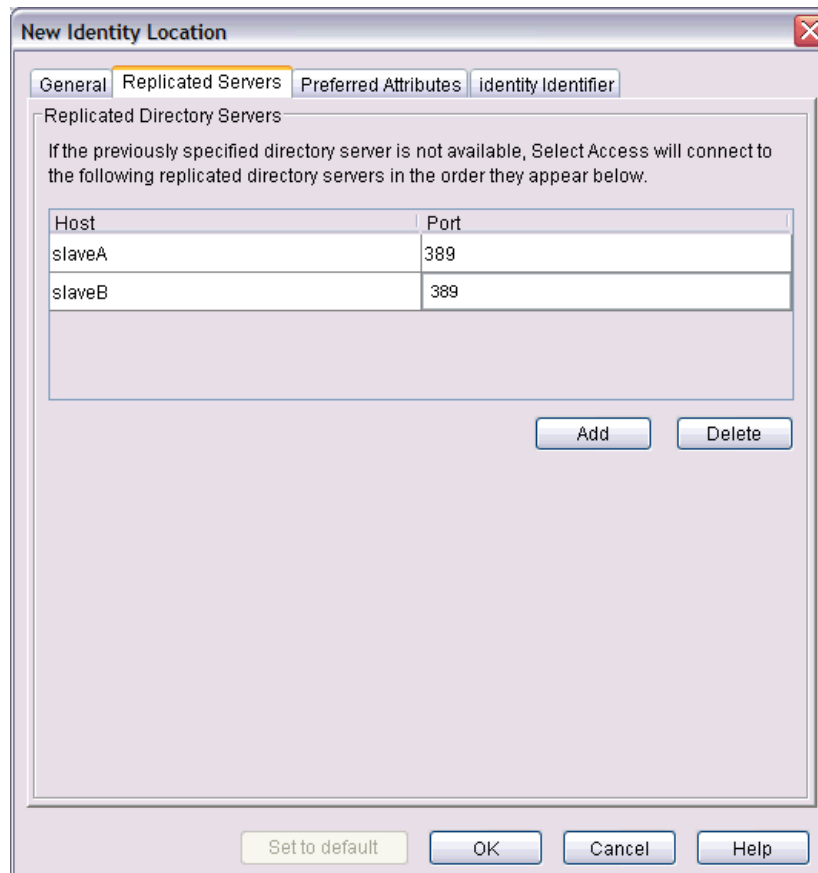


Figure 11 Identity Location Dialog Box Replicated Servers Tab

- 2 Add servers to the list as necessary:
 - Click **Add**.
 - Configure the hostname (or IP address) and port the server runs on.
- 3 To delete a directory server that no longer shares the same identity location and data, select the corresponding row and click **Delete**.

To select the preferred identity attributes

- 1 In the **New Identity Location** dialog box, select the **Preferred Attributes** tab, as shown in Figure 12.

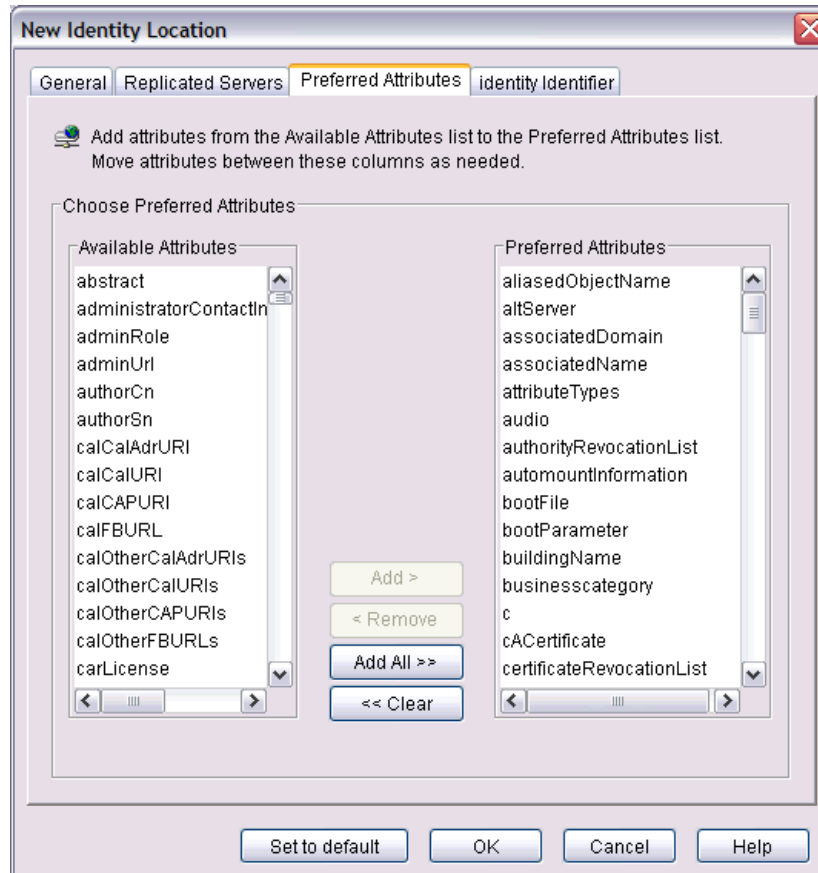


Figure 12 Identity Location Dialog Box Preferred Attributes Tab

- 2 Select all the attributes you require. Do this by selecting one or more attributes in the **Available Attributes** list and clicking **Add** to move them to the **Preferred Attributes** list.
 - Available attributes are read from the directory server's schema. Schema attributes are not just limited to user attributes, therefore, ensure that the attribute you are selecting is an attribute included in an identity profile. If you do not see this attribute in an identity profile, then your attribute logic decision point always denies access to all identities.
 - If you make `givenname` a preferred attribute on ADS, note that ADS directories have a maximum string limit of 64 unicode characters for this attribute.

- 3 To remove attributes in the **Preferred Attributes** list, do one of the following:
 - Select individual attributes and click **Remove**.OR
 - Click **Clear** to remove all listed attributes.

To specify how identities will be identified in the Policy Builder

- 1 In the **New Identity Location** dialog box, select the **Identity Identifier** tab, as shown in Figure 13.

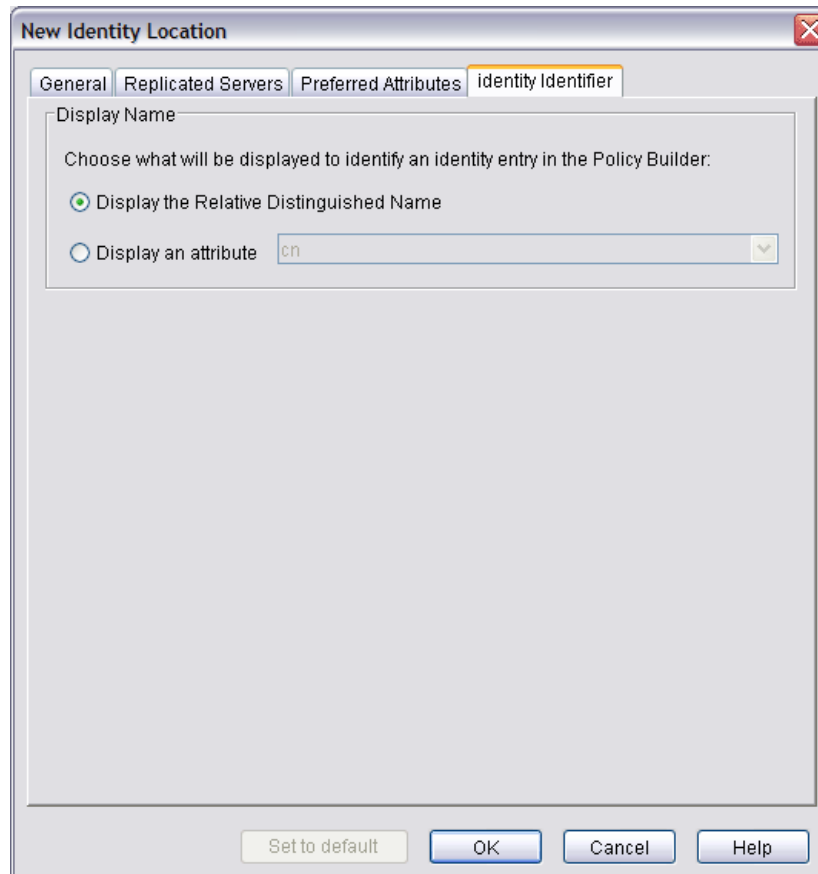



Figure 13 Identity Location Dialog Box Identity Identifier Tab

- 2 Choose how identities will be displayed on the Known Identities tree:
 - Click the **Display Relative Distinguished Name** option, if you want use the RDN if one exists.
 - Click the **Display an Attribute** option, if you want to use a specific attribute. Select an attribute from the adjacent list. This list contains the attributes you selected in the **Preferred Attributes** tab. For details, see [To select the preferred identity attributes](#) on page 37.

To select an identity location

- 1 To display the **Select Location** dialog box, click **Browse** from the **Identity Location** dialog box. This displays the profiles on your Identities Tree (if any). All identity locations are represented by the  icon.

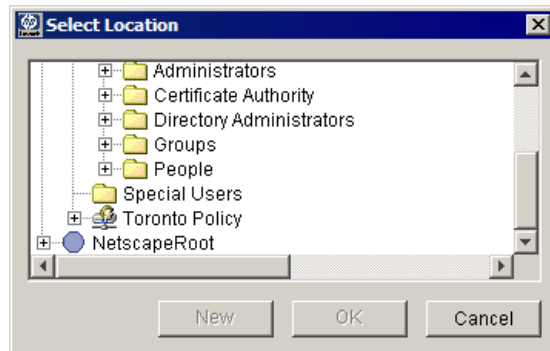


Figure 14 Select Location Dialog Box

- 2 Do one of the following to add the DN of this location to the **Directory** field in the **Identity Location** dialog box:
 - To use an existing branch on this tree as your identity location, select the folder and click **OK**.
 - Only folders are rendered on the Identities Tree. Profiles are not displayed.
 - To create a new location, click **New**. This displays the **New Folder** dialog box. Enter a name for this folder in the **Name** field and click **OK**.

To import a CA certificate for a new identity location

- 1 From either the **New Identity Location** or the **Identity Location Properties** dialog box, click **Import CA Certificate**. The **Import CA Certificate** dialog box appears.
- 2 Choose one of the following locations to import a certificate from and click its corresponding **Browse** button to define the path to it:
 - **Import from policy data location:** Search the directory server acting as your Policy Store for the certificate. The certificate must already be uploaded to this location or an error message appears.
 - **Import from identity location:** Search the directory server acting as one of your identity location branches for the certificate. The certificate must already be uploaded to this location or an error message appears.
 - **Import from file:** Search the host computer's hard drive (or the network) for the certificate.
- 3 Click **OK**.

Manually Adding or Modifying an Identity Profile

Once you have created an Identities Tree, you can add new identities to any specific identity location or a folder below this branch, or modify one you have already added as part of a specific identity location.

These profiles are automatically written to the directory server, so you do not have to directly edit the directory itself.

- Identities can only self-manage passwords on Microsoft ADS if Microsoft ADS is running over SSL. Therefore, you cannot create identity profiles that require passwords, modify passwords, or use password management, unless SSL is enabled. For details on password self-management, see [Chapter 8, Managing Identity Profiles](#).
- Additionally, password lengths must meet the requirements of the directory unless you disable ADS' password policy. For details, see [Active Directory 2003 and Profile Password Setup Problems](#) on page 300.

To create or modify an identity profile

- 1 Do one of the following:
 - Right-click a folder or identity location branch in the Identities Tree and click **New** → **Identity**.
 - Right-click an existing identity profile and click **Properties**.

The corresponding **New Identity** or **Editing Identity** dialog box appears.

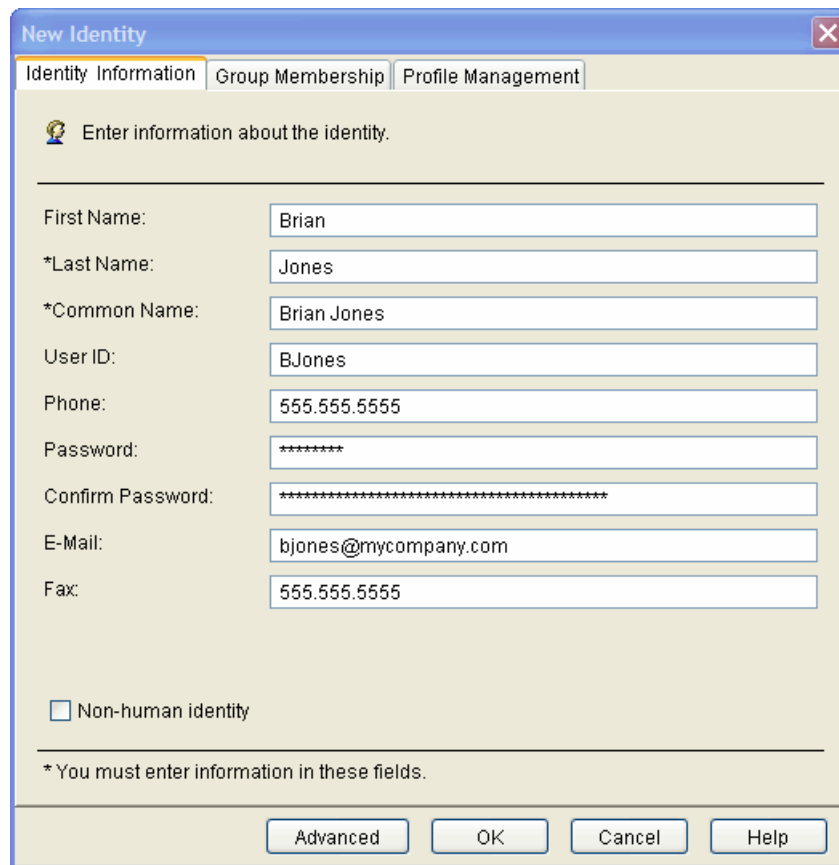
- The contents of the **New Identity** dialog box vary depending on your directory server.



For Active Directory, the identity's object class is `User`, not `inetOrgPerson`, which is the object class used by all other directory servers. The difference in user object class impacts the following components and features, because the number and the types of user attributes between these two classes vary:

- How the Policy Validator performs password-based authentication
- How the Policy Validator registers new identities
- Password management of identities

If an attribute is not available in the `User` class, you can add it by clicking **Advanced** of the **Identity** properties dialog box, and modifying the **Attributes** tab accordingly. ADS does not allow you to add an attribute that is contrary to the schema definition for identity profiles. For details, see [Configuring Advanced Identity Profile Properties](#) in the *HP OpenView Select Access 6.2 Concepts Guide*.



The image shows a 'New Identity' dialog box with three tabs: 'Identity Information', 'Group Membership', and 'Profile Management'. The 'Identity Information' tab is active. It contains a message: 'Enter information about the identity.' followed by several input fields. The fields are: First Name (Brian), *Last Name (Jones), *Common Name (Brian Jones), User ID (BJones), Phone (555.555.5555), Password (masked with asterisks), Confirm Password (masked with asterisks), E-Mail (bjones@mycompany.com), and Fax (555.555.5555). There is a checkbox for 'Non-human identity' which is unchecked. At the bottom, there is a note: '* You must enter information in these fields.' and four buttons: 'Advanced', 'OK', 'Cancel', and 'Help'.

Figure 15 New Identity Dialog Box

- 2 Enter or review the information outlined in [Table 6](#) on the **Identity Information** tab.

Table 6 Fields of the New Identity Dialog

Field	Description
First Name	Required for all directory servers. Enter the end user's first name.
Last Name	Required for all directory servers. Enter the end user's last name.
Common Name	<p>Required for all directory servers. Enter the end user's full name. (For example, John Smith or John T. Smith.) The string you enter is used to display the identity profile on the Identities Tree.</p> <p>Note: For iPlanet and Sun ONE directory servers, do not create a name with two or more backslashes in a row. Otherwise, your directory server experiences difficulties when looking up these profiles. This can result in an "object not found" exception when you try to expand the folder containing the item. However, you can create names with a single backslash, as well as with multiple backslashes that are separated by other characters.</p>
ID	Enter an identifier.

Table 6 Fields of the New Identity Dialog (cont'd)

Field	Description
Profile Name	Required for Active Directory . The logon name used to support non-Windows 2000 clients and servers (Windows 95, Windows and LAN Manager).
Principal Name	Optional for Active Directory. A string property that specifies the principal name of the end user in the form of an Internet-style login name.
Password, Confirm Password	Optional for Active Directory if connecting over SSL. For details, see the note at the beginning of To create or modify an identity profile on page 40. Enter the end user's password.
Phone	Optional for all directory servers. Enter the end user's telephone number.
E-Mail	Optional for all directory servers. Enter the end user's email address.
Fax	Optional for all directory servers. Enter the end user's fax number.
Non-human Identity	Optional. Check this box to specify a non-human identity. The box is unchecked by default, for human identities.



Non-human identities are created and protected in the Policy Builder in same way as human identities.

- 3 Click **OK** to commit these changes to the directory server for that identity profile and add the identity to the Identities Tree.



You can either use the Common Name or the User ID as the relative distinguished name (RDN). For details on setting the RDN, see [To specify how identities will be identified in the Policy Builder](#) on page 38.

To refresh data

To refresh data, click **View** → **Refresh**. The information currently shown in the Identities Tree, Resources Tree, Policy Matrix, Rule Builder, and the authentication services list is refreshed.



Refreshing data is particularly important when multiple administrators are making different changes that can often overlap.

Deleting an Identity

When you delete an identity, the profile is permanently deleted from the Identities Tree and from the directory server.

To delete an identity

- 1 On the Identities Tree, right-click an identity profile and click **Delete**. A confirmation dialog box appears.
- 2 Click **Yes**. The identity is deleted from that identity location.

About the Resources Tree

Your resource information is shown in the **Resources Tree**. The Resources Tree contains network services and resources you can protect with access policies. The tree contains services, resources, and folders, as shown in [Figure 16](#). This enables you to set a single policy and have it apply to all access points, web or wireless.

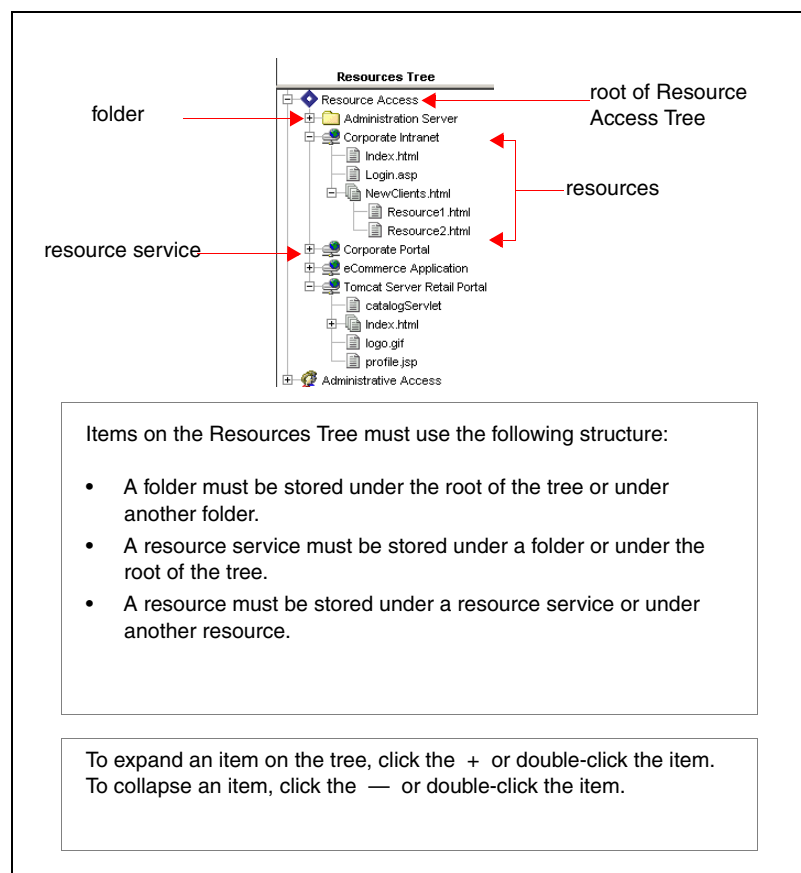


Figure 16 Resources Tree



- A **network resource service** provides access to one or more resources. For example, a web server provides access to the data that resides on the server, and an NT domain provides access to the data available on the domain. A service can also provide access to other services. For example, an extranet can provide access to a company's web server, FTP server, and NT domain.
- A **network resource** is a discrete piece of information identities can access over the network, such as a folder, file, or URL. A resource can also contain other resources. For example, a folder on an FTP server can contain files, and a URL on a web server (such as

www.mycompany.com) can have sub-URLs (such as www.mycompany.com/accounting, www.mycompany.com/accounting/january, and www.mycompany.com/accounting/january/default.htm).

Building the Resources Tree

You build the branches of the Resources Tree by first adding network services such as FTP servers, web servers, application servers, and so on. Once you have added these services, you can determine what network resources are available through the service (such as folders, files, and URLs).

Depending on the number of services and resources on your network, there are different techniques you can use:

- **For services:** Policy Builder gives you two options, based on your network size and security requirements:
 - *Scan your network for network services:* Use this technique when you have a large, distributed network, where manually adding or maintaining a list of services is a cumbersome and tedious task. Scanning for services can take some time to complete, especially on global networks.
 - *Manually create a new network service:* Use this technique when you have a small, relatively localized network or when adding new services sporadically when they come online. In these cases, it is faster to add the service than it is to perform a manual discovery of new services on your network.
- If you add one or more resources below another resource, the icon automatically changes from  to , thereby changing a resource entry to a directory of resources.

For details, see [Adding Network Resource Services to the Resources Tree](#) on page 45.

- **For resources:** Policy Builder gives you three options, based on your network size and security requirements:
 - *Run an automated resource discovery:* The Policy Builder includes a Network Resource Discovery plugin for HTTP or HTTPS services and adds discovered resources to a corresponding service's branch. However, if you have services other than HTTP or HTTPS, you can create and upload a custom one. For details, see [Uploading Custom Plugins](#) on page 289.
 - *Import a list:* You can use any third-party tool to scan a given service. The tool outputs URLs as a list that you can import into the Policy Builder.
 - *Manually create a new resource on a service branch:* Do this if you do not have many resources to add to the tree or if you have already run a network discovery and a few new resources have recently been made available. You might also use this technique if certain plugins are not allowed access to the service in question.

The directory server contains the information used to create the Resources Tree. This information is stored in the Policy Data location you selected when configuring the directory server. For details, see [About the Resources Tree](#) on page 43.

Updating the Resources Tree

The Policy Builder builds the Resources Tree using the information stored in the directory server, and does not check your network to see if resources have been added or removed. You are responsible for adding new network resources to the Resources Tree and deleting items that are no longer available on your network.

For example, suppose your network contains an HTTP resource called `www.mycompany.com` that you added to the Resources Tree. You later add a new resource called `www.mycompany.com/sales` to your network, so you must also add this resource to the Resources Tree. You can add the resource by discovering the resources on `www.mycompany.com` or by manually adding the new resource to the tree.

Adding Network Resource Services to the Resources Tree

A network resource service provides access to one or more resources. Examples of services include web servers and FTP servers. Network services can be divided into two categories:

- **Server-specific resource services:** Like a mirrored FTP site, these services provide access to one or more servers.
- **Non-server-specific resource services:** These services are not tied to one specific server.
 - Any Enforcer-protected resource services that you do not add to the Resources Tree inherit the access policy that is set against the root of the Resources Tree. Therefore, to ensure that the Policy Validator applies the right access decision to a resource request, we recommend that you add all Enforcer-protected resource services to the Resources Tree. This allows you to apply an explicit policy against it.

There are two ways to add network services to the Resources Tree. These alternatives are listed in [Table 7](#).

Table 7 Resources Tree Overview

Service Registration Method	Details
Creating a new network service	To create a new network service on page 45
Scanning your network to discover your network services	To discover your network resource services on page 48

To create a new network service

- 1 Right-click a folder or the root of the Resources Tree.
- 2 Click **New** → **Resource Server**. The **New Resource Server** dialog box appears, as shown in [Figure 17](#).

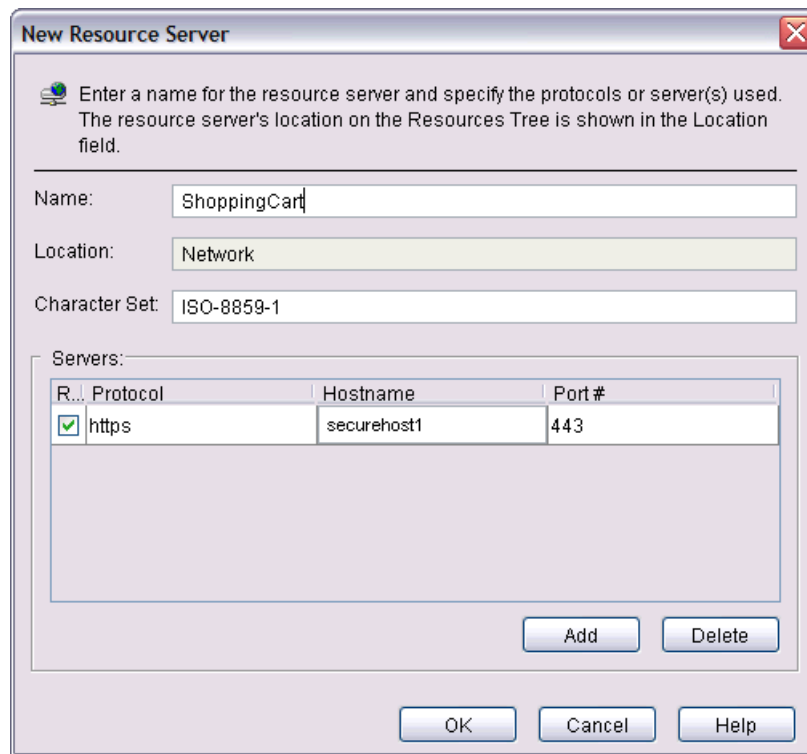


Figure 17 New Service Dialog Box

- 3 In the **Name** field, enter a name for the service to be used on the Resources Tree. For example, if you are creating a service for the web server, you can use the web server's hostname (for example, `www.mycompany.com`) or a description of the web server (for example, Internal Sites) for the service name.
 - Do not use two or more consecutive backslashes in the resource's entry name. Policy Builder cannot read or delete an entry in the directory server that contains multiple, consecutive backslashes.
 - The **Location** field shows where the service is created on the Resources Tree.
- 4 In the **Character Set** field, type the name of the character set used by this service, if the character set used is something other than ASCII (that is, ISO-8859-1). The encoding you select will be used for resource discoveries as well. For details, see [To run a discovery plugin for network resources](#) on page 58.

Valid character sets are those that are supported by Java. They include character sets from two categories:

- Basic Encoding sets
- Extended Encoding sets

- For a complete list of supported character sets, see <http://java.sun.com/j2se/1.4.2/docs/guide/intl/encoding.doc.html>. Note that some encodings have canonical names that are different from the names shown in the specification on this page. The required names of these encodings are supported through an alias mechanism: US-ASCII maps to ASCII, ISO-8859-1 to ISO8859_1, UTF-8 to UTF8, UTF-16BE to UnicodeBigUnmarked, and UTF-16LE to UnicodeLittleUnmarked.

- 5 Enter information about the resource service. For details, see one of the following sections:
 - [Entering information for a non-server-specific resource service](#) on page 47
 - [Entering information for a server-specific network resource service](#) on page 47
- 6 Click **OK**. The resource service is added to the Resources Tree.

Entering information for a non-server-specific resource service

If the resource service is not tied to one specific server, enter the protocol the service uses.

- 1 Click **Add**. A new row appears.
- 2 Click in the **Protocol** field and do one of the following:
 - Click the arrow that appears and select the protocol used by the server.
 - Manually enter the protocol name.
 - The protocol names and port numbers (if any) are defined in the Network Resource Services list.
 - Entering a large port range (for example, 80-8000) causes a limit warning message.

Entering information for a server-specific network resource service

If the resource service provides access to one or more servers, enter the protocol, hostname, and port for each server.

- Entering a large port range (for example, 80-8000) causes a limit warning message.

If you have multiple servers that contain the same resources, you can add all the servers to this tab. This allows you to create access policies for the servers as a group. All the servers use the access policies that you create for the resource service. For example, if you have multiple servers that contain the same resources (such as mirrored web servers), you can enter all the servers, as shown in [Figure 18](#).

R...	Protocol	Hostname	Port #
<input checked="" type="checkbox"/>	https	securehost1	443
<input type="checkbox"/>	https	securehost2	443
<input type="checkbox"/>	https	securehost3	443

Figure 18 Editing Resource Service Dialog Box

Or, if the same resources are available through different ports on the same server, enter all the ports used to access the resources, as shown in [Figure 19](#).

R...	Protocol	Hostname	Port #
<input type="checkbox"/>	https	securehost1	443
<input type="checkbox"/>	ftp	securehost2	21

Figure 19 Editing Resource Service Dialog Box

To add a server-specific resource service

- 1 Click **Add**. A new row appears.
- 2 Click the arrow that appears in the **Protocol** column, and select the server's protocol. When you select a protocol, the corresponding port number is entered automatically in the **Port #** field.
 - The protocol names and port numbers are defined in the Network Resource Services list.
- 3 In the **Hostname** column, enter the server's fully qualified host name.
- 4 In the **Port #** column, modify the port number if necessary. You can enter a single port number (for example, 80), a range of numbers separated by a hyphen (for example, 80-120), or a list of numbers separated by commas (for example, 10, 20, 40-75, 100).
 - Entering a large port range (for example, 80-8000) causes a limit warning message.
 - If the **Port #** field is blank, Policy Builder uses the port number defined for the protocol in the Network Resource Services list.
- 5 Select the **REP** check box beside the server you want to use as the representative server. When you run resource discovery on the resource service, only this server is scanned.

To discover your network resource services

- 1 Click **Tools** → **Discover Network Resource Servers**. The **Discover Network Resource Servers** dialog box appears.
- 2 Click the **Networks** tab to select the networks to scan, as shown in [Figure 20](#).

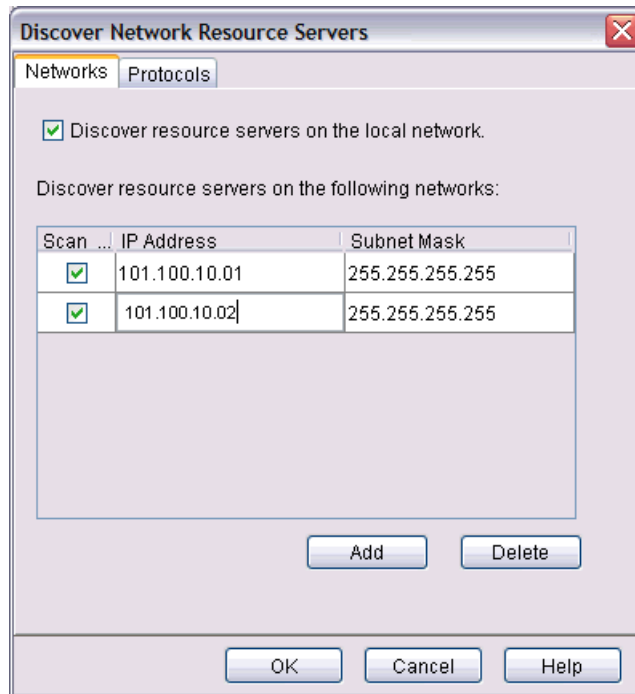


Figure 20 Discover Network Resource Servers Dialog Box Networks Tab

- 3 To scan the network to which the local computer is connected, select **Discover resource servers on the local network**. Policy Builder scans each computer in the network.
- 4 To scan specific networks or computers, do the following for each network or computer you want to scan:
 - Click **Add**. A new row is added.
 - In the **IP Address** column, enter the network's IP address.
 - In the **Subnet Mask** column, enter the network's subnet mask.
 - Select the **Scan** check box beside each network you want to scan. If you do not want to scan a network, clear the network's **Scan** check box.
- 5 To delete a network from the list, select the row the network is in and click **Delete**.
- 6 To select the ports you want to scan on each computer, click **Protocols**, as shown in [Figure 21](#). This tab contains common network protocols and the default ports these protocols run on.

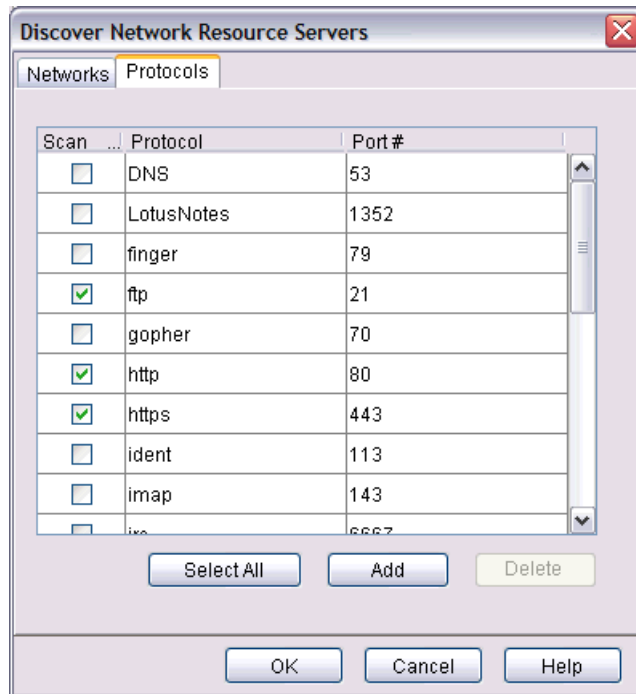


Figure 21 Discover Network Resource Servers Dialog Box

As illustrated by [Figure 22](#), for each item you select on this tab, network discovery finds all the resource services running on the specified port and adds the resource services to the Resources Tree. The resource services are stored in folders according to the protocol name.

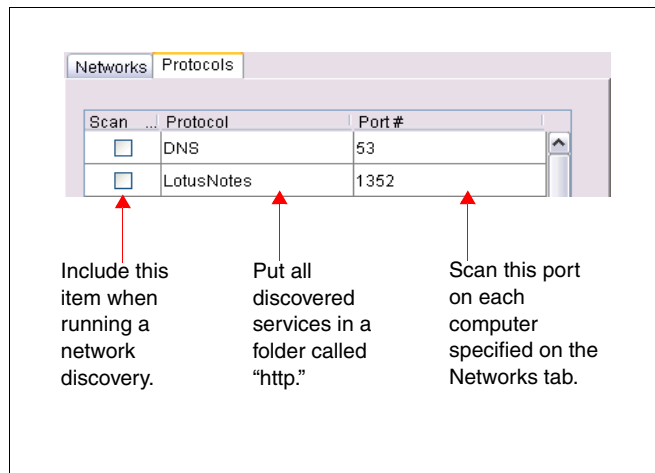



Figure 22 Description of the Discover Network Resource Servers Dialog Box

- 7 If necessary, add protocols to the list:
 - Click **Add**. A new row is added.
 - In the **Protocol** field, enter the protocol name. This name is used to create a folder on the Resources Tree.
 - ▶ The protocol name must exactly match the protocol name the Policy Enforcer plugin sends to the Policy Validator.


- In the **Port #** field, enter the ports on which the protocol is running. If the protocol is running on multiple ports, you can enter a range of ports (for example, 1-10, 100, 200-300). The Policy Builder uses the port number to access the protocol when running network discovery.
 - You can delete a protocol from the list by clicking in the row and clicking **Delete**.
- 8 If you are using the default protocols entered on the **Protocols** tab, make sure the ports shown are correct. If you have configured one of your network protocols to use a different port, be sure to update the **Port #** field.
 - 9 Select the **Scan** check box beside each protocol you want to scan. If you do not want to scan an item, clear the item's **Scan** check box.


 Click **Select All** to select all the protocols in the list, and click the button again to deselect all the protocols in the list.

- 10 Click **OK**. The **Network Resource Servers Discovery Progress** dialog box displays status messages as the network resource services discovery runs.


The Network Discovery plugin advances through your network by moving from computer to computer. Once a new computer is discovered, its IP address is displayed as well as details about that computer. If the computer is a host of any of the protocols you selected, the progress dialog box tells you the time it took to locate the hosts, and the number of hosts that were found.

- If you do not want to view these messages, click **Close**. You can click the flashing ball icon in the lower-right corner of the status bar to reopen the progress dialog box.
- If you want to cancel network resource services discovery, click **Stop**. Policy Builder adds any services discovered up to this point to the Resources Tree.

 Depending on the size of your network, the network discovery can take a fair amount of time to complete. If your network discovery is interruptive, you can terminate it at any time. For details, see [Terminating a Network Discovery](#) on page 63.

 You can rename the folders on the Resources Tree after running network discovery.

- 11 Once the plugin has finished scanning the network, a “Network Discovery Complete” message appears in the **Network Resource Servers Discovery Progress** dialog box. Click **Close** to close this dialog box while the discovery continues.

 You can cancel resource service discovery once it starts. For details, see [Terminating a Network Discovery](#) on page 63.

The resource services are added to the Resources Tree. In the Policy Matrix, the new services automatically inherit the access policy created for their parent branch on the tree.

To modify a network resource server

- 1 On the Resources Tree, right-click the resource server then click **Properties**. For details on these properties, see [To create a new network service](#) on page 45.
- 2 Modify any information.
- 3 Click **OK** to commit the changes to the Policy Store.

To delete a network resource service

- 1 On the Resources Tree, right-click the service and then click **Delete**. A confirmation dialog box appears.
- 2 Click **Yes** to commit to your changes to the Policy Store.
 - ▶ When you delete a network resource service, the service is permanently deleted from the Resources Tree and from the directory server. All resources under the service are also deleted.

Adding Network Resources to the Resources Tree

A network resource is a discrete piece of information that can be accessed over the network, such as a folder, file, or URL. Once you have added a resource service to the Resources Tree, you can add the resources that are available through the service. [Table 8](#) lists three methods you can use.

- ▶ When adding URLs to the Resources Tree, be aware that the Policy Validator uses the exact path requested by the identity when determining access. For example, if an identity requests a URL that points to a folder (such as `www.mycompany.com/customers`), the Policy Validator uses the access policies for this folder, not the access policies for the folder's default page (such as `www.mycompany.com/customers/index.htm`). Do not add the default page to the Resources Tree; instead, use the folder to set the authorization for the page.

Table 8 Network Resources Overview



Resource Registration Method	Details
1 Manually adding a new resource under a resource service.	Manually Adding a Network Resource to a Resource Server on page 52
2 Discovering the resources available through a service by using a Network Resource plugin to scan the service and add the resources to the tree.	Automatically Generating a List with a Discovery Plugin on page 54
3 Discovering the resources available through a service by using any tool to scan the service and then importing a list of resources.	Importing a Resource List on page 61

Manually Adding a Network Resource to a Resource Server

You can manually add a network resource to a resource service. Do this when:

- You do not have many resources to add.
- You have already run a network discovery and a few new resources have recently been made available.
- Certain plugins are not allowed access to the resource service in question.

- ▶ This method can be problematic and difficult to maintain if resources move on a regular basis.

- If you add one or more resources below another resource, the icon automatically changes from  to , thereby changing from a resource entry to a directory of resources.

To create a new network resource or edit an existing one

- 1 Do one of the following on the Resources Tree:
 - To create a new resource, right-click a resource service or resource and choose **New → Resource**.
 - To modify an existing resource, right-click a resource and choose **Properties**.

The corresponding **New Resource** or **Resource Properties** dialog box appears.

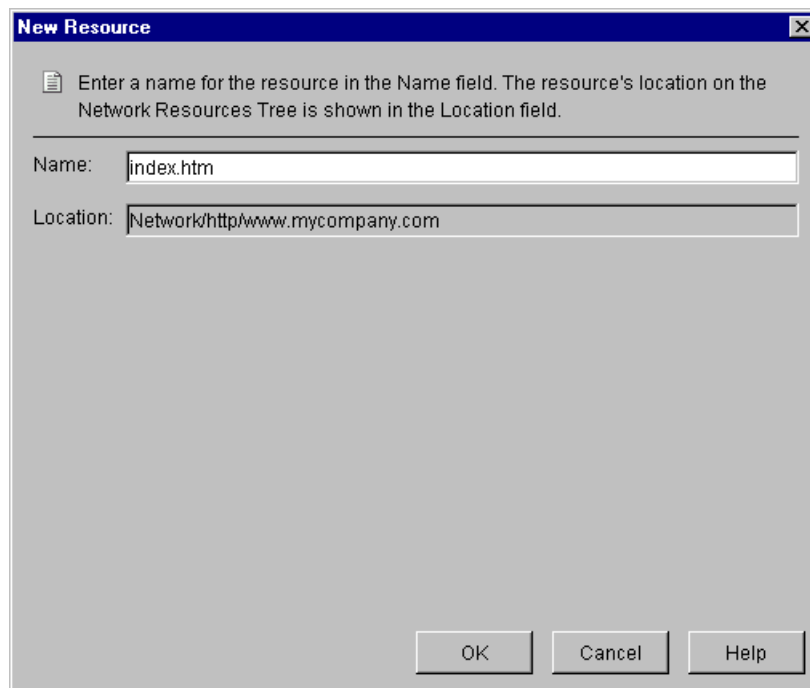


Figure 23 New Resource Dialog Box

- 2 In the **Name** field, enter a name for the network resource.

➤ The **Location** field shows where the resource is created on the Resources Tree.

⚠ The character “/” cannot be in the resource name. “/” is always treated as a resource path symbol.
- 3 Click **OK**. The resource is added to the Resources Tree.

Automatically Generating a List with a Discovery Plugin

A Network Resource plugin is any tool that scans a network resource service and generates a list of resources available through that service. You can have different plugins designed to discover resources for different types of services. For example, you can have a plugin that scans an FTP server and retrieves a list of the URLs on the server. You can use:

- [The HTTP or the HTTPS Network Resource plugin](#): This plugin is provided with the Policy Builder to discover the resources available through an HTTP or HTTPS resource service. These plugins scan a network service (the latter over SSL) to collect data on web-based resources, including redirected URLs.
- [A custom plugin you have uploaded to the Policy Builder](#): These plugins are used to discover resources on resource services other than HTTP or HTTPS. For details on how to upload a custom plugin, see [To upload a custom Decision Point or Authentication plugin](#) on page 289.



You can cancel resource discovery once it starts. For details, see [Terminating a Network Discovery](#) on page 63.

Plugin requirements

You can use any Network Resource Discovery plugin that meets the following requirements:

- The plugin runs on the command line.
 - The plugin outputs a list of resource URLs.
 - The output contains one URL per line.
 - The URLs output by the plugin use one of the formats described in [Table 9](#).
- The Policy Builder ignores any lines not containing valid URLs.
 - URL tags must contain a relative, rather than an absolute path to a resource on the same web server for the Network Resource plugin to discover redirected URLs. That is, the HTTP and HTTPS Network Resource plugins only detect a redirect if they locate the following type of tag:

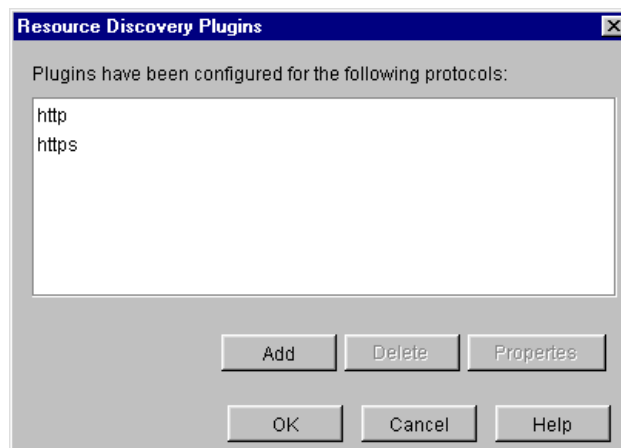
```
<META HTTP-EQUIV="Refresh" CONTENT="0;URL=allow.html">
```

Table 9 URL Output Formats

Format	Syntax
url	<code><protocol>://<hostname>:<port>/<dir></code> where <i>port</i> and <i>dir</i> are optional. The plugin outputs the full URL. For example: <code>http://www.mycompany.com:80/sales/default.asp</code> <code>https://www.mycompany.com</code> <code>ftp://ftp.mycompany.com</code>
protocol	<code>protocol://</code> The plugin outputs the name of the protocol. For example: <code>ftp://</code> <code>http://</code>
host	<code>hostname</code> The plugin outputs the host name. For example: <code>www.mycompany.com</code>
port	<code>port</code> The plugin outputs the port number. For example: <code>80</code>
dir	<code>dir</code> The plugin outputs the starting directory. For example: <code>sales</code>

To create a global Resource Discovery plugins list

- 1 Click **Tools** → **Resource Discovery Plugins**. The **Resource Discovery Plugins** dialog box appears. The plugins are listed according to the protocol they use, as shown in [Figure 24](#).

**Figure 24 Resource Discovery Plugins Dialog Box**

This dialog box allows you to enter a list of the Network Resource Discovery plugins you want to use. Select a plugin from this list when discovering the resources for a resource service.

- The Policy Builder's built-in HTTP and HTTPS plugins are already entered for you. If you want to use your own HTTP or HTTPS plugin instead, you can remove the built-in plugin from the list and add your own.
- 2 To add a new plugin location to this list, click **Add**. This displays the **New Plugin** dialog box, which allows you to configure a new plugin.
- 3 To modify a plugin already in this list, select the corresponding entry and click **Properties**. This displays the **Plugin Properties** dialog box, which allows you to change the properties you configured for this plugin.
- For details on adding or modifying a plugin, see [To configure a new or existing Resource Discovery plugin](#) on page 56.
- 4 To delete a plugin from the list, select the plugin and click **Delete**.

To configure a new or existing Resource Discovery plugin

- 1 Click **Tools** → **Resource Discovery Plugins**. The **Resource Discovery Plugins** dialog box appears.
- 2 Do one of the following:
 - To create a new plugin, click **Add**.
 - To modify an existing plugin, select a plugin from the list and click **Properties**.

The **Plugin Properties** dialog box appears, as shown in [Figure 25](#).

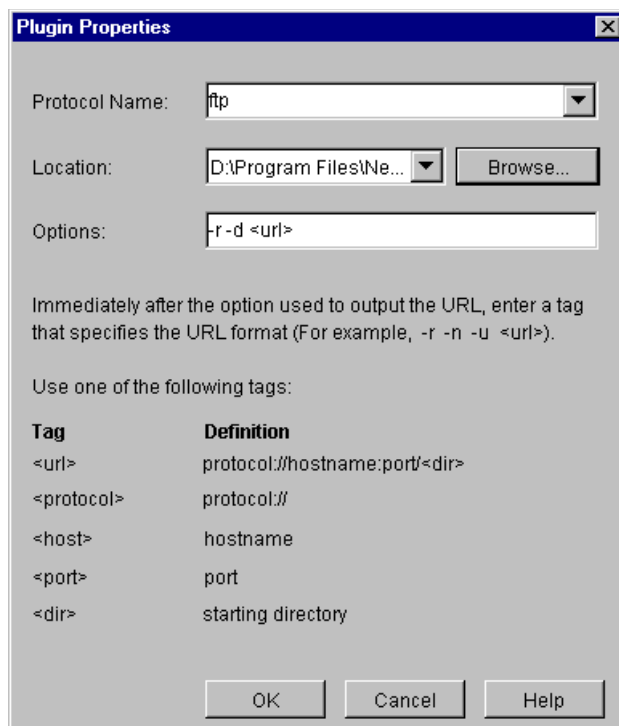


Figure 25 Plugin Properties Dialog Box

- 3 Enter the information outlined in [Table 10](#).

Table 10 Plugin Properties

Field Name	Description
Protocol Name	Select the protocol used by the plugin. <i>Note:</i> This list contains the protocols you added through the Network Resource Services list.
Location	Click Browse . Use the Open dialog box to find and select the plugin.
Options	<ul style="list-style-type: none">Enter the command-line arguments that configure how the plugin collects resource data. For example, in some programs <code>-r</code> tells the plugin to advance recursively. <i>Note:</i> Arguments are program-specific and vary from plugin to plugin. For details on specific plugin options, consult the creators of the plugin you are using. <ul style="list-style-type: none">Immediately after the argument used to run the program, enter the tag that specifies the URL format the plugin passes. For details on the available tags, see To create a global Resource Discovery plugins list on page 55.

- 4 Click **OK**. Once Policy Builder adds it to the global list of available Resource Discovery plugins, you can run it from the Resources Tree. For details, see [Running a Network Resource Plugin](#) on page 58.

Sample scenario: [Resource Discovery with FTP plugin](#)

For example, to run a resource discovery against your FTP plugin using the options shown in [Figure 26](#).

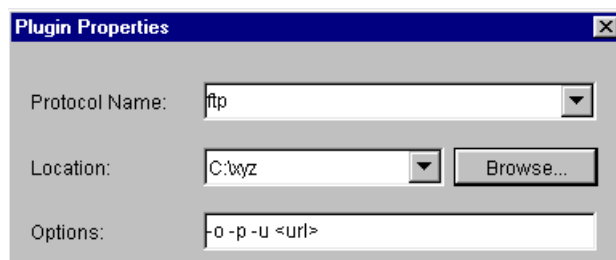


Figure 26 Plugin Properties Dialog Box

In this example, the `-u <url>` options are used to generate the resource URLs:

- The `xyz` plugin uses the `-u` argument to output the URL.
- The `<url>` tag defines the format of the URL output, which is `<protocol>://<hostname>:<port>/<dir>`.

This tag tells the plugin to substitute these parameter options with real data when it discovers the resources on the network. By formatting the output correctly with tags, you guarantee resources are listed correctly in the Resources Tree.



When you select a plugin to be used in network discovery (in the **Discover Network Resources** dialog box), the plugin and its corresponding command-line arguments are dynamically displayed in the **Plugin Settings** box. These arguments vary from plugin to plugin. Running network discovery is described in the next section, [Running a Network Resource Plugin](#).

Running a Network Resource Plugin

You can run a Network Resource plugin on a resource service to discover all available resources and add them to the Resources Tree.



A Java error sometimes occurs in the Policy Builder after running Network Discovery, which results in the Resources Tree not being properly refreshed. Clicking **Refresh** on the **View** menu will cause the correct information to appear under the Resources Tree.

Before you run resource discovery

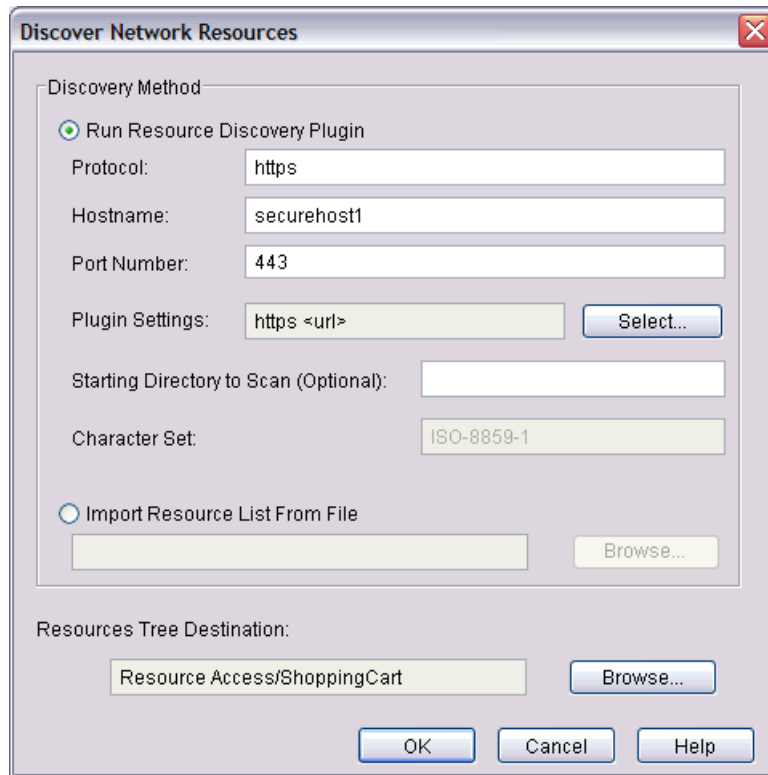
Resource discovery is a tool that allows you to populate web resources into the Policy Builder. Before you run resource discovery, the following conditions must be met in order for it to work:

- No enforcer plugin is installed on the web server or the policy is set to **ALLOW** all, to allow unknown users. Resource discovery cannot scan the web server for resources if the Enforcer plugin is protecting the resources.
- The web server must be configured to allow index pages to be shown. For example, when you go to a URL that doesn't have a default `index.html`, it should show all of the resources (`http://test.can.hp.com/test` should list all of the pages in the test directory if index pages are configured).

If index pages aren't configured, the Resource Discovery plugin can only follow the links on the URL you provide. For example, if `http://test.can.hp.com/index.html` is a main page with links to other pages on the same server, the plugin will recursively follow all of the links on the main page and all the links on link pages, etc. If the main page is just a page that says "hello" with no links, the Resource Discovery plugin will end at the main page.

To run a discovery plugin for network resources

- 1 Make sure you have configured the Network Resource plugin. For details, see [To create a global Resource Discovery plugins list](#) on page 55.
- 2 On the Resources Tree, right-click the resource service you want to scan for available resources.
- 3 Click **Run Discovery** → **Resources**. The **Discover Network Resources** dialog box appears, as shown in [Figure 27](#).



The dialog box is titled "Discover Network Resources" and contains the following fields and controls:

- Discovery Method:**
 - ☒ Run Resource Discovery Plugin
 - Protocol:
 - Hostname:
 - Port Number:
 - Plugin Settings:
 - Starting Directory to Scan (Optional):
 - Character Set:
 - ☐ Import Resource List From File
 -
 -
- Resources Tree Destination:**
 -
- Buttons:

Figure 27 Discover Network Resources Dialog Box

- Information about the resource service’s representative server is entered automatically in the **Protocol**, **Hostname**, and **Port Number** fields. Policy Builder takes this information from the service’s properties.
 - If you have configured a plugin for the resource service’s protocol, the plugin’s configuration details are entered automatically in the **Plugin Settings** field.
- 4 Select **Run Resource Discovery Plugin** and enter the information described in [Table 11](#).

Table 11 Discover Network Resources Properties

Property Name	Description
Protocol	Enter the protocol name the resource service uses.
Hostname	Enter the hostname of the resource service you want to scan (for example, <code>www.mycompany.com</code> , <code>ftp.mycompany.com</code>).
Port Number	Optional. Enter the port number the resource service is running on.

Table 11 Discover Network Resources Properties (cont'd)

Property Name	Description
Plugin Settings	To select a plugin, do the following: <ol style="list-style-type: none">1 Click Select. The Configure Resource Discovery Plugins dialog box appears.2 Select the protocol that matches the protocol you entered in the Protocol field.3 Click OK. <p>Note: If necessary, you can click Properties and modify the plugin options. You can also click Add and configure a new plugin.</p>
Starting Directory to Scan	Optional. Enter the starting directory to scan. For example, if you want to begin scanning at <code>www.mycompany.com/sales</code> , enter <code>sales</code> . If you leave this field blank, the scan begins at the resource's root directory.
Character Set	Non-configurable. Reads the name of the character set you configured when you registered the service to which future discovered resources belong. For details, see To create a new network service .

- 5 Select the location on the Resources Tree to add the resources. There are two methods of doing so.

First method:

- Click **Browse** beside the **Network Resources Tree Destination** field. The **Select Resource Destination** dialog box appears.
 - Select the resource location and click **OK**.
- When browsing to resource discovery destinations, only folders are rendered on the Resources Tree. Other Resources Tree entries do not appear.

Second method:

- Select a folder or the root of the Resources Tree.
- Click **New** and create a new resource service.
- Select it in the **Select Resource Destination** dialog box and then click **OK**.

- 6 Click **OK**.

➤ You can cancel resource discovery once it starts. For details, see [Terminating a Network Discovery](#) on page 63.

- 7 Click **Refresh** → **View** to ensure discovery results are correctly displayed.

Importing a Resource List

You can add resources to the Resources Tree by importing a text file containing a list of resources. The file must contain resources for one type of protocol only. For example, the file can contain HTTP, HTTPS resources, or FTP resources.

Resource list requirements

You must identify each resource in the text file by its URL, and the file must contain one URL per line. You can use any tool to generate the text file. Before importing the file, remove any lines that are not resource URLs.

Your URL must be of valid format; otherwise, it will be ignored. Properly formatted URLs use the following syntax:

```
<protocol>://<domain_name>:<port>/<dir>
```

where *port* and *dir* are optional URL components.

For example, if you are importing resources for an FTP service, the text file might contain URLs such as:

```
ftp://ftp.mycompany.com/header/images/logo.gif
```

```
ftp://ftp.mycompany.com/header/images/products.gif
```

These URLs are added to the Resources Tree under the service you select, as shown in [Figure 28](#).

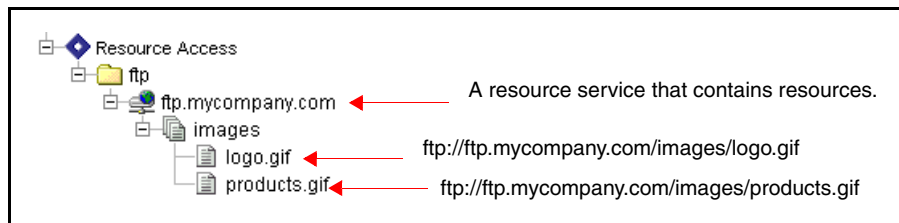


Figure 28 Resources Tree Description

To import resource URLs

- 1 On the Resources Tree, right-click the resource service to which you want to add the resources.
- 2 Click **Run Discovery** → **Resources**. The **Discover Network Resources** dialog box appears, as shown in [Figure 29](#).

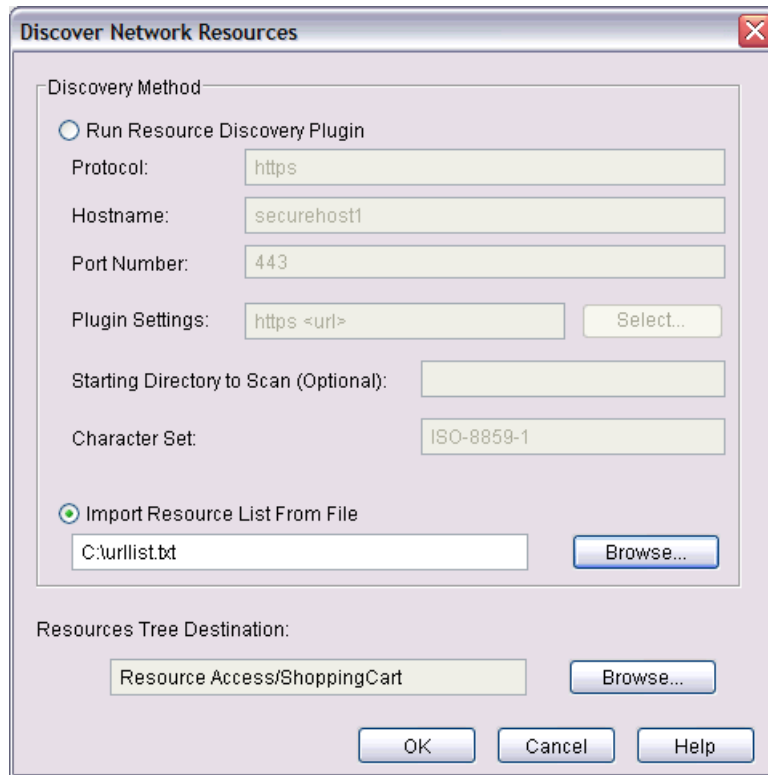


Figure 29 Discover Network Resources Dialog Box

- 3 Select **Import Resource List From File**.
- 4 Click **Browse** and locate the file.
- 5 Select the location on the Resources Tree to add the resources. Do the following:
 - Click **Browse** beside the **Network Resources Tree Destination** field. The **Select Resource Destination** dialog box appears.
 - Create or select a resource service. To create a resource service, select a folder or the root of the Resources Tree and then click **New**. To select a newly created or existing service, choose it in the **Select Resource Destination** dialog box and click **OK**.
- 6 Click **OK**. The icon at the bottom of the Policy Builder window flashes to indicate that the resource list is being imported successfully.



When browsing to resource discovery destinations, only folders are rendered on the Resources Tree. Other Resources Tree entries do not appear.

Deleting a Resource

When you delete a resource, the entry is permanently deleted from the Resources Tree and from the directory server that acts as the Policy Store.

To delete a resource

- 1 On the Resources Tree, right-click a resource entry and click **Delete**. A confirmation dialog box appears.
- 2 Click **Yes**. The resource is deleted from that resource service branch.

Terminating a Network Discovery

Network discoveries are time-intensive scans of your resource services or resources. Because these discoveries can be lengthy and use a great deal of network overhead, you may occasionally need to terminate a discovery. You can stop service and resource discoveries at any time. To terminate this process, click **Tools** → **Terminate Network Discovery**.



Terminating a discovery makes it incomplete. Run the discovery again to ensure all services or resources are added.

4 Organizing Identities and Resources

This chapter describes the ongoing maintenance of your identities and resources, which includes organizing them into logical and/or discrete units.

By logically organizing your identities, you can:

- Locate corresponding profiles more quickly when creating the access policies for identity and resource pairs.
- Create groups and dynamic groups so they logically meet your organization's needs.
- More easily understand the steps you need to take to secure your resources fully.

Chapter Overview

This chapter includes the following topics:

- [Before You Begin](#) on page 65
- [Understanding the Differences Between Organizational Units](#) on page 66
- [Working with Identities, Groups, Dynamic Groups, and Folders](#) on page 68
- [Expanding, Searching, and Hiding a Group, Dynamic Group, or Folder](#) on page 77

Before You Begin

A clearly-architected tree structure goes a long way in minimizing the confusion that a large-scale access policy setting operation can cause. Before you begin organizing your identities and resources, think about your corporate and network structure and answer the following questions:

- Corporate-specific questions that affect the Identities Tree:
 - How do you intend to maintain this tree as the number of known identities shifts over time?
 - How will the corporate organizational tree affect decisions when organizing employees?
 - Do sales, marketing, or suppliers have any unique needs that must be met within the directory structure, to allow these business units to take advantage of Select Access' personalization feature?
- Network-specific questions that affect the Resources Tree:
 - How closely does the Resources Tree need to mirror the network topology?

- How do you intend to maintain this tree as the number of known resources shifts over time?

Understanding the Differences Between Organizational Units

Three organizational units can be used to categorize your identities or resources. Organizational units enable you to define different administrative units while, in some cases, keeping a central instance of the entry itself intact. How you intend to manage and delegate access for the identity and resource entries largely determines the architecture of these entries.

Table 12 Organizational Units Overview

Organizational Unit	Details
Groups: Use this organizational unit to categorize identities based on a particular function. You can only use groups on the Identities Tree.	What Are Groups? on page 66
Dynamic Groups: Use this organizational unit to categorize identities based on attributes they have. You can only use dynamic groups on the Identities Tree.	What Are Dynamic Groups? on page 66
Folders: Use this organizational unit to systematically create a hierarchy of data, much as you use folders and directories on your operating system. You can use folders on both the Identities and Resources Trees.	What Are Folders? on page 67

What Are Groups?

Groups are collections of identities listed as an entry in a directory server. Members are not listed as separate identities, but are actually attributes of the group they are listed under.

For more information about identities, see [Profiles: Understanding Directory Entries and Attributes](#) in the *HP OpenView Select Access 6.2 Concepts Guide*.

For example, if you want to protect resources based on the functional teams identities belong to, you might want to put identities into groups based on these teams. In this case, some typical groups you might create include Marketing, Sales, and Production.

For more details on groups, see [Creating and Modifying a Group](#) on page 69.



Groups are intrinsic to an identity location. This means that identities must be in the same identity location for which the group has been created. If you are unsure of the implication of this outcome, consider adding mirror groups across all of your identity locations.

What Are Dynamic Groups?

Dynamic Groups are dynamic collections of identities whose membership is based on a shared set of attributes configured in the identity entry. As a result, a dynamic group can constantly change at any given time as identities are added and removed automatically as their attributes change.

For more information about identities, see [Profiles: Understanding Directory Entries and Attributes](#) in the *HP OpenView Select Access 6.2 Concepts Guide*.

For example, a department store wants to display customized resources to different identities depending on how much a customer spends per year. In this case, some typical dynamic groups you might include are Bronze Customer, Silver Customer, Gold Customer and Platinum Customer. As spending habits change, identities automatically shift into and out of these dynamic groups.

For more details on dynamic groups, see [To create or modify a dynamic group](#) on page 73.



Dynamic Groups are intrinsic to an identity location. This means that identities must be in the same identity location for which the dynamic group has been created. If you are unsure of the implication of this outcome, consider adding mirror dynamic groups across all of your identity locations.

What Are Folders?

Folders are organizational units for categorizing actual identity profiles (as well as groups and dynamic groups) and network resources. Folders can appear in any of these Tree locations:

- On an identity location branch
- Under the network root
- Under a service branch
- Nested in another folder

Identity scenario

For example, if a company's regional head offices each have a directory server with identities not just for the head office, but for all satellite offices in the region, consider using folders to classify these identities further under the top-level identity data branch that appears on the Identities Tree. In this case, if you have a Canadian regional office, you might create folders for Waterloo, Toronto, Vancouver, and Montreal satellite offices.



When organizing identities by folder, make considered, intelligent choices; Policy Builder currently does not allow you to move identities from one folder to another.

Resource scenario

Additionally, you might organize content on a particular service by types of files. For example, if your service is a web server, you might create folders such as Images, HTML, MPEGs, Documents, and so on. This categorization allows you to quickly determine which resources need protecting.

For more details on folders, see [To create or modify a folder to categorize your identities](#) on page 76 and [Profiles: Understanding Directory Entries and Attributes](#) in the *HP OpenView Select Access 6.2 Concepts Guide*.

Working with Identities, Groups, Dynamic Groups, and Folders

Before you can create identities, groups, dynamic groups and folders in Policy Builder, you need to understand how information is stored in the directory server. Directory server entries are organized in a conceptual hierarchical structure called the Directory Tree. Directory entries appear in the tree as attribute-value pairs, as shown in [Figure 30](#).

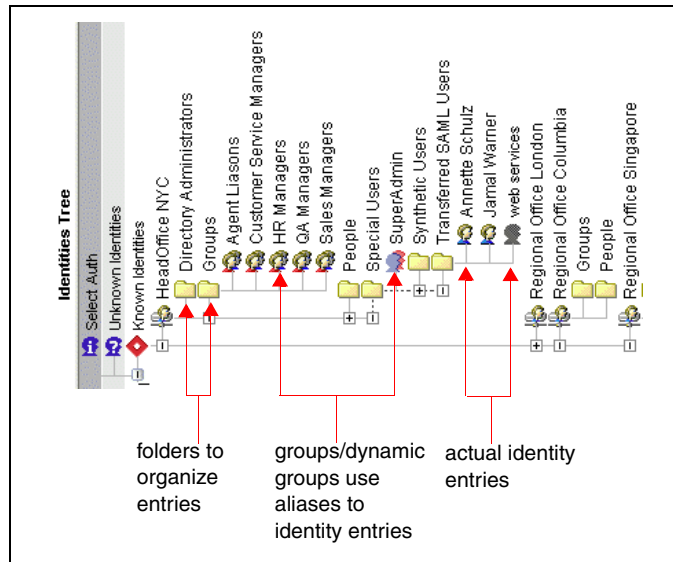


Figure 30 Identities Tree Description

In the directory server, you can create identity, group, and dynamic group entries in a folder as shown in [Figure 30](#). A folder is a special type of entry (often called an organizational unit) used to store other directory entries. When you use the Policy Builder to create a new identity, group or dynamic group, first select (or create) the folder where you want to create the directory entry.

Notice that when an identity is a member of a group or dynamic group, the identity is shown in two different locations in the tree:

- The *actual* identity entry appears under the folder where the entry is stored in the directory server.
- An *alias* to the identity entry also appears under any groups or dynamic groups the identity belongs to. The alias is only a pointer (or shortcut) to the actual identity entry.

Understanding How to Organize Entries

Before creating identities, groups, and dynamic groups, decide how you want to organize these entries on the Identities Tree.

- **Use folders to store your identities and resources, groups, and dynamic groups:** When you create a new identity, group or dynamic group, select the location on the tree where you want to store the identity, group, or dynamic group. We highly recommend using folders so you can take advantage of the Policy Builder's scalability. When you add a new identity, group, or dynamic group to a folder, it automatically inherits the folder's access policies.

► You cannot move identities between folders.

- **Use groups and dynamic groups to categorize your identities:** You can use groups and dynamic groups to organize your identities in very specific categories. Groups allow you to easily change which group the identity belongs to. Dynamic Groups differ from groups in that membership to them is dynamic. Use dynamic groups when you do not need to have manual control over who gets added or removed from them.

For more information about identities, see [Profiles: Understanding Directory Entries and Attributes](#) in the *HP OpenView Select Access 6.2 Concepts Guide*.

For example, create groups for the different divisions in your company (Sales, Marketing, Development), and assign your employees to these groups. Conversely, you can create a dynamic group for customers who speak German rather than English.

- When working with identities, groups, dynamic groups and folders, information is being written to and deleted from the directory server. Before you delete any of these entries, be sure you want the record permanently destroyed.
- For information on how to set up authentication services for group and dynamic group authentication, see [Avoiding Incorrect Service Setup for Groups and Dynamic Groups](#) on page 127.
- Groups and dynamic groups are intrinsic to an identity location. This means that identities must be in the same user location for which the group or dynamic group has been created. If you are unsure of the implication of this outcome, consider adding mirror groups or dynamic groups across all of your user locations.



Because OpenLDAP 2.2.27 does not support wildcard LDAP filtering very well, if you define a dynamic group using a wildcard condition, OpenLDAP may not return the expected group members.

Creating and Modifying a Group

Groups must be created before identities can be assigned to them as members. Groups can contain identities or even other groups or dynamic groups.



Groups cannot span multiple identity locations. You must create groups in the same identity location as the members' identity profiles.



Active Directory does not allow you to nest groups. This is because the group type is a container for identities only. It will not allow you to add other groups of the same native type.

For example, if you create a group called “User Experience” you can assign Technical Writing, Training, and Technical Support groups to it as well as individual identity profiles like the Director of R&D and the VP of Customer Care.

To create or modify a group

- 1 Do one of the following:
 - Right-click a folder or identity location branch in the Identities Tree, then click **New → Group**.
 - Right-click an existing group, then click **Properties**.

The corresponding **New Group** or **Group Properties** dialog box appears.

New Group

Group Information | Group Membership | Directory Information

Enter information about the group.
Note: On the Directory Information tab you can select which field is used as the group's directory entry name.

*Group Name: Marketing

Description: Marketing division employees

* You must enter information in these fields.

Advanced OK Cancel Help

Figure 31 New Group Dialog Box

- 2 Enter values for the following fields of the **Group Information** tab:
 - **Group Name:** Enter the group's name. This is the group's entry name (or RDN) and it appears on the Identities Tree.
 - **Description:** Optionally, enter a description of the group.
- 3 Click **OK** to commit these changes to the directory server for that identity location.

Assigning Group Membership

Groups can contain identities and other groups. All members of a group inherit the access policies created for the group, but you can override the access policy for a specific group member if necessary. A summary of how to assign members to a group is listed in Table 13.

Table 13 Group Assignment Options

Option	Details
Assign an identity to a group by changing an identity's group membership.	To change an identity's group membership on page 71
Assign an identity or a group to a group by changing a group's members.	To change a group's members on page 71

To change an identity's group membership

- 1 On the Identities Tree, right-click an identity and then click **Group Membership**. The **Group Membership** tab appears.

The **Group Membership** tab contains the following lists:

- **Available Groups:** Contains the groups to which you can assign the identity. The valid groups you can choose from are highlighted. Other directory entries (such as identities and folders, and groups in other identity locations) are disabled and appear grayed out.

➤ **Available Groups** uses the same threshold value as the Identities Tree. If you try to expand an entry that contains more entries than the threshold value, you are prompted to search for the entries you want to view.

- **Member of:** Contains the groups to which the identity currently belongs.

- 2 In the **Available Groups** list, select the group to which you want to add the identity and click **Add**. The group is added to the **Members** list.

➤ Use CTRL+CLICK or SHIFT+CLICK to select multiple identities.

- 3 You can also:

- Search for an entry in either list. Right-click an entry and click **Find**, or enter search criteria in the **Find** box below the list. For more details on searching, see [Finding a Tree Entry](#) on page 77.
- Hide an entry in a list. Select one or more entries, right-click the entries, then click **Hide**. A dotted line in a tree indicates that one or more entries are hidden. For details, see [To hide a tree entry](#) on page 82.

➤ These commands are also available from the **Edit** menu.

- 4 To remove an identity from a group, select the group in the **Member of** list and click **Remove**.
- 5 Click **OK** to commit these changes.

To change a group's members

- 1 On the Identities Tree, right-click a group and then click **Group Properties**.
- 2 Click the **Group Membership** tab, as shown in [Figure 32](#).

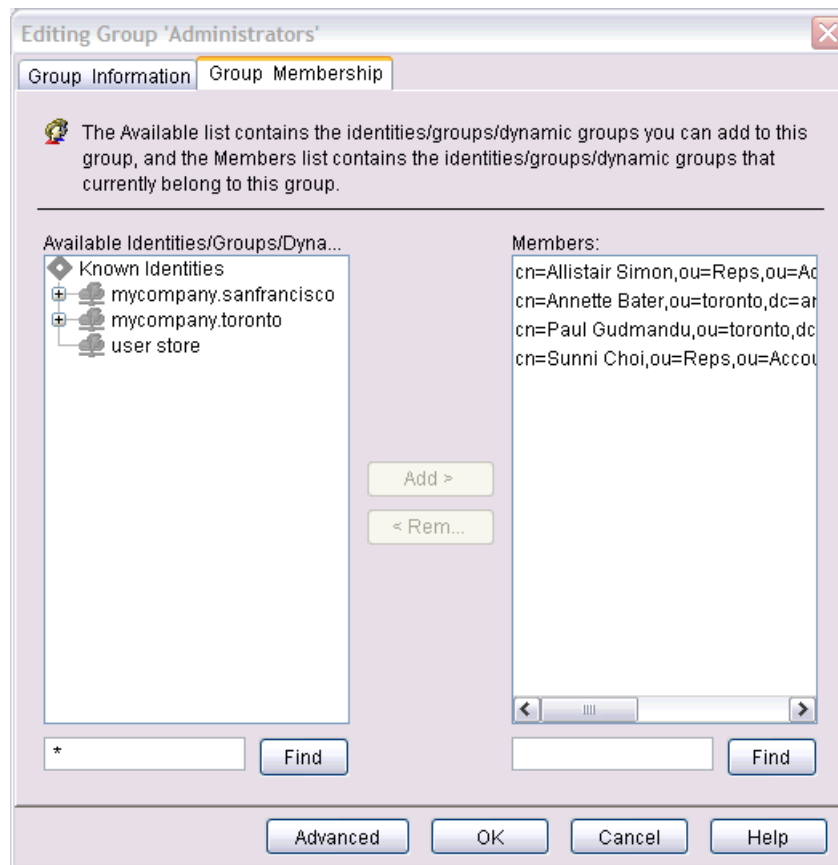


Figure 32 Editing Group Dialog Box

The **Group Membership** tab contains the following lists:

- **Members:** Contains the identities and groups that currently belong to the group.
 - **Available Identities/Groups/Dynamic Groups:** Contains the identities, groups, and dynamic groups you can assign to the group. The valid identities and groups you can choose from are highlighted.
 - The **Available Identities/Groups/Dynamic Groups** list uses the same threshold value as the Identities Tree. If you try to expand an entry that contains more entries than the threshold value, you are prompted to search for the entries you want to view.
- 3 In the **Available Identities/Groups/Dynamic Groups** list, select the entry (an identity, group, or dynamic group) you want to add as a member and click **Add**. The entry is added to the **Members** list.
- Use CTRL+CLICK or SHIFT+CLICK to select multiple identities.
- 4 You can also:
- Search for an entry in either list. Right-click an entry and click **Find**, or enter search criteria in the **Find** box below the list. For more details on searching, see [Finding a Tree Entry](#) on page 77.

- Hide an entry in a list. Select one or more entries, right-click the entries and then click **Hide**. A dotted line in the tree indicates that one or more entries are hidden.

➤ These commands are also available from the **Edit** menu.

- 5 To remove an entry from a group, select the entry in the **Members** list and click **Remove**.
- 6 Click **OK** to commit these changes.

➤ A group using the `posixGroup` object class cannot contain other groups as members. Groups created using the Policy Builder do not use this object class, but groups created with other applications may. For details on checking a group's object classes, see [To view an entry's DN and RDN](#) in the *HP OpenView Select Access 6.2 Concepts Guide*.

Creating and Modifying a Dynamic Group

Dynamic groups facilitate the way you control access to content and resources, and vary based on your business requirements. Dynamic groups can contain identities or groups; however, create a dynamic group before identities are dynamically assigned to them. Because membership is determined by identity or group attributes you define via a search expression, dynamic group assignment is automatic and gets updated dynamically. You cannot manually add an identity to a dynamic group.

When creating a dynamic group, keep the following tips in mind:

- Dynamic groups cannot span multiple identity locations. Dynamic groups must be created in the same identity location as the members' identity entries.
- The creation of a dynamic group can have an impact on Select Access' performance, depending on the cache refresh interval you have configured. The more dynamic groups you have, the larger the impact on performance if your lookups are in real-time. Gauge your decision on this trade-off.
- While all members of a dynamic group inherit the access policies created for the dynamic group, you can override the access policy for a specific dynamic group member if necessary.
- If a dynamic group has only hidden members, it will be show on the tree as if it has members but the members will not be visible.

To create or modify a dynamic group

- 1 Do one of the following:
 - Right-click a folder or identity location branch in the Identities Tree, then click **New** → **Dynamic Group**.
 - Right-click an existing dynamic group, then click **Properties**.
 - Click **Tools** → **Dynamic Groups** and either create a new dynamic group by clicking **New**, or modify an existing one by selecting it from the list.

➤ When you create a new dynamic group, in the **Select Dynamic Group Location** dialog box, select the identity location in which it will be created and click **OK**.

The corresponding **New Dynamic Group** or **Dynamic Group Properties** dialog box appears.

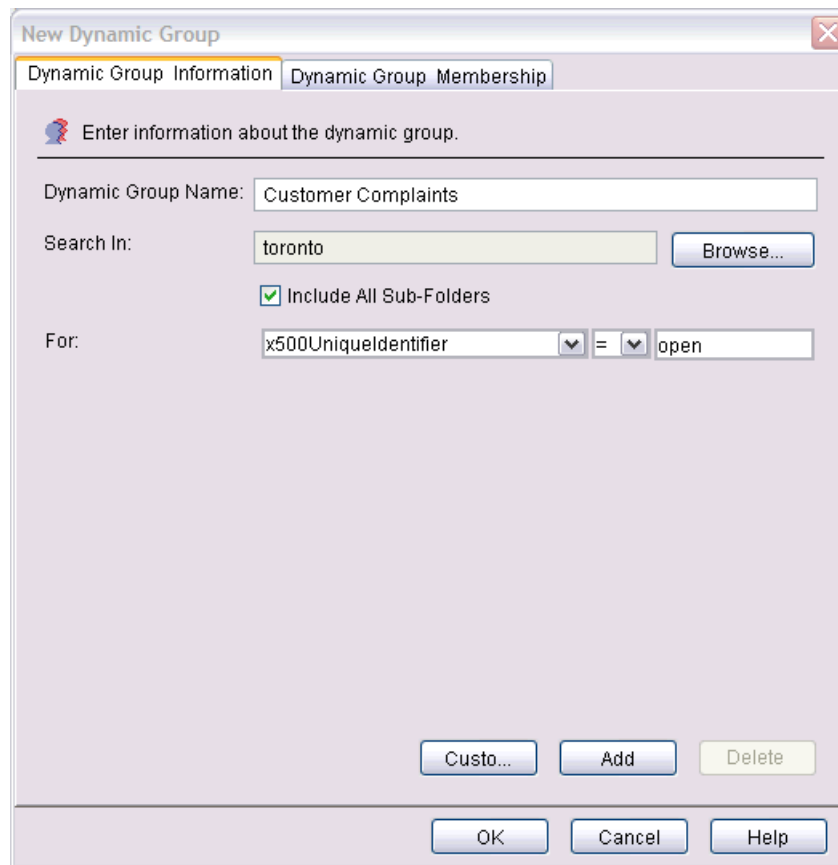


Figure 33 New Dynamic Group Dialog Box

- 2 Define the name of the dynamic group and the attributes used to determine membership in the **Dynamic Group Information** tab.
 - **Dynamic Group Name:** Enter the dynamic group's name. This is the dynamic group's entry name (or RDN) that appears in the Identities Tree.
 - Certain characters can cause unpredictable behavior by your directory server. A list of invalid characters and a list of corresponding directory servers is provided at the end of this manual. For details, see [Appendix A, Invalid Characters](#).
 - **Search In:** Specify the location from which to start the search for identities by clicking **Browse**.
 - **Include All Sub-Folders:** Specifies that you want to do a multi-level search for entries in all subfolders.
 - **For:** Defines the filter you want to use. Identities become members of a dynamic group when an entry's LDAP attributes match the value assigned in the expression.
 - For details on search expressions, see [Appendix C, Writing LDAP Expressions](#).
- 3 If you do not want to use default filter creation method described previously, click **Custom**. This toggles the view to a text window which allows you to build a custom filter. If you are writing your own filter, place the logical operator as the last node on each level of the expression you are creating.

For example, the Policy Builder cannot represent the following filter on the screen:

```
(&(|(objectclass=groupOfUniqueNames)(objectclass=group))(! (cn=*)) )
```

Instead, you must write this search expression as follows:

```
(&(! (cn=*)) (|(objectclass=groupOfUniqueNames)(objectclass=group)) )
```

- 4 Once you have finished writing your filter, you can toggle back to the default view by clicking the corresponding **Default** button. For example, using the custom search expression described above, the default filter is represented by the figure below.

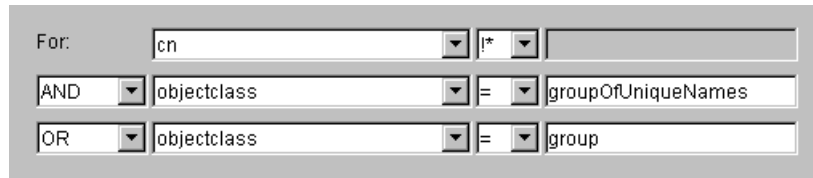


Figure 34 Custom Filter Represented as Default Filter Method

- 5 Click **OK** to commit these changes to the directory server for that identity location. The dynamic group is added to the Identities Tree and all identities who meet the attribute values you specified are automatically added as members.

To view dynamic group membership

- 1 On the Identities Tree, right-click a dynamic group and then click **Properties**. The **Editing Dynamic Group** dialog box appears.
- 2 The **Dynamic Group Membership** tab displays all identities who have met the search expression defined in the **Dynamic Group Information** tab. For details on how to modify this tab, see [To create or modify a dynamic group](#) on page 73.
- 3 To hide identities who belong to this dynamic group, select the corresponding entry and click **Hide**.
- 4 A dotted line in a tree indicates that one or more entries are hidden. To unhide identities who might belong to the group, but do not appear in the membership list click **Find**.
 - Remember, you cannot add or remove identities from a dynamic group. Membership is dynamic, based on attributes you define.
 - If you are expanding a branch or folder in order to browse for identities, you are presented with the **Quick Search** dialog box. The dialog uses the current Identities Tree expansion threshold. For details on how to use this dialog box, see [To perform a quick search](#) on page 78.
 - If a dynamic group has only hidden members, it will be show on the tree as if it has members but the members will not be visible.

Creating and Modifying a Folder

Folders are often used as an organizational unit for identities and network resources, as well as dynamic groups and groups. Unlike dynamic groups or groups that determine membership based on attributes, folders organize actual identity and resource entries.

As with dynamic groups, you can expand a folder to browse for identities. Should this folder contain a large number of identities, you are presented with the **Quick Search** dialog box. The dialog uses the current Identities Tree expansion threshold. For details on how to use this dialog box, see [To perform a quick search](#) on page 78.



If you are using folders to organize your identities, note that Active Directory servers are restricted to certain parts of the Identities Tree. By default, a folder can only be created beneath folders that have an object class of `domainDNS`, `o`, and `ou`. This rule is defined by Microsoft. For example, Active Directory uses a default folder called **Identities** to hold profile information. The `objectclass` of this folder is `container`. Therefore, you cannot create a subfolder below it without Active Directory creating an exception. However, the root entry of Active Directory is an instance of `domainDNS`. In this case, we can create a subfolder without any problem.

To create or modify a folder to categorize your identities

1 Do one of the following:

- Right-click a folder or identity location branch in the Identities Tree, then click **New** → **Folder**.
- Right-click an existing folder, then click **Properties**.

The corresponding **New Folder** or **Folder Properties** dialog box appears.

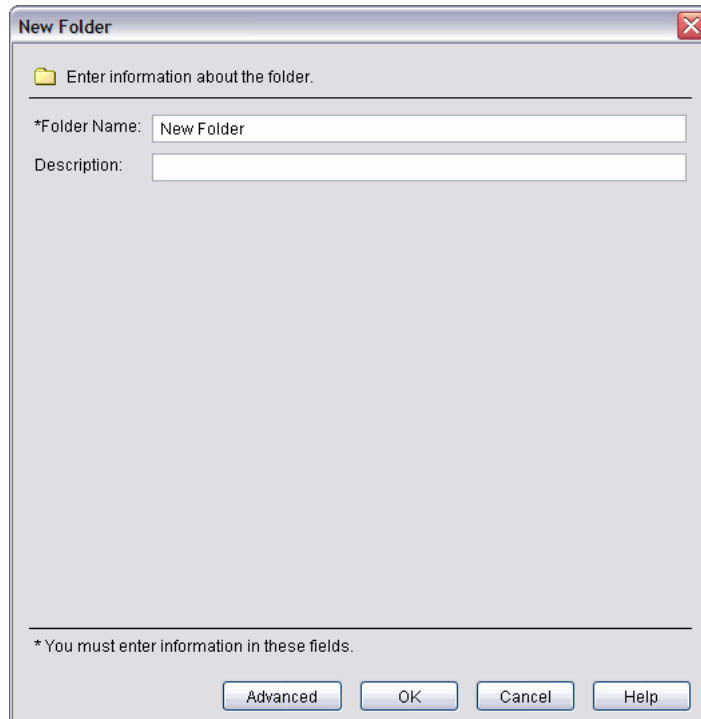


Figure 35 New Folder Dialog Box

2 Enter the following information on the **Folder Information** tab:

- **Folder Name:** Enter the folder's name. This is the folder's entry name (or RDN) and is shown on the Identities Tree.
- **Description:** Optionally, enter a description of the folder.

- 3 Click **OK** to commit these changes to the directory server for that identity location. The folder is added to the Identities Tree.

To create or modify a folder to categorize your resources

- 1 Do one of the following:
 - Right-click a service branch or folder in the Resources Tree, then click **New** → **Folder**.
 - Right-click an existing folder, then click **Properties**.

The corresponding **New Resource** or **Resource Properties** dialog box appears.

- 2 Enter the folder's name in the **Name** field. This is the folder's entry name (or RDN) and it appears on the Resources Tree.
- 3 Click **OK** to commit these changes to the directory server. The folder is added to the Resources Tree.

Deleting a Group, Dynamic Group or Folder

When you delete a group, dynamic group or folder, the entry is permanently deleted from the corresponding tree and from the directory server.



Take care when deleting folders, groups, and dynamic groups. Depending on what you delete, the result on the directory server varies: when you delete a folder, any groups, dynamic groups, identities, or resources within the folder are also deleted; when you delete a group or dynamic group, any identities that belong to the group or dynamic group are *not* deleted.

To delete a group, dynamic group, or folder

- 1 On the corresponding tree, right-click a group, dynamic group, or folder and then click **Delete**. A confirmation dialog box appears.
- 2 Click **Yes**. The group, dynamic group or folder is deleted.

Expanding, Searching, and Hiding a Group, Dynamic Group, or Folder

If you try to expand a group, dynamic group, or folder that contains more members or entries than the threshold value, you are prompted to search for the members or entries you want to view. For more details on searching, see [Finding a Tree Entry](#) on page 77.

You can also hide a member or an entry. Select one or more members or entries, then right-click and choose **Hide**. A dotted line in a tree indicates that one or more entries are hidden. For details, see [To hide a tree entry](#) on page 82.

Finding a Tree Entry

The Identities Tree and the Resources Tree can contain hundreds, thousands, or even millions of entries. Fully expanding these trees can be time-consuming, and can also make it difficult to quickly locate a specific entry.

There are two ways to find a tree entry. Depending on what kind of quick search you want to perform, you can use either of these options:

- Using the **Find** command to display the **Quick Search** dialog box. For details, see [To perform a quick search](#) on page 78.
- Double-clicking (also known as expanding) a collapsed entry. This displays the **Quick Search** dialog box. This dialog also appears when configuring:
 - Authentication services (from the Policy Builder and from the Rule Builder)
 - Groups/dynamic groups

For details, on expanding a collapsed entry, see [Expanding a Collapsed Entry](#) on page 79.

To perform a quick search

- 1 Expand a tree entry.
- 2 Right-click the entry you want to search and click **Find**. The **Quick Search** dialog box appears, as shown in [Figure 36](#).

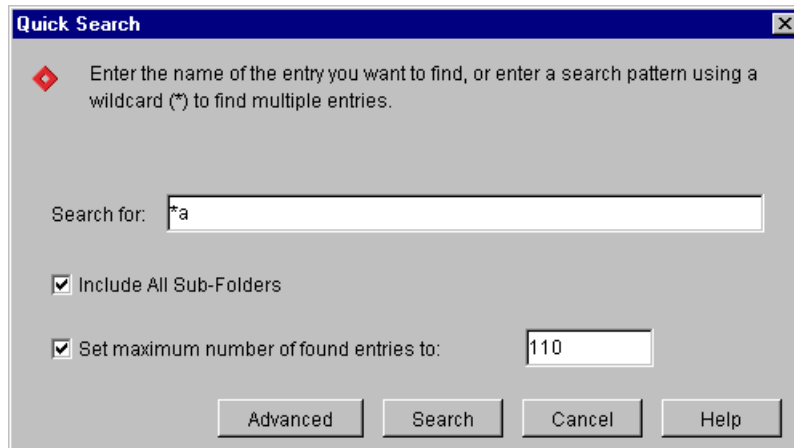


Figure 36 Quick Search Dialog Box

- 3 There are two types of entries you can make in the **Search for** box:
 - [To find an exact entry](#): Enter the name of the entry you want to find.
 - [To find multiple entries](#): Enter a search pattern by using a wildcard (*). For example, to find all names beginning with s, enter s*. To find all entries, enter *.
- 4 To do a multi-level search for entries in all subfolders, check the **Include All Sub-Folders** box.
- 5 To configure a size limit during a search operation:
 - Select the **Set maximum number of found entries to** check box.
 - Enter a value in the corresponding field. The value you enter must be greater than 0.

By default, this box is enabled and the value used is the one you configured as your threshold value. For details on how you set this value, see [To set tree thresholds](#) on page 83.
- 6 If you want to perform an advanced search, click **Advanced**. For details, see [To perform an advanced search](#) on page 80.

- 7 Click **OK** to begin your search.

➤ Hidden entries are included in search results if they fall under the size limit you specify. However, while hidden entries appear in the search results, they are not shown as members of groups or dynamic groups.

Expanding a Collapsed Entry

To help you manage trees containing a large number of entries, you can set a threshold value that determines the maximum number of entries to display when expanding a tree or a tree entry (such as a folder, dynamic group, or network service). If you try to expand an entry that contains more entries than the threshold value, you are prompted to search for the entries you want to view. For details on configuring a threshold value, see [Setting Tree Threshold Values](#) on page 83.

If the threshold value you have configured is less than the number of entries that appear on a tree entry you are double-clicking, the **Quick Search** dialog box appears because the number exceeds the threshold value. When searching, you need to increase this value.

To perform a quick search by expanding a collapsed entry

- 1 Double-click a collapsed entry. The **Quick Search** dialog box appears, as shown in [Figure 37](#).

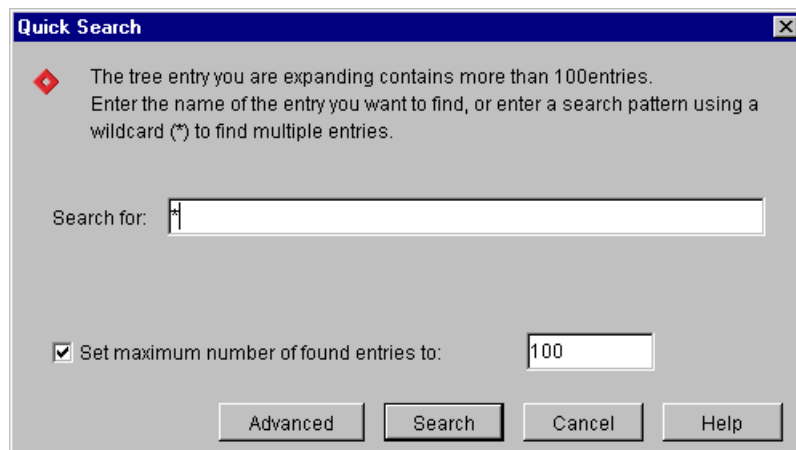


Figure 37 Quick Search Dialog Box

- 2 There are two types of entries you can make in the **Search for** box:
 - **To find an exact entry:** Enter the name of the entry you want to find.
 - **To find multiple entries:** Enter a search pattern by using a wildcard (*). For example, to find all names beginning with *s*, enter *s**. To find all entries, enter ***.

By default all subfolders beneath the parent folder are searched.

- 3 To configure a size limit during a search operation:
 - Check the **Set maximum number of found entries to:** box.
 - Enter a value in the corresponding field. The value you enter must be greater than 0.

By default, this box is enabled and the value used is the one you configured as your threshold value. For details on how you set this value, see [To set tree thresholds](#) on page 83.

- 4 If you want to perform an advanced search, click **Advanced**. For details, see [To perform an advanced search](#) on page 80.
- 5 Click **Search**. The **Search Results** dialog box appears. For details, see [Understanding Post-Search Results](#) on page 81.

To perform an advanced search

- 1 From any **Quick Search** dialog box, click **Advanced**. The **Advanced Search** dialog box appears, as shown in [Figure 38](#)

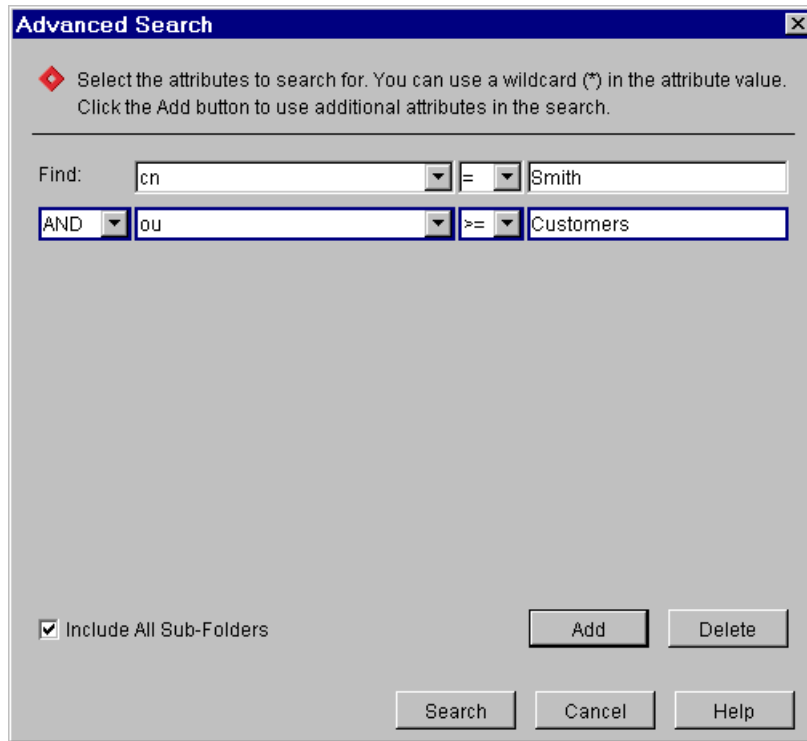


Figure 38 Advanced Search Dialog Box

- 2 Select an attribute for which to search, select an operator, and enter a search value. For details on using comparison operators, see [Appendix C, Writing LDAP Expressions](#).
- 3 On the Identities Tree, to search for entries with a `cn` (common name) that equals `Smith`, configure the **Find** field, as shown in [Figure 39](#).



Figure 39 Advanced Search Dialog Box

- 4 On the Resources Tree, to search for services with a port of `80`, configure the **Find** field, as shown in [Figure 40](#).

➤ The port number, hostname, and protocol name fields only apply to network services.



Figure 40 Advanced Search Dialog Box

- To search for additional attributes, click **Add**.
 - To remove the last attribute from the list, click **Delete**.
- 5 To search the current folder and all subfolders, select **Include all Sub-Folders**.
- The **Include All Sub-Folders** option is only available if you are searching for an item. If you are expanding a tree entry, the search only includes the entries directly beneath that entry. For example, if you try to expand the root of the Identities Tree, your search only includes entries directly beneath the tree root; it does not include any folders, groups, dynamic groups or identities within these entries.
- 6 Click **Search**.

Understanding Post-Search Results

Depending on the results of your search, there are two possible outcomes:

- **If no matching entries are found:** Click **OK** and modify your search results.
 - **If matching entries are found:** The **Search Results** dialog box appears. If entries are already displayed on the branch you are searching on, the dialog box also includes a second group box which gives you the ability to determine how to display those results, as shown in [Figure 41](#).
- Hidden entries are included in search results if they fall under the size limit you specify. However, while hidden entries appear in the search results, they are not shown as members of groups and/or dynamic groups.

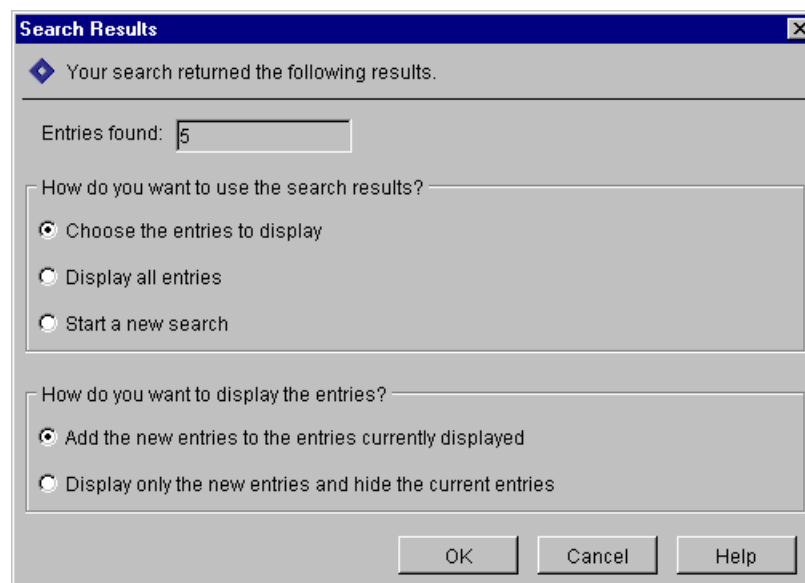


Figure 41 Search Results Dialog Box

To determine which search results to display

- 1 Choose how you want to use the search results. You can:
 - Choose the entries to display.
 - Display all entries.
 - Start a new search.
- 2 Choose how you want to display the search results. You can:
 - Add the new entries to the entries currently displayed on the tree.
 - Display only the new entries and hide the current entries on the tree.
- 3 Click **OK** to display the search results as you have configured them to appear.

If you selected **Choose the entries to display**, your search results are as shown in the **Entries Found** window.

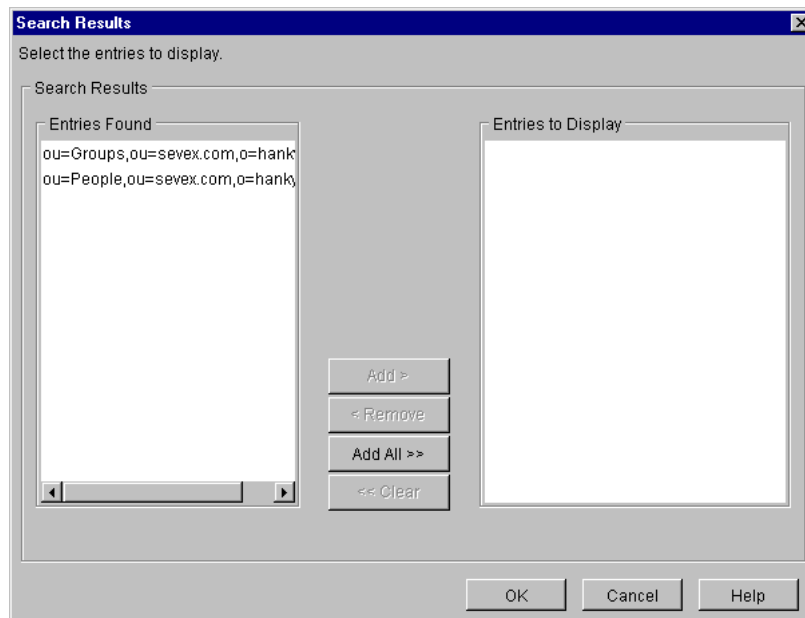


Figure 42 Search Results Dialog Box

- 4 In the **Entries Found** list, select the entries to display and click **Add**. The entries move to the **Entries to Display** list.
- 5 Do one of the following:
 - Use CTRL+CLICK or SHIFT+CLICK to select multiple entries, or click **Add All** to select all the entries.
 - Use **Remove** to remove a selected entry from the **Entries to Display** list.

To hide a tree entry

- 1 Right-click an entry and then click **Hide**.

- 2 You can display hidden entries by searching for them. For details, see [Finding a Tree Entry](#) on page 77.

► Dotted lines on the Identities Tree or Resources Tree indicate that one or more entries are hidden.

To unhide a tree entry

- 1 Double-click a collapsed entry.
- 2 If the number of collapsed entries falls within the threshold value, they reappear in the tree.

Setting Tree Threshold Values

Threshold values help you manage trees containing a large number of entries. You can set a threshold value that determines the maximum number of entries to display when expanding a tree or a tree entry (such as a folder, group, or network service). If you try to expand an entry that contains more entries than the threshold value, you are prompted to search for the entries you want to view.

► When you set the threshold value for the Administrative Access tree in the current administration session, the setting is not immediately recognized by the Policy Builder. However, if you exit and then restart the Policy Builder applet, the threshold value you set in the previous session is recognized.

To set tree thresholds

- 1 Click **File** → **Configure Client Settings**.
- 2 Select the **Tree Thresholds** tab in the **Configure Client Settings** dialog box. This dialog box allows you to enable the use of tree thresholds. Tree thresholds are the maximum number of entries to display without performing a search.
- 3 Enter the information as outlined in Table 14.

Table 14 Directory server configuration

In this field...	Do this...
Set Identities Tree Threshold Value to	Enable an Identities Tree threshold by: <ol style="list-style-type: none">1 Checking the corresponding box.2 Entering the maximum number of entries to display without a search. You must enter a value greater than 0. <p>Note: By default, a threshold is set for the Identities Tree with an initial value of 100 entries maximum.</p>
Set Resources Tree Threshold Value to	Enable a Resources Tree threshold by: <ol style="list-style-type: none">1 Checking the corresponding box.2 Entering the maximum number of entries to display without a search. You must enter a value greater than 0. <p>Note: By default, Resources Tree threshold values are disabled.</p>

- 4 Click **OK**.

5 Authentication Basics: Select Auth & Personalization

This chapter introduces you to the fundamentals of authentication and personalization. Authentication is the process by which an unknown user is identified as a known user. Once the identity is known to the Select Access system, content can be personalized for a given user.

Chapter Overview

This chapter includes the following topics:

- [Authentication Criteria](#) on page 85
- [Elements of Select Access Authentication](#) on page 86
- [Using Select Auth to Authenticate Identities](#) on page 87
- [Enabling Personalization](#) on page 92

Authentication Criteria

To become a known and authenticated user means that the identity must:

- [Have an identity entry on the directory server](#): Without an identity entry, the Select Access system cannot know who the person is. The identity entry describes the identity through a set of user attributes, which you can use to personalize content for that user.

For details on how to set up personalization on Select Access, see [When to Enable Personalization](#). For details on how to integrate Select Access personalization with your web server's personalization capabilities, see [Chapter 6, Implementing Select Access Personalization With Your Web Server](#), in the *HP OpenView Select Access 6.2 Network Integration Guide*.

- [Provide credentials that match those in the corresponding user entry](#): Without the correct set of credentials the Select Access cannot confirm that the identity is who s/he claims to be. For details on understanding the elements of Select Access authentication, see [Elements of Select Access Authentication](#) below.

Once authenticated, the identity can access generic or personalized content according to the access policies you set and the attributes that exist in the identity's entry on the directory server.



Good practice dictates that user access ultimately be determined by an access policy, not an authentication service. Setting the proper access policy is the only way to guarantee consistent access behavior. For details, on setting policy, see [Chapter 7, Controlling Network Access](#).

Elements of Select Access Authentication

Authentication is determined by two key elements:

- **An authentication service:** Is used by Select Access to perform the authentication. There are two elements:
 - The authentication service that deploys the authentication method technology (described in the subsequent bullet).
 - The authentication plugin that acts as the Select Access agent on the authentication service.

When you enable Select Auth, you must choose one or more authentication service(s) that Select Auth deploys to validate an identity's credentials. For details, see [Using Select Auth to Authenticate Identities](#).

➤ Authentication services are also used by other features of Select Access that require an authentication function. These other features include the authentication decision point used within a conditional access rule and Delegated Administration.

- **An authentication method:** Is a mechanism deployed by the service to evaluate that user's claim. Some methods require that Enforcer-protected web servers collect data from identities that request access to your network resources with support forms shipped with Select Access. For details on these support forms, see [Setting Up Authentication Forms Used by Authentication Services](#) on page 128.

The authentication methods supported by authentication services include those listed in [Table 15](#).

Table 15 Service-Specific Authentication Methods

This Authentication Service...	Uses this Authentication Method...
NTLM	Windows NTLM
Registration	defined set of user attributes
Integrated Windows	desktop userID and password
SecurID	tokens
RADIUS	secrets
Certificate	PKI
Kerberos	Windows Kerberos
Password	user ID and password

Using Select Auth to Authenticate Identities

Select Auth is Select Access' native authentication feature, which is represented as a column in the Policy Matrix. It allows you to pick the authentication services used to authenticate any unknown identities who try to access each of your network resources. The Policy Validator uses the information gathered by the authentication service's plugin to identify the identity.

The Select Auth column allows you to quickly select a Select Auth policy for each entry in the Resources Tree. Once you enable Select Auth for a network resource, Select Access uses Select Auth to identify any user accessing that resource via a specific authentication service:

- **If an identity is authenticated:** He becomes a *known user*. The Policy Validator then checks the corresponding access policy for the identity and resource to determine the identity's access to the requested resource.
- **If an identity is not authenticated:** He remains an *unknown user*. Policy Validator uses the access policy for unknown identities and the resource to determine the identity's access to the requested resource.

➤ If personalization is an important feature of your site, you can encourage unknown identities to become known identities. Unknown identities become known by registering with the company via a registration service that has been set up with Select Auth. By registering, the identity submits user information to the Select Access system. Select Access then uses this information to create an identity entry from it. For details on how to configure a registration service, see [Registration Authentication Service](#) on page 107.

When an Identity Cannot be Authenticated by Policy Validator

Policy Validator is not able to identify an identity if:

- Select Auth is disabled.
- The identity does not exist in the Identities Tree and the identity has not registered.
- There is insufficient information to validate the identity.

As an alternative, create an authorization rule that contains an authentication decision point, and assign this rule to a resource you want to protect. This authentication decision point helps to validate the identity much in the same way as an authentication service does. Once identified, Policy Validator uses the authorization rule for the identity and resource pair, to determine the identity's access for that resource.

➤ For details on creating an authorization rule, see [Chapter 7, Controlling Network Access](#). For details on creating a rule, see [Chapter 9, Creating Conditional Access Rules with the Rule Builder](#).

About the Select Auth Column

The Select Auth policies you have chosen for each entry on the Resources Tree are shown in the Select Auth column, as shown in [Figure 43](#). The icons represent these policies and indicate whether Select Auth is enabled or disabled for each entry in the Resources Tree. Select Auth policies are inherited down the Resources Tree, unless you set an explicit policy that overrides it. Different policies are represented by different Select Auth icons.

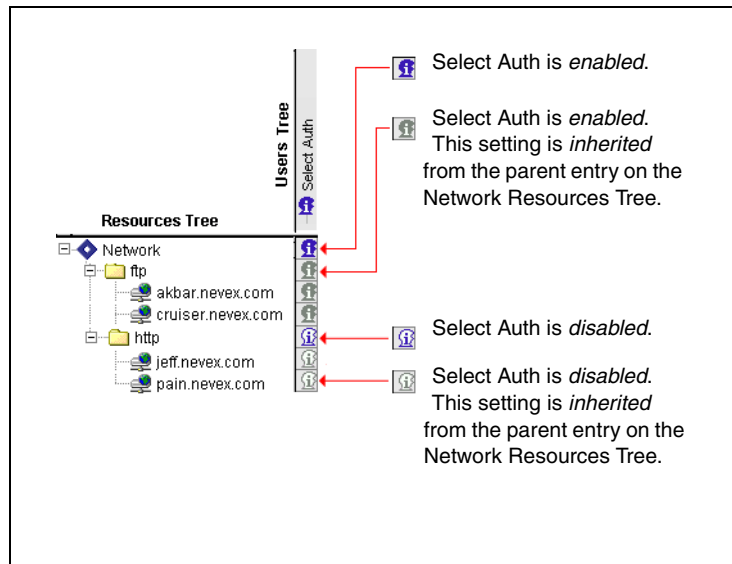


Figure 43 Select Auth Icon Descriptions

Setting a Select Auth Policy

You can select the Select Auth policy used for each entry on the Resources Tree, including the root and each folder, service, and resource.

To set a Select Auth policy

- 1 Right-click the **Select Auth** column beside an entry in the Resources Tree.
- 2 Select the **Select Auth** policy for the entry, as outlined in [Table 16](#).

Table 16 Select Auth Functions

Select Auth Function	Description	Details
Disable Select Auth	Do not try to identify the identity. Treat anyone attempting to access the entry as an unknown user.	To disable Select Auth on page 89
Enable Select Auth	Use one or more authentication services to identify the person attempting to access the entry.	To enable Select Auth on page 89
Inherit Select Auth	Inherit the Select Auth policy that the parent entry uses on the Resources Tree.	To inherit Select Auth on page 90
Select Auth Properties	Change the authentication services used.	To change Select Auth properties on page 91

To disable Select Auth

To disable Select Auth, right-click the square in the **Select Auth** column beside the entry, then click **Disable Select Auth**.



If you disable Select Auth for an entry on the Resources Tree, Policy Validator automatically uses the access policies for unknown identities and does not try to identify the person accessing the entry.

To enable Select Auth

- 1 Right-click the square in the **Select Auth** column beside the entry, then click **Enable Select Auth**. The **Select Auth Properties** dialog box appears, as shown in [Figure 44](#).

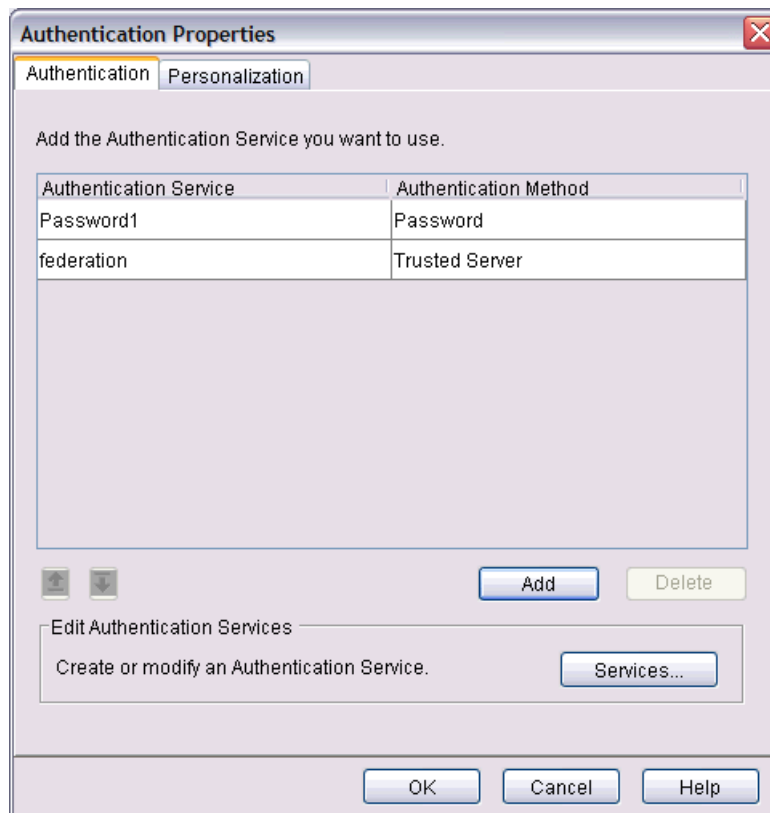


Figure 44 Authentication Properties Dialog Box

- 2 Click the **Authentication** tab. This tab allows you to determine which authentication services to use to authenticate the unauthenticated user.
 - If you have not created an authentication service, an empty screen might appear. In this case, click **Close** to display the **Authentication Properties** dialog box and then click **Services** to create a list of services. For details, see [To configure authentication services](#) on page 101.
 - If you are configuring an authentication method that requires you to browse to a folder that contains a large number of profiles that exceed the Tree threshold you have set, the **Quick Search** dialog box appears. For details, see [To perform a quick search](#) on page 78. For details on how to change the Tree threshold, see [To set tree thresholds](#) on page 83.

- 3 Click **Add**. The **Available Authentication Services** dialog box appears. For details, see [To choose from a list of available authentication services](#) on page 90.

To inherit Select Auth

Right-click the square in the Select Auth column beside the entry, then click **Inherit Select Auth**. Instead of specifically setting the Select Auth policy for an entry on the Resources Tree, this entry inherits the same policy used by the parent entry. Select Auth inheritance follows the same inheritance guidelines as authorization policy inheritance. For details, see [About Access Policy Inheritance](#) on page 133.

To choose from a list of available authentication services

- 1 Click the corresponding cell and choose **Enable Select Auth** from the menu. The **Authentication Properties** dialog box appears.
- 2 Click **Add**. The **Available Authentication Services** dialog box appears, as shown in [Figure 45](#).

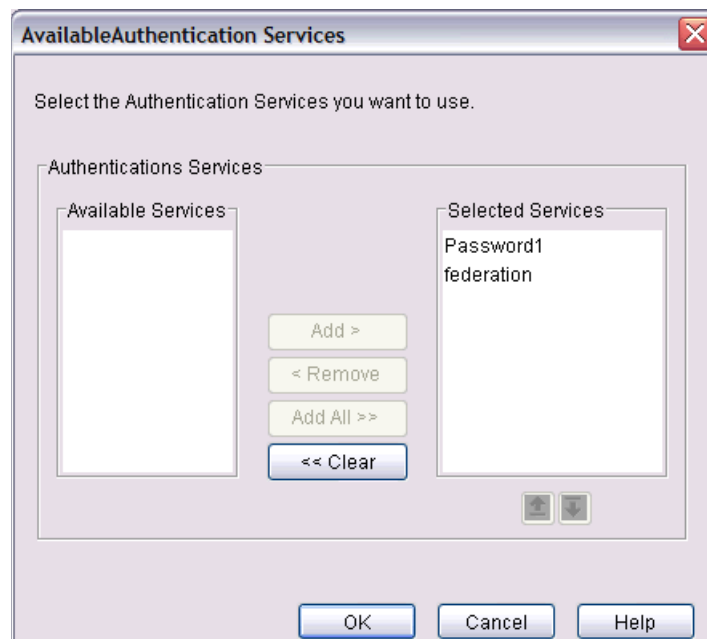


Figure 45 Available Authentication Services Dialog Box

This dialog box contains the following lists:

- The **Available Services** list contains the authentication services you have configured.
 - The **Selected Services** list contains the authentication services to be used with this decision point.
- 3 In the **Available Services** list, select the service you want to use and click **Add**. The service appears in the **Selected Services** list.

➤ Use CTRL+CLICK or SHIFT+CLICK to select multiple services.

To reorder the services, select a service in the **Selected Services** list and click either the up or down arrow. Repeat as necessary. Reordering the list of selected authentication services defines the order in which these services authenticate the identities.

- 4 To remove a service, select the service in the **Selected Services** list and click **Remove**.

- 5 Use the arrows to prioritize the services. The services are used in this order to identify an identity. (The arrows are also available on the **Authentication Properties** dialog box.)
- 6 Click **OK** to close the **Available Authentication Services** dialog box.
- 7 If you want to create or modify an authentication service, click **Services**. For details on creating an authentication service, see [To configure authentication services](#) on page 101.
- 8 Click the **Personalization** tab to export data from your directory server into the environment variables required to generate dynamic web pages. As shown in [Figure 46](#), this tab contains subtabs: **User Data**, **Group Data**, and **Dynamic Group Data**. For details on how to set up personalization, see [To enable personalization](#) on page 93.

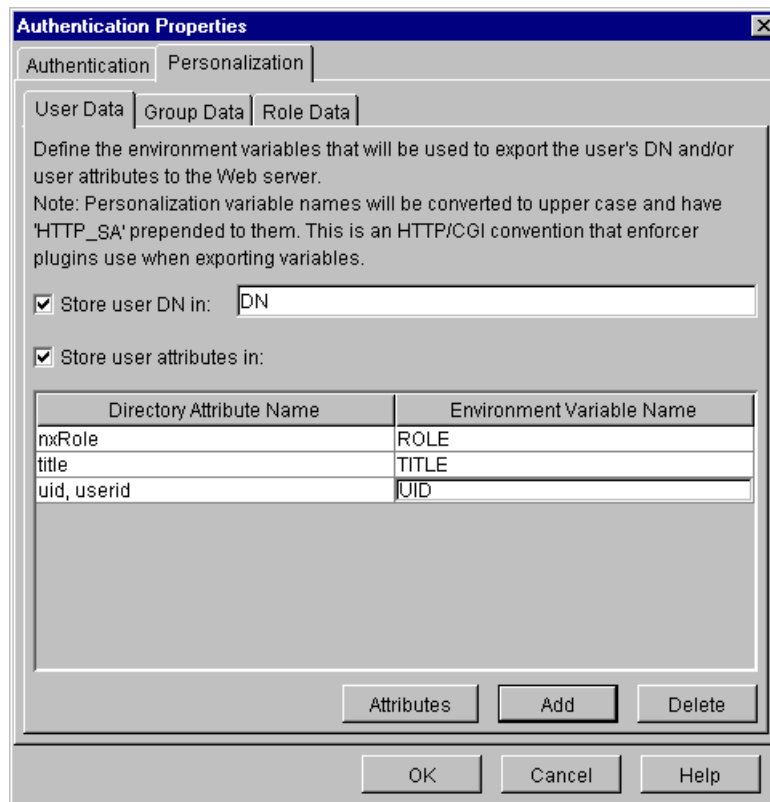


Figure 46 Authentication Properties Dialog Box

- 9 Click **OK** to close the **Select Auth Properties** dialog box and commit the changes to the Policy Store.

➤ If you want to create or modify an authentication service, click **Services**.

To change Select Auth properties

- 1 Do one of the following:
 - Double-click a square where Select Auth is enabled.
 - Right-click a square where Select Auth is enabled, then click **Select Auth Properties**.
- 2 Use the **Select Auth Properties** dialog box to select the authentication services.
- 3 Click **OK**.

Enabling Personalization

Personalization is the process of generating or modifying dynamically generated pages to customize web sites (Internet, intranet, and extranet) for identities, groups of identities, or identities belonging to a pre-defined dynamic group. With information either obtained from the directory server, or provided in real-time by a registering user, the communications between enterprise and user is altered to fit that user's stated needs as well as needs perceived by the business based on the available user information.



This section only outlines information on how to enable personalization in Select Access so that user attributes can be encoded as HTTP header variables. For information on how extract the attributes from these variables, see [Chapter 6, Implementing Select Access Personalization With Your Web Server](#) in the *HP OpenView Select Access 6.2 Concepts Guide*.

How Personalization Works

With Select Access, personalization is a function of authentication. This means that an identity must:

- [Have an identity entry on the directory server](#): Without an identity entry, the Select Access system cannot know who the person is, nor can they know what attributes they have. User attributes are obtained from the directory server. Attributes can contain:
 - Static information (like a directory UID attribute)
 - Dynamic information (like order status)

If the identity is known to an organization, the entry is typically created by a security administrator, and is populated with initial information. If the identity is unknown, the data is provided in real-time by a registering user. Once the entry is in place, the entry can be maintained by either the administrator, the identity, or third-party technologies that dynamically track and update information as needed. For details on attributes, see [About Directory Attributes](#) in the *HP OpenView Select Access 6.2 Concepts Guide*.

- [Provide credentials that match those in that entry](#): Without the correct set of credentials the Select Access cannot confirm that the identity is who s/he claims to be.

How Select Access Processes Identity Data for Personalization

The sequence of Select Access behavior is summarized by the following steps:

- 1 The Policy Builder records the attributes you activate to the Policy Store. Users only get access to personalized content when attribute values meet those defined by the administrator. For details on how to enable these personalization attributes, see [To enable personalization](#) on page 93.
- 2 The Policy Validator receives an authentication query, and downloads the personalization attributes from the Policy Store. These attributes are only included if the user has an allow policy set for the resource in question.

- 3 The Policy Validator then builds a reply to the Enforcer plugin with personalization data in XML. When the Enforcer plugin gets the reply, it exports these attributes as environment variables through HTTP headers that contain the XML data. For details, see [The Structure of a Policy Validator's Reply](#) in the *HP OpenView Select Access 6.2 Network Integration Guide*.
 - The Enforcer plugin is limited in the way it exports data. You can enhance the way you handle personalization if you write your own plugin.
- 4 The Web server then takes variables, decodes them, and displays the requisite content.

When to Enable Personalization

Because personalization is a function of authentication, you can enable personalization from one of two places in the Policy Builder:

- **As part of Select Auth:** If you want to forward user attributes at the earliest point in which the Policy Validator knows who a given user is, configure personalization here.
- **As part of an Authentication decision point:** If you want to redefine personalization for an identity depending on the resource they request, configure personalization here. For details on the Authentication decision point, see [The Authentication Properties Decision Point](#) on page 173.
 - If an identity inherits multiple rules with an authentication decision point in each, the last authentication decision point determines which HTTP headers and their corresponding set of attributes are used.
 - You also see the personalization tab when you configure Delegated Administration properties. However, personalization has no effect on this feature. You do not need to configure this tab.

To enable personalization

- 1 Display the **Authentication Properties** dialog box, and click the **Personalization** tab.

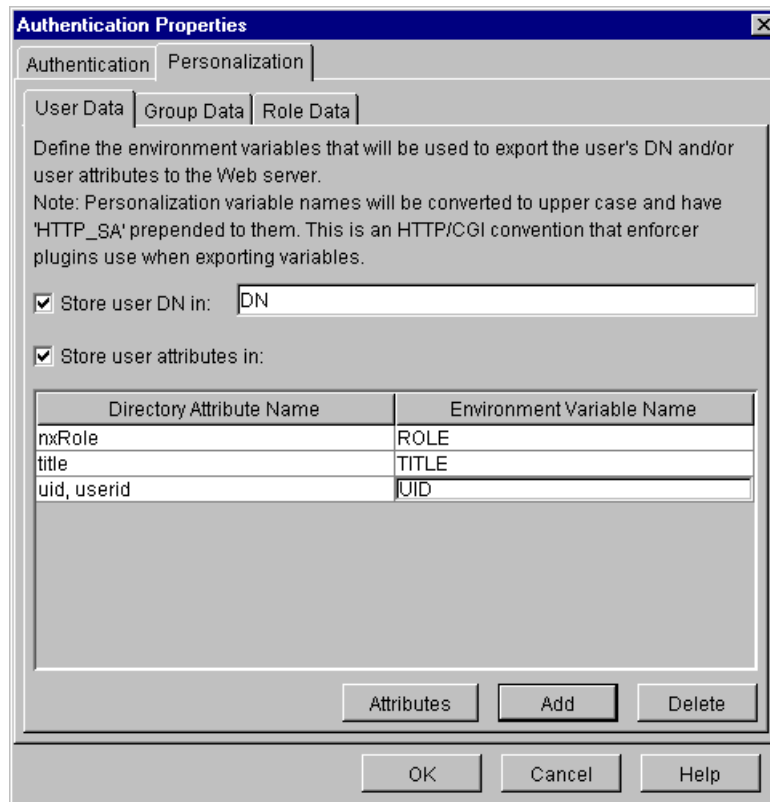


Figure 47 Personalization Tab

This tab contains subtabs that export data from your directory server into the environment variables required to generate dynamic web pages:

- **User Data:** Allows you to set up attribute and environment variables for identities.
- **Group Data:** Allows you to set up attribute and environment variables for groups.
- **Dynamic Group Data:** Allows you to set up attribute and environment variables for dynamic groups. Unlike the unlimited possibilities of exporting user and group attributes, dynamic groups are more restrictive.

► You can export any attribute for identities and groups. Attributes can include: LDAP-specific user attributes, LDAP operational attributes, as well as site-specific attributes you manually add to the identity or group entry. However, you can only export the following attributes for dynamic groups: `nxrole`, `nxsearchbasedn`, `nxsearchfilter`, and `nxsearchscope`. If dynamic groups are too limiting, use user or group attributes to personalize content only.

For details on how to determine which user or operational attributes directory servers support, see [To determine which directory-specific attributes to use for identities and groups](#) on page 95.

- 2 Click the corresponding tab and check the following boxes as necessary.
 - **Store user DN/group name/dynamic group name in:** Enable this option to export the identity's DN, group name, and dynamic group name to the environment variable that you define in the corresponding box.

If you are exporting a DN, the DN is a combination of the RDN and the parent DN. For details on DNs, see [Viewing Attributes](#) in the *HP OpenView Select Access 6.2 Concepts Guide*. The group name is the value of `cn` attribute for the group and the dynamic group name is the value of `nxRole` attribute for the dynamic group.

- **Store user/group/dynamic group attributes in:** Enable this option to export the identity's activated attributes to environment variables.
- 3 Click **Add** to create a new row. The row is appended to the bottom of the list.
 - 4 Enter all attributes that are used to determine what personalized content is viewed by the identity in the **Directory Attribute Name** column.
 - 5 For each attribute, enter the corresponding **Environment Variable Name** that it is to be exported to.
 - ▶ The Enforcer plugin exports environment variables such as HTTP headers. To that end, the Enforcer plugin prepends "HTTP_SA" to the variable's name as well as makes the variable uppercase. This modification ensures the variable is Select Access-specific, making it less likely to be forged in order to gain access to sensitive content.
 - ▶ You cannot use binary attribute values with attribute names you have activated for personalization. The only supported attributes are simple string attributes.
 - 6 Click **OK** to finish.

To determine which directory-specific attributes to use for identities and groups

- 1 Right-click an identity or group on the Identities Tree and then click **Properties**. The corresponding **Properties** dialog box appears.
- 2 Click **Advanced**. The **Advanced** attributes dialog box for that entry appears.
- 3 Click the **Attributes** tab.
- 4 Click **Add**. The **Add Attribute** dialog box appears, displaying a list of attributes you can export as environment variables. For details on how to configure this dialog, see [Creating a List of Preferred Attributes](#) in the *HP OpenView Select Access 6.2 Concepts Guide*.

6 Setting Up Authentication Services

This chapter is the counterpart to [Chapter 5, Authentication Basics: Select Auth & Personalization](#). It continues the explanation of how Select Access authenticates identities using the supported authentication services.

Chapter Overview

This chapter includes the following topics:

- [Understanding the Mechanics of Authentication Services](#) on page 97
- [Configuring Your Authentication Services](#) on page 97
- [Validating Identities When Profiles Are Not on the Directory Server](#) on page 99
- [Setting Up Your List of Authentication Services](#) on page 100
- [Avoiding Incorrect Service Setup for Groups and Dynamic Groups](#) on page 127
- [Setting Up Authentication Forms Used by Authentication Services](#) on page 128

Understanding the Mechanics of Authentication Services

Select Access supports a number of authentication services. The authentication service is not part of the Select Access system; the technology employed to authenticate user identities are typically native to a third-party authentication service. However, when you configure the authentication service, Select Access deploys the service's corresponding Policy Validator authentication plugin. The authentication plugin performs the authentication logic for the Select Access system. The plugin requires configuration and/or connection information in order to communicate with the third-party service. This configuration information resides in the Policy Store.

Configuring Your Authentication Services

There are three Select Access features that use the authentication services you configure. They are:

- [Select Auth](#): As described in [Chapter 5, Authentication Basics: Select Auth & Personalization](#), Select Auth is Select Access' native authentication feature. It uses one or more configured services to authenticate an identity.
- [The Authentication Properties decision point](#): Add this decision point to a conditional rule, if you need an alternate authentication method when:

- Select Auth is disabled.
- The credentials provided are either not secure enough for the resource requested or the ones provided were incomplete. For example, if the credentials provided were user ID and password, but the identity now requests access to a very sensitive resource, you can create and apply a conditional rule that contains an authentication decision point. This decision point could then require a SecurID token from the identity to further guarantee the identity's identity claim.

For details, see [The Authentication Properties Decision Point](#) on page 173.

- **Delegated Administration:** Like identities who request access to a protected network resource, administrators must be authenticated before they are allowed to administer changes in the Policy Matrix. For details, see [Enabling Administration Server Resources](#) on page 199.

To ensure all features have access to a list of authentication services, you must set up a global service list. Setting up this list requires that you follow the steps described in [Table 17](#).

Table 17 Configuration Overview

Configuration Task	Details
1 Create a folder and/or group if you are using an authentication service that uses a data source other than a directory server used by Select Access as its user source. This folder and/or group is used to create transient user profiles.	Validating Identities When Profiles Are Not on the Directory Server on page 99
2 Create a global list of authentication services that is used by Select Access' authentication features.	Setting Up Your List of Authentication Services on page 100
3 Ensure you use the authentication services you have configured correctly, especially for groups and dynamic groups. Otherwise, it can appear as if the Policy Validator is not evaluating them correctly.	Avoiding Incorrect Service Setup for Groups and Dynamic Groups on page 127
4 Set up your login forms used by the Enforcer plugin to collect credentials on behalf of the authentication service.	Setting Up Authentication Forms Used by Authentication Services on page 128

Validating Identities When Profiles Are Not on the Directory Server

Certificate, SecurID, RADIUS, NTLM, Kerberos, Integrated Windows, and Trusted Server authentication services do not necessarily validate identities with data in a directory server. In most cases, these services use their own database to authenticate identities requesting access to a particular network resource, as described in [Table 18](#).

Table 18 User Validation Without a Directory Server Entry

Service Type	How It Authenticates
Certificate	Checks the contents of an encrypted digital identification, called a client certificate, issued from a mutually trusted third-party organization.
SecurID	Uses a cryptographic exchange with tokens that act as passcodes. The service checks the passcode to ensure its validity. SecurID passcodes are updated every 60 seconds.
RADIUS	Uses a cryptographic exchange with a shared secret that is not sent over a network. The service checks the secret to ensure its validity.
NTLM	Uses an Windows domain NTLM authentication service on the domain controller to authenticate identities given the identity credentials received from the Enforcer plugin.
Kerberos	Uses a Windows domain Kerberos authentication service on the domain controller to authenticate identities given the identity credentials received from the Enforcer plugin.
Integrated Windows	Uses authenticated Windows credentials sent by the Enforcer plugin in a special format.
Trusted Server	Uses authenticated Windows credentials sent a trusted server. These credentials are intercepted by the Enforcer plugin and forwarded in a special format.

Why Transient Identity Profiles Are Created

While some services can maintain their own user databases, the Policy Validator can still authenticate an identity, even though there is no profile for that user in the LDAP directory server. However, subsequent attempts to reuse authentication information (for example, to load a Java application on a related Web page) then either fail, or require repeated reauthentication because authentication information changes within a short time frame (for example, SecurID).

In order to avoid these problems, Policy Validator has a mechanism for handling these special cases: it “synthesizes” user profiles to appear as if it were retrieved from the directory server. This creates a transient identity profile on the Identities Tree.

Where Transient Identities Are Stored

Transient identities are stored in the Policy Validator's cache. When the Policy Validator shuts down, the identities' data is temporarily lost; however, as identities log into the component, their data is again created.

For example, suppose you create a folder called Transient Identities on your Known Identities branch. If a RADIUS service authenticates an identity as `john_doe`, the Policy Validator manufactures a transient profile with the following information: `uid=john_doe, ou=Transient_Users, o=mycompany.com`. This information is temporarily cached as if John Doe were an actual profile on the Identities tree. As a result, if the security administrator:

- *Knows in advance* that `john_doe` is a legitimate user ID, then she can create a permanent identity profile that matches this person exactly. This profile is only checked once the identity was authenticated.
- *Does not know in advance* that `john_doe` exists, she can set an authorization rule for the entire Transient User folder. All transient user profiles that are generated by that particular authentication service then inherit the same authorization rule.



You can create different IdentitiesTree profiles for different authentication services.

Setting Up Your List of Authentication Services

Your list of authentication services displays all services you have already configured and can be used by any of the three features that require authentication (that is, Select Auth, Delegated Administration, and the authentication decision point).



If one or more administrators are adding, modifying, and deleting authentication services, you may need to refresh your Policy Builder regularly to ensure the list of current services are correct. For details, see [To refresh data](#) on page 42. If you do not refresh your data regularly, the Policy Builder prompts you to do so when needed.

Supported Authentication Services Types

Create a list of the authentication services you want to use with Select Access in the **Authentication Services** dialog box. The Policy Builder allows you to create the following types of authentication services, as described in [Table 19](#).

Table 19 Authentication Service Overview

Authentication Service	Configuration Details
Integrated Windows	Integrated Windows Authentication Service on page 103
NTLM	NTLM Authentication Service on page 105
Registration	Registration Authentication Service on page 107

Table 19 Authentication Service Overview (cont'd)

Authentication Service	Configuration Details
Trusted Server	Trusted Servers Authentication Service on page 112
RADIUS	RADIUS Authentication Service on page 114
SecurID	SecurID Authentication Service on page 117
Certificate	Certificate Authentication Service on page 120
Password	Password Authentication Service on page 124
Kerberos	Kerberos Authentication Service on page 125

➤ You can additionally create your own custom authentication plugins and upload them to the directory server. For details on creating your own authentication plugin, refer to the *HP OpenView Select Access 6.2 Developer's Tutorial Guide*.

To configure authentication services

- 1 Click **Tools** → **Authentication Services**. The **Authentication Services** dialog box appears, as shown in [Figure 48](#).

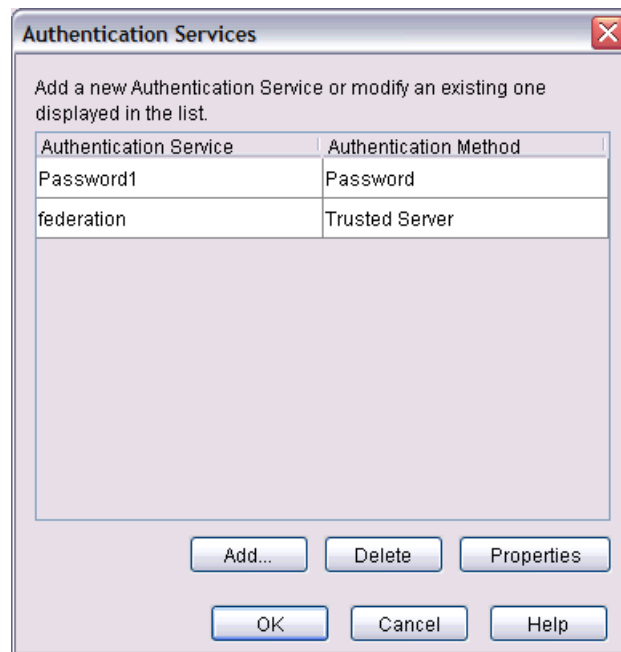


Figure 48 Authentication Services Dialog Box

- 2 To add a new authentication service and define an authentication method with that service, click **Add**. For details on defining an authentication method for the service you want to add, see [To define an authentication method for a new service](#) on page 102.
- 3 To modify an existing authentication service in your global authentication services list, select a service and click **Properties**. For details on modifying an authentication service you have already created, see:
 - [Integrated Windows Authentication Service](#) on page 103
 - [NTLM Authentication Service](#) on page 105
 - [Registration Authentication Service](#) on page 107
 - [Trusted Servers Authentication Service](#) on page 112
 - [RADIUS Authentication Service](#) on page 114
 - [SecurID Authentication Service](#) on page 117
 - [Certificate Authentication Service](#) on page 120
 - [Password Authentication Service](#) on page 124
 - [Kerberos Authentication Service](#) on page 125
- 4 To delete an authentication service from your global authentication services list, select a profile and click **Delete**.
- 5 Click **OK** to write these configuration details to the Policy Store.

To define an authentication method for a new service

- 1 Click **Tools** → **Authentication Services**.
- 2 In the **Authentication Services** dialog box, click **Add**. The **Authentication Service** dialog box appears, as shown in [Figure 49](#).

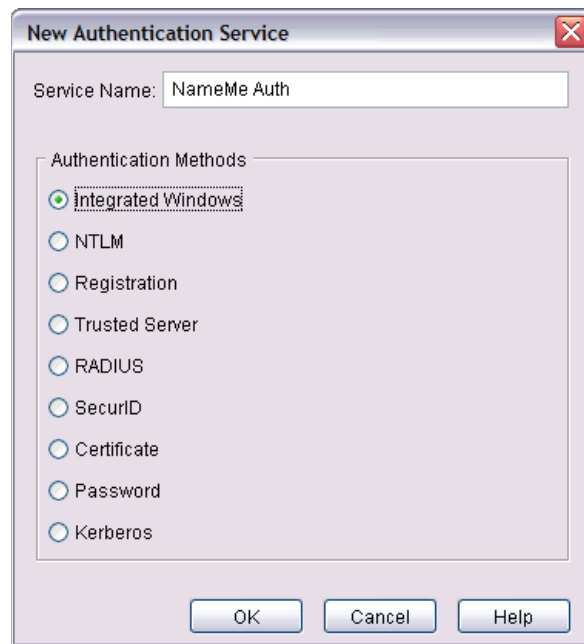


Figure 49 Authentication Service Dialog Box

- 3 In the **Service Name** box, enter a name for the service. The name must contain at least two characters.
 - Only the following alphanumeric characters can be used in a service name: A–Z, 0–9, _.
- 4 In the **Authentication Methods** group, click the service name that will be used to authenticate identities.
- 5 Click **OK** to configure the service properties for the corresponding authentication service. For details, see:
 - [Integrated Windows Authentication Service](#) on page 103
 - [NTLM Authentication Service](#) on page 105
 - [Registration Authentication Service](#) on page 107
 - [Trusted Servers Authentication Service](#) on page 112
 - [RADIUS Authentication Service](#) on page 114
 - [SecurID Authentication Service](#) on page 117
 - [Certificate Authentication Service](#) on page 120
 - [Password Authentication Service](#) on page 124
 - [Kerberos Authentication Service](#) on page 125

Integrated Windows Authentication Service

The **New Integrated Windows Service** dialog box allows you to create a service that uses the authenticated credentials sent by the Enforcer plugins in a special format. The web/application servers actually authenticate the identities internally and the Enforcer plugins extract the identity credentials from the web/application environment. The Integrated Windows service ensures credentials are received in the right format, as well as handles transient identities if necessary.

Not only does this allow Select Access to leverage the security features of the Windows operating system, but it also allows you to treat native Windows identities as Select Access identities without duplicating user data and credentials in the directory server(s) acting as your identity location.

- Integrated Windows service supports identities authenticated using NTLM or Kerberos, as does IIS web server.
- Deploying a desktop authentication solution requires that you configure both your IIS web server and Select Access to support this mechanism. As a result, both Microsoft and HP have specific requirements that you must meet to ensure that Integrated Windows authentication is successfully implemented. For details, see the table in [To use IIS's automatic logon mechanism: Integrated Windows Authentication](#) of the *HP OpenView Select Access 6.2 Network Integration Guide*.
- In addition, if IIS6 is configured for Integrated Windows Authentication (IWA), then write permission must be given to all possible identities on the NETWORK_SERVICE account. This is because IIS will impersonate the identity and serve the request under that user account. Because the IIS Enforcer plugin code is not executed until after the impersonation takes place, the identity must have write permission to the log file in order for messages to be logged there.

Sequence of integrated authentication

The sequence of desktop-based authentication events is as follows:

- 1 The end user logs onto the desktop using native logon credentials.
- 2 The end user opens an IE browser session and tries to access web content on the IIS web server.
- 3 IIS authenticates the end user's identity and locates the profile. The order of authentication mechanisms used by IIS is as follows:
 - Anonymous authentication
 - Integrated Windows authentication
 - Digest authentication (if applicable)
 - Basic/clear text authentication
- 4 The IIS Enforcer plugin collects the end user's credentials and forwards them to the Policy Validator. It uses the Integrated Windows service you configure to perform the authentication itself by "impersonating" the validated identity using the credentials that were extracted.

➤ If you follow the instructions in this section, and you continue to experience problems with desktop authentication with IIS on a Windows 2000 host, see [Integrated Windows authentication issues on IIS](#) on page 298 for further configuration details.

To configure a new or existing Integrated Windows authentication service

- 1 Click **Tools** → **Authentication Services**. The **Authentication Services** dialog box appears, displaying a list of available services.
- 2 Do one of the following in the **Authentication Services** dialog box:
 - Click **Add** to display the **Authentication Method** dialog box. Enter a service name and click the **Integrated Windows** option before clicking **OK**. This displays the **New Integrated Windows Service** dialog box.
 - Select an Integrated Windows service in your list and click **Properties** to display the **Integrated Windows Service Properties** dialog box.

Both dialog boxes appear similar to the one shown in [Figure 50](#).

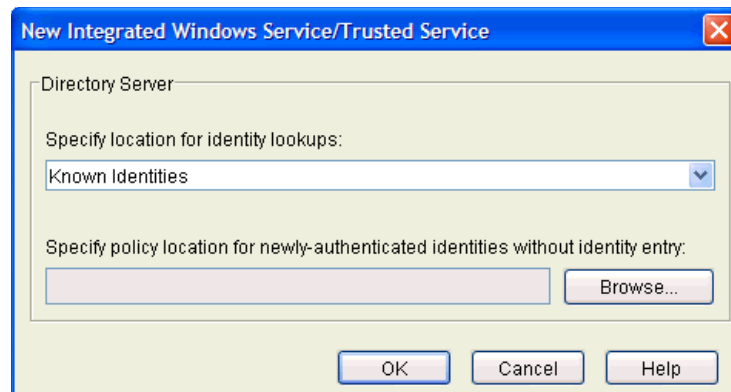


Figure 50 Integrated Windows Service Dialog Box

- 3 In the **Specify location for identity lookups** drop-down list, select a lookup destination from your global identity location list for this service. Irrespective of whether the profiles are stored in the directory service, or synthesized as a result of being stored in another data source, select a corresponding location. Depending on whether you select **Known Identities** or a specific identity location, the Policy Validator's behavior varies:
 - **Known Identities:** Search in all identity locations, based on the order specified in the global identity locations list. This option is a good choice when you are unsure of where an identity profile is stored.

Because DNs for each identity location are unique, you are guaranteed that no authentication ambiguities occur as a result of cached identity profiles on the Policy Validator.
 - **Specific identity location:** Search in this identity location *only*. This option offers faster performance.
- 4 Click **Browse** and select the group or folder in the **Specify policy location for newly authenticated identities without identity entry** field. This location is only used when transient entries are synthesized.

This group or folder acts as the repository for the access policy *only*. Once an identity is authenticated by this service, the Policy Validator checks this location for the corresponding access policy.
- 5 Click **OK** to commit these configuration parameters.

NTLM Authentication Service

The New NTLM Service dialog box allows you to set up a new NTLM service. NTLM services use a Windows domain NTLM authentication service on the domain controller to authenticate identities given the identity credentials received from an Enforcer plugin. This option is available to Windows 2000 Domain Controllers.

Not only does this allow Select Access to leverage the security features of the Windows operating system, but it also allows you to treat native Windows identities as Select Access identities without duplicating user data and credentials in the directory server(s) acting as your identity location.



If you are using NTLM or Kerberos authentication, and want the identity to be able to modify her Windows domain password, then you must meet the following conditions: you must be using an Active Directory server, and the Policy Validator and the Windows 2000 domain controller must be using the exact same identity location.

To configure a new or existing NTLM service

- 1 Click **Tools** → **Authentication Services**. The **Authentication Services** dialog box appears, displaying a list of available services.
- 2 Do one of the following:
 - Click **Add** to display the **Authentication Method** dialog box. Enter a service name and click the **NTLM** option before clicking **OK**. This displays the **New NTLM service** dialog box.
 - Select an NTLM service in your list and click **Properties** to display the **NTLM Service Properties** dialog box.

Both dialog boxes appear similar to the one shown in [Figure 51](#).

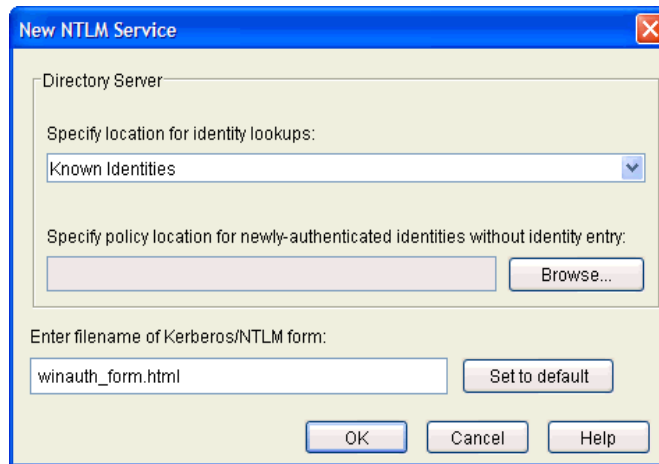


Figure 51 New NTLM Service Dialog Box

- 3 In the **Specify location for identity lookups** drop-down list, select a lookup destination from your global identity location list, for this service. Irrespective of whether the profiles are stored in the directory, or synthesized as a result of being stored in another data source, you must select a corresponding identity location. Depending on whether you select **Known Identities** or a specific identity location, the Policy Validator's behavior varies:

- **Known Identities:** Search in all identity locations, based on the order specified in the global identity locations list. This option is a good choice when you are unsure of where an identity profile is stored.

Because DNs for each identity location are unique, you are guaranteed that no authentication ambiguities occur as a result of cached identity profiles on the Policy Validator.

- **Specific identity location:** Search in this identity location *only*. This option offers faster performance.

- 4 Click **Browse** and select the group or folder in the **Specify policy location for newly authenticated identities without identity entry** field. This location is only used when transient entries are synthesized.

This group or folder acts as the repository for the access policy *only*. Once an identity is authenticated by this service, the Policy Validator checks this location for the corresponding access policy.

- 5 In the **Enter filename of Kerberos/NTLM login form** field, type the name of the form to be used. You can use the default form, `winauth_form.html`, or you can specify an alternative name for a form you have customized.

➤ If you need to revert to the default form name at any time, simply click **Set to default**.

- 6 Click **OK** to write these configuration details to the Policy Store.

Registration Authentication Service

The **New Registration Service** dialog box, as shown in [Figure 52](#), allows you to set up a new registration service. When an unknown user tries to access one of your network resources, you can ask the identity to register with you. You can choose one of two configuration methods:

- Registration via the Policy Validator
- Registration via the Administration server

The registration method you choose is transparent to the identity. The Policy Validator uses HTML forms to collect user information, whereas the Administration server uses JSP pages. However, configuring registration through the Administration server provides two principle benefits:

- Allows you finer control of the information that identities must provide. You can select the which attributes are used for the identity's RDN, which attributes the identity must provide, and which object classes the new profile will use.
- Enables you to apply a workflow condition to the registration process. If a workflow condition is applied, the identity can register, but no profile is created until one or more designated administrators approve the registration. The identity is not permitted to access protected resources until this profile is created.

➤ Registration via the Policy Validator has been deprecated for Select Access 6.2. It remains available only for backwards compatibility. In most cases, new directory servers supported in Select Access 6.2 will not be able to register using the Policy Validator.

Once the directory server profile is created for the identity, they can log in and access those resources for which they have permission. You must configure the server to automatically add newly-registered identities to a group you have created specifically for them. The access policies you create for this group are used by all registering identities, allowing you to control which network resources these identities are allowed to access.

➤ If you intend to allow identities to change their passwords (either via a profile-self management terminal point, or as a result of a corporate password policy), note that only password authentication and registration methods use this updated password. This is because only the password for the identity profile are changed, not those used by other authentication methods. For details, see [The Profile Self-Management Terminal Point](#) on page 193 and [Configuring Password Policies](#) on page 145.

➤ Before you configure your registration service, be sure to create the group (such as a "Reg Identities") to which all registering identities are added.

To configure a new or existing registration service

- 1 Click **Tools** → **Authentication Services**. The **Authentication Services** dialog box appears, displaying a list of available services.
- 2 Do one of the following:
 - Click **Add** to display the **Authentication Method** dialog box. Enter a service name and click the **Registration** option before clicking **OK**. This displays the **New Registration service** dialog box.
 - Select an Registration service in your list and click **Properties** to display the **Registration Service Properties** dialog box.

Both dialog boxes appear with the **General** tab displayed by default, as shown in [Figure 52](#).

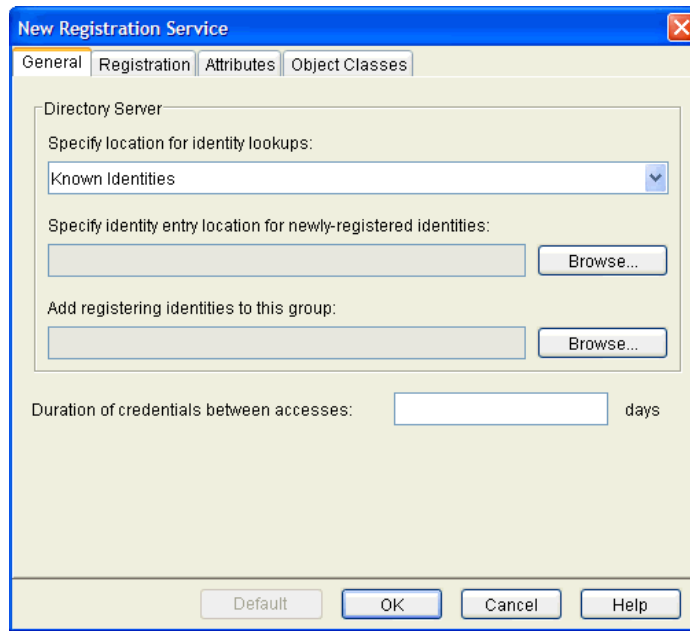


Figure 52 New Registration Service Dialog Box

- 3 In the **Specify location for identity lookups** drop-down list, select a lookup destination from your global identity location list, for this service. Depending on whether you select **Known Identities** or a specific identity location, the Policy Validator's behavior varies:

- **Known Identities:** Search in all identity locations, based on the order specified in the global identity locations list. This option is a good choice when you are unsure of where an identity profile is stored.

Because DNs for each identity location are unique, you are guaranteed that no authentication ambiguities occur as a result of cached identity profiles on the Policy Validator.

- **Specific identity location:** Search in this identity location *only*. This option offers faster performance.



If the Policy Validator cannot find an identity profile in this location, the identity cannot be authenticated and access to the resource is denied. Ensure you select the correct location for this service.

- 4 If your service performs identity lookups against a data source other than one of your configured LDAP identity locations in your global list, click **Browse** and select the group or folder in the **Specify policy location for newly-registered identities** field.

This group or folder acts as the repository for the access policy *only*. Once an identity is authenticated by this service, the Policy Validator checks this location for the corresponding access policy.

- 5 In the **Add registering identities to this group** field, click **Browse** and select the group to which registering identities are to be added.

- 6 In the **Duration of credentials between accesses** field, enter the number of days the identity has before Select Access requires them to log in again.
 - If the Administration server and the web server are on different machines, you *must* set the SSO cookie domain for the delegated Administration server Enforcer plugin. For information on setting this option, see [To configure central Enforcer plugin parameters](#) on page 256.
 - If the Administration server and the web server are on different domains, you *must*:
 - Add the web server to the Delegated Administration Enforcer plugin's MD-SSO table
 - Add the Administration server to the web server Enforcer plugin's MD-SSO table

For more information on adding a server to the MD-SSO table, see [To configure central Enforcer plugin parameters](#) on page 256.

 - Long-lived registration cookies are *not* supported when the Administration server and the web server are on different domains. In this case, if the identity exits a session, they will be required to re-login on the registration page the next time they try to access those resources protected by the registration authentication service.
- 7 Click the **Registration** tab. This tab, shown in [Figure 53](#), allows you to choose which component will manage registration.

The screenshot shows a dialog box titled "New Registration Service" with four tabs: "General", "Registration" (selected), "Attributes", and "Object Classes". The "Registration" tab contains two radio button options: "Registered by Validator" (unselected) and "Registered by Administration Server" (selected). Under "Registered by Validator", there is a text field for "Enter filename of registration form:" containing "registration_form.html" and a "Set to default" button. Under "Registered by Administration Server", there is a text field for "Administration Server URL:" containing "https://abater.americas.hpqcorp.net:9992/self_registration/register.jsp", a text field for "Enter URL path relative to the Administration Server:" containing "register.jsp" with a "Set to default" button, and a checkbox labeled "Enable workflow:" which is unchecked, with a dropdown menu showing "Workflow". At the bottom of the dialog are four buttons: "Default", "OK", "Cancel", and "Help".

Figure 53 New Registration Service Registration Tab

8 Choose one of the following options:

- **Registered by Validator:** If you choose **Registered by Validator**, review the registration form the Policy Validator uses for registration and authentication and modify it if necessary. You can use the default form, `registration_form.html`, or you can specify an alternative name for a form you have customized.

▶ If you need to revert to the default form name at any time, simply click **Set to default**.

Once you have entered the form name, proceed to Step 13.

- **Registered by Administration Server:** If you choose Registered by Administration Server, do the following:

— Review the registration form the Administration server uses for registration and authentication and modify it if necessary. You can use the default form, `register.jsp`, or you can specify an alternative name for a form you have customized.

▶ If you need to revert to the default form name at any time, simply click **Set to default**.

▶ You can create a static link to this URL instead of protecting a resource with the registration authentication service. If you do so, you must add three HTML parameters to the URL:

- `authentication_server`: The name of the registration authentication service which is configured in the Policy Builder and whose properties are to be used by the JSP registration page.
- `referer`: The complete path to the final target URL to which the Administration server will redirect the identity to after successfully registering them.
- `method`: The HTML method used. On a static link, its value will be `GET`.

For example, a sample static link URL might be:

```
https://adminserver-host:9992/self_registration/
register.jsp?authentication_server=reg_server&referer=ht
tp://web-server-host:80/index.html&method=GET
```

▶ If you have enabled a password policy in the Policy Builder, it will be enforced when new identities attempt to register. For information on enabling password policy, see [Configuring Password Policies](#) on page 145.



If you are using the Administration server to register your identities, ensure the JSP form collects the identity's first name. Otherwise, identities are able to create passwords that include part of their name or userID.

— If you want user registration to be approved before the identity profile is created, click **Enable workflow** and select a workflow rule from the adjacent drop-down list.

▶ You must first create a workflow rule before enabling this option. For information on creating workflow rules, see [To create a new workflow rule](#) on page 221.

- 9 Click the **Attributes** tab. This tab, shown in [Figure 54](#), allows you to specify which attributes the identity must supply when registering. By default, the minimal set of attributes required by your directory server are already selected. This list varies depending on which directory server you are using.

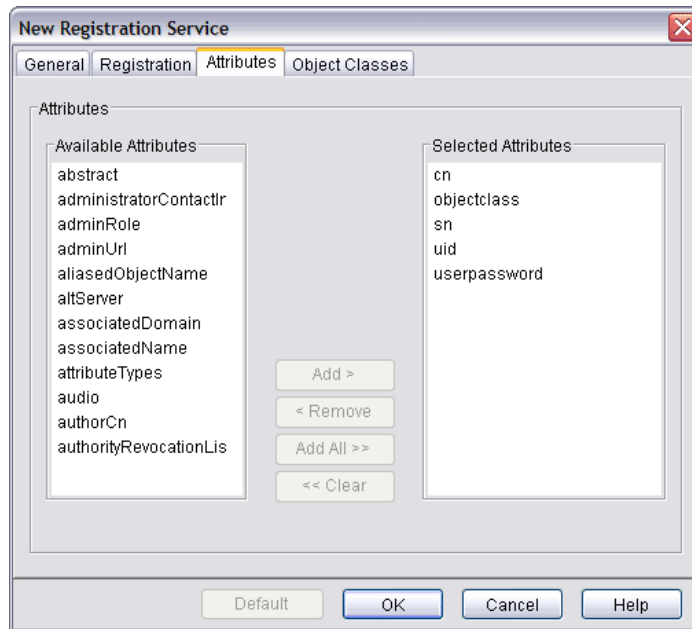


Figure 54 New Registration Service Attributes Tab

- 10 Review the list of **Selected Attributes** that must be filled out by the identity in the registration form and modify it as necessary.
- To add an attribute, select it from the **Available Attributes** list and click **Add** to move them to the **Selected Attributes** list.
 - To remove attributes, select them in the **Selected Attributes** list and click **Remove**.
 - To restore the list of default attributes, click **Default**.
- 11 Click the **Object Classes** tab. This tab, shown in [Figure 55](#), allows you to select the object classes the attributes selected on the **Attributes** tab belong to. By default, the object classes to which the default attributes belong are selected.
- For more information on object classes, see [About Object Classes](#) in the *HP OpenView Select Access 6.2 Concepts Guide*.

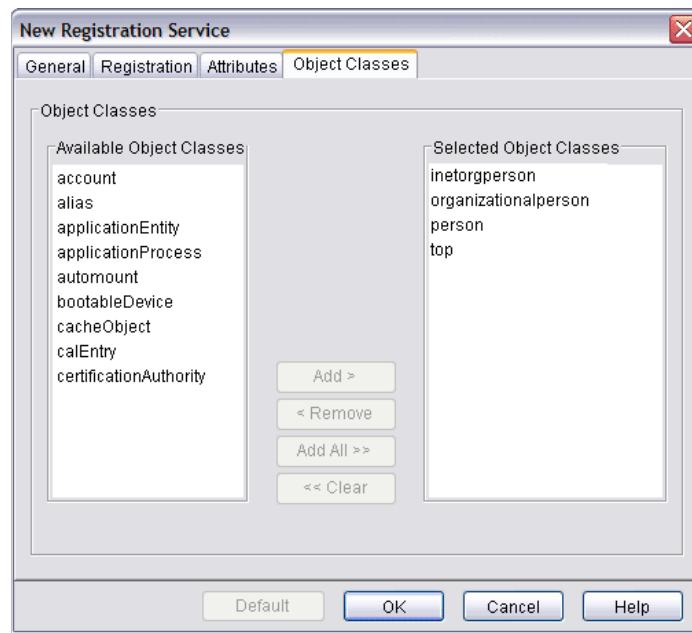


Figure 55 New Registration Service Object Classes Tab

- 12 Review the list of selected object classes and modify it as necessary:
 - To add an object class, select it from the **Available Object Classes** list and click **Add** to move them to the **Selected Object Classes** list.
 - To remove attributes, select them in the **Selected Object Classes** list and click **Remove**.
 - To restore the list of default object classes, click **Default**.

➤ You must select the object classes to which every attribute selected on the Attributes tab belongs.
- 13 Click **OK** to write these configuration details to the Policy Store.

Trusted Servers Authentication Service

This service allows any trusted third-party server you configure to securely processing and authenticate credentials instead of Select Access. This service is useful when you are using any authentication mechanism outside of Select Access, but would still like to use Select Access for authorization of identities to determine individual entitlements. An example scenario is if you are federating among one or more organizations via SAML and/or Liberty servers.

How does the Trusted Server Policy Validator plugin work?

Unlike other authentication plugins, the Trusted Servers service does not truly authenticate the identity. Instead, the plugin expects that the identity has been pre-authenticated on the identity's originating domain. The originating server relays all of the authenticated user's credentials and even user attributes to the Enforcer plugin. This triggers the following authentication process:

- 1 The IIS Enforcer plugin forwards credentials and attributes to the Trusted Server plugin on the Policy Validator.

- 2 The Trusted Server plugin processes the authentication information.
- 3 The Policy Validator either creates a transient identity profile or locates an existing identity profile in the identity data location for Select Access.
- 4 The Policy Validator returns an allow/deny/conditional decision and creates a cookie for the identity.
- 5 The Enforcer plugin returns the cookie to the client.

To configure a new or existing trusted authentication service

- 1 Click **Tools** → **Authentication Services**. The **Authentication Services** dialog box appears, displaying a list of available services.
- 2 Do one of the following
 - Click **Add** to display the **Authentication Method** dialog box. Enter a service name and click the **Trusted Servers** option before clicking **OK**. This displays the **New Trusted Servers Service** dialog box.
 - Select an Trusted Server authentication service in your list and click **Properties** to display the **Trusted Servers Properties** dialog box.

Both dialog boxes appear similar to the one shown in [Figure 56](#).

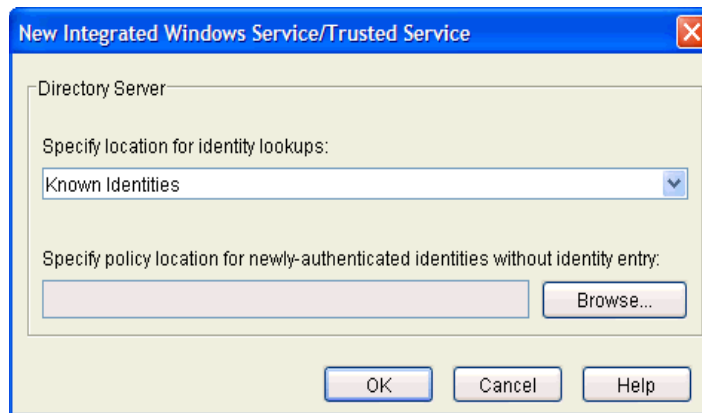


Figure 56 Trusted Servers Dialog Box

- 3 In the **Specify location for identity lookups** drop-down list, select a lookup destination from your global identity location list, for this service. Irrespective of whether the profiles are stored in the directory server, or synthesized as a result of being stored in another data source, select a corresponding location. Depending on whether you select **Known Identities** or a specific identity location, the Policy Validator's behavior varies:
 - **Known Identities:** Search in all identity locations, based on the order specified in the global identity locations list. This option is a good choice when you are unsure of where an identity profile is stored. Because DNs for each identity location are unique, you are guaranteed that no authentication ambiguities occur as a result of cached identity profiles on the Policy Validator.
 - **Specific identity location:** Search in this identity location *only*. This option offers faster performance.

- 4 Click **Browse** and select the group or folder in the **Specify policy location for newly authenticated identities without identity entry** field. This location is only used when transient entries are synthesized.
 - This location acts as the repository for the access policy *only*. Once an identity is authenticated by this service, the Policy Validator checks this location for the corresponding access policy.
- 5 Click **OK** to commit these configuration parameters.

RADIUS Authentication Service

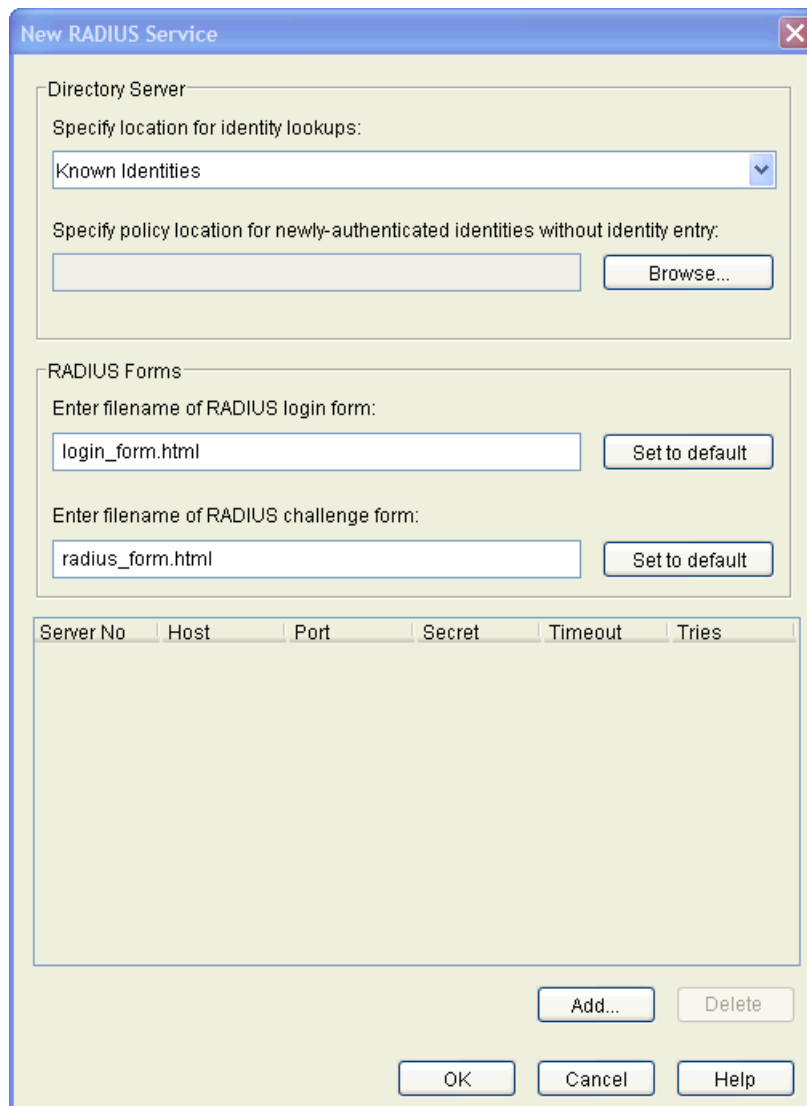
The **New RADIUS Service** dialog box allows you to set up a new RADIUS service, as shown in [Figure 57](#). Unlike some other authentication methods that authenticate the identity with the Policy Validator, the RADIUS service acts as the authenticator in this case. However, before the RADIUS service can challenge the end user, her identity must be a known identity and consequently is required to log into the service first. Only then can the service challenge the known user for a secret. If the secret the end user supplies matches the secret on the authentication service, the identity is authenticated.

- Before you configure the properties of your RADIUS service, consider creating a group or folder (such as a “Transient RADIUS Identities”). This allows you to create an authorization rule for identities authenticated by this service.
- You cannot add the same type of challenge/response service (RADIUS) more than once in a conditional access rule because each instance of the service makes use of the same login form that was shipped with Select Access.

To configure a new or existing RADIUS service

- 1 Click **Tools** → **Authentication Services**. The **Authentication Services** dialog box appears, displaying a list of available services.
- 2 Do one of the following:
 - Click **Add** to display the **Authentication Method** dialog box. Enter a service name and click the **RADIUS** option before clicking **OK**. This displays the **New RADIUS Service** dialog box.
 - Select an RADIUS service in your list and click **Properties** to display the **RADIUS Service Properties** dialog box.

Both dialog boxes appear similar to the one shown in [Figure 57](#).



The dialog box is titled "New RADIUS Service" and contains the following sections:

- Directory Server:**
 - Specify location for identity lookups: A drop-down menu with "Known Identities" selected.
 - Specify policy location for newly-authenticated identities without identity entry: An empty text box with a "Browse..." button next to it.
- RADIUS Forms:**
 - Enter filename of RADIUS login form: A text box containing "login_form.html" with a "Set to default" button.
 - Enter filename of RADIUS challenge form: A text box containing "radius_form.html" with a "Set to default" button.
- Table:** A table with columns: Server No, Host, Port, Secret, Timeout, Tries. The table is currently empty.
- Buttons:** "Add..." and "Delete" buttons are located below the table. At the bottom of the dialog are "OK", "Cancel", and "Help" buttons.

Figure 57 RADIUS Service Properties Dialog Box

- 3 In the **Specify location for identity lookups** drop-down list, select a lookup destination from your global identity location list, for this service. Irrespective of whether the profiles are stored in LDAP, or synthesized as a result of being stored in another data source, select a corresponding location. Depending on whether you select **Known Identities** or a specific identity location, the Policy Validator's behavior varies:
 - **Known Identities:** Search in all identity locations, based on the order specified in the global identity locations list. This option is a good choice when you are unsure of where an identity profile is stored.

Because DNs for each identity location are unique, you are guaranteed that no authentication ambiguities occur as a result of cached identity profiles on the Policy Validator.
 - **Specific identity location:** Search in this identity location *only*. This option offers faster performance.
- 4 Click **Browse** and select the group or folder in the **Specify policy location for newly authenticated identities without identity entry** field. This location is only used when transient entries are synthesized.

This group or folder acts as the repository for the access policy *only*. Once an identity is authenticated by this service, the Policy Validator checks this location for the corresponding access policy.

- 5 In the RADIUS Forms group, configure the following fields:
 - **Enter filename of RADIUS login form:** type the name of the RADIUS login form used to authenticate identities. You can use the default form, `login_form.html`, or you can specify an alternative name for a form you have customized.
 - **Enter the filename of RADIUS challenge form:** type the name of the RADIUS challenge form used to present challenges to and capture user responses. You can use the default form, `radius_form.html`, or you can specify an alternative name for a form you have customized.



 If you need to revert to the default form names at any time, simply click **Set to default**.
- 6 To define service-specific information, click **Add**. This creates a row where new RADIUS authentication services are numbered sequentially. You can specify up to ten RADIUS services.
- 7 Enter the information as described in [Table 20](#) in the row that is created.

Table 20 RADIUS Service Properties

Column	Description
Host	A valid domain name or IP address of the RADIUS service.
Port	Any valid port number between 1-65535.
Secret	A shared string between the RADIUS service and the end user. A matching Secret indicates that user is authenticated. The maximum number of characters is limited to 1000.
Timeout	The amount of time allocated before a connection attempt with the RADIUS service times out. Enter the timeout value in seconds. The timeout limit is 999 seconds.
Tries	The number of connection attempts. The retry limit is 99.

Repeat as necessary.

- 8 To delete a service, select the row you want to remove and click **Delete**.

 You cannot delete a RADIUS service if it is the only one you have created.
- 9 Click **OK** to write these configuration details to the Policy Store. The Policy Builder checks the validity of the information before it is written to the directory server. If an incorrect value has been entered at any point, an error message directs you to the problem and offers a potential solution.

SecurID Authentication Service

The **New SecurID Service** dialog box allows you to set up a new SecurID service, as shown in [Figure 58](#) on page 118. Unlike some other authentication methods that authenticate the identity with the Policy Validator, the SecurID service acts as the authenticator in this case. SecurID support allows Select Access to tie into an enterprise's token-based authentication scheme, as well as username and password, X.509 digital certificates, and user self-registration.

- Before you configure the properties of your SecurID service, be sure to create a group or folder such as a "SecurID transient identities". This allows you to create an authorization rule for identities authenticated by this authentication service.
- For SecurID to work with Select Access, ensure that:
 - 1 On Windows, ensure you have the RSA ACE/Agent Windows installed as your SecurID client.
 - 2 On all platforms, ensure `sdconf.rec` is saved in the appropriate platform-specific location:
 - For Windows 2000: `C:\WINNT\system32`
 - For Windows 2003: `C:\Windows\system32`
 - For UNIX: `/var/ace/`
 - 3 On all platforms, ensure the SecurID client's host is registered as an agent of the SecurID server.
- You can set up multiple SecurID authentication services to authenticate identities in different identity locations. However, using multiple services and identity locations can have negative implications: one service can short-circuit another service depending on which service accepts the identity's credentials first and which identity location the identity's profile is stored in. Therefore, to avoid unpredictable authentication behaviors, HP recommends that you restrict the number of SecurID authentication services to one, and configure Select Auth to use this service against the Known Identities branch only.

To configure a new or existing SecurID service

- 1 Click **Tools** → **Authentication Services**. The **Authentication Services** dialog box appears, displaying a list of available services.
- 2 Do one of the following:
 - Click **Add** to display the **Authentication Method** dialog box. Enter a service name and click the **SecurID** option before clicking **OK**. This displays the **New SecurID Service** dialog box.
 - Select an SecurID service in your list and click **Properties** to display the **SecurID Service Properties** dialog box.

Both dialog boxes appear similar to the one shown in [Figure 58](#).

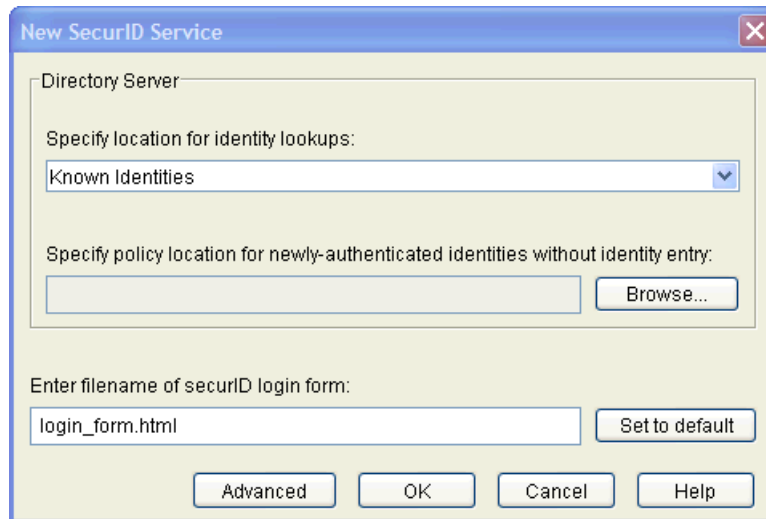


Figure 58 New SecurID Service Dialog Box

- 3 In the **Specify location for identity lookups** drop-down list, select a lookup destination from your global identity location list, for this service. Depending on whether you select **Known Identities** or a specific identity location, the Policy Validator's behavior varies:

- **Known Identities:** Search in all identity locations, based on the order specified in the global identity locations list. This option is a good choice when you are unsure of where an identity profile is stored.

Because DNs for each identity location are unique, you are guaranteed that no authentication ambiguities occur as a result of cached identity profiles on the Policy Validator.

- **Specific identity location:** Search in this identity location *only*. This option offers faster performance.

- 4 Click **Browse** and select the group or folder in the **Specify policy location for newly authenticated identities without identity entry** field. This location is only used when transient entries are synthesized.

This group or folder acts as the repository for the access policy *only*. Once an identity is authenticated by this service, the Policy Validator checks this location for the corresponding access policy.

- 5 In the **Enter filename of SecurID login form** field, type the name of the registration form to be used for user authentication. You can use the default form, `login_form.html`, or you can specify an alternative name for a form you have customized.

► If you need to revert to the default form name at any time, simply click **Set to default**.

- 6 If you want to configure advanced SecurID properties, click **Advanced**. This displays the **SecurID Advanced Configuration** dialog box, which allows you to configure specific Select Access actions for SecurID error codes. For details, see [To configure advanced SecurID properties](#) on page 119.
- 7 Click **OK** to write these configuration details to the Policy Store.

To configure advanced SecurID properties

- 1 Display the **SecurID Advanced Properties** dialog box. Do this by:
 - Clicking **Tools** → **Authentication Services**.
 - Adding a new, or modifying an existing SecurID service. For details, see [To configure a new or existing SecurID service](#).
 - In the **New SecurID Service** or **Edit SecurID Service Properties** dialog box, clicking **Advanced**.

The **SecurID Advanced Properties** dialog box appears.



Altering the default behavior of SecurID return codes can have a detrimental impact on the security mechanisms of SecurID. Choose your actions carefully.

Return Code	Action	Personalization Value
1515	Pass	Token submitted was a su...
314	Fail	Please contact technical su...

Figure 59 SecurID Advanced Properties Dialog Box

- 2 Create an HTTP header from the personalization string you enter in the **Return Personalization String in HTTP** header field. This string is used to encode the personalization value(s) you configure in subsequent steps.
- 3 For each SecurID return code you want to alter the outcome for, configure a line in the table by doing the following:

- Click **Add**. This inserts a new row in the table.



You must configure the cells of this row. If you have inadvertently added a row you do not need, select it and click **Delete**.

- Enter the **Return Code**. The return code can be any whole number that is higher than 0. However, HP recommends that you limit error codes to the following:

0=ACM_OK

1=ACM_ACCESS_DENIED

2=ACM_NEXT_CODE_REQUIRED

5=ACM_NEW_PIN_REQUIRED

- Choose an **Action** for the code you just define. You can choose either **Pass** or **Deny**.

- Enter a **Personalization Value**. The value can be any text string. Select Access encodes this value within the HTTP header you defined earlier. This string is ultimately displayed to the identity.
- 4 Click **OK** to write these configuration details to the Policy Store.

Certificate Authentication Service

The **New Certificate Service** dialog box allows you to set up a new service for the Policy Validator to authenticate identities with a certificate, as shown in [Figure 60](#).

Before the Policy Validator allows the identity to access the resource she requested, the identity's certificate:

- Must be signed by the root certificate you configure with this dialog.
- Can match the certificate on the directory server. This is not necessarily required, depending on how you configure your certificate service.

When both of these cases are true, the Policy Validator validates the certificate for that user, and the Enforcer plugin executes the authorization rule.



The directory server must contain an entry with a `certificationAuthority` object class and a `caCertificate` attribute. Otherwise, you receive a message indicating that a certificate authority policy cannot be found.



Consider creating a group or folder (such as a “Transient Cert Identities”) to create an authorization rule for identities authenticated by this authentication service.

To configure a new or existing certificate service

- 1 Click **Tools** → **Authentication Services**. The **Authentication Services** dialog box appears, displaying a list of available services.
- 2 Do one of the following:
 - Click **Add** to display the **Authentication Method** dialog box. Enter a service name and click the **Certificate** option before clicking **OK**. This displays the **New Certificate Service** dialog box.
 - Select a Certificate service in your list and click **Properties** to display the **Certificate Service Properties** dialog box.

Both dialog boxes appear similar to the one shown in [Figure 60](#).

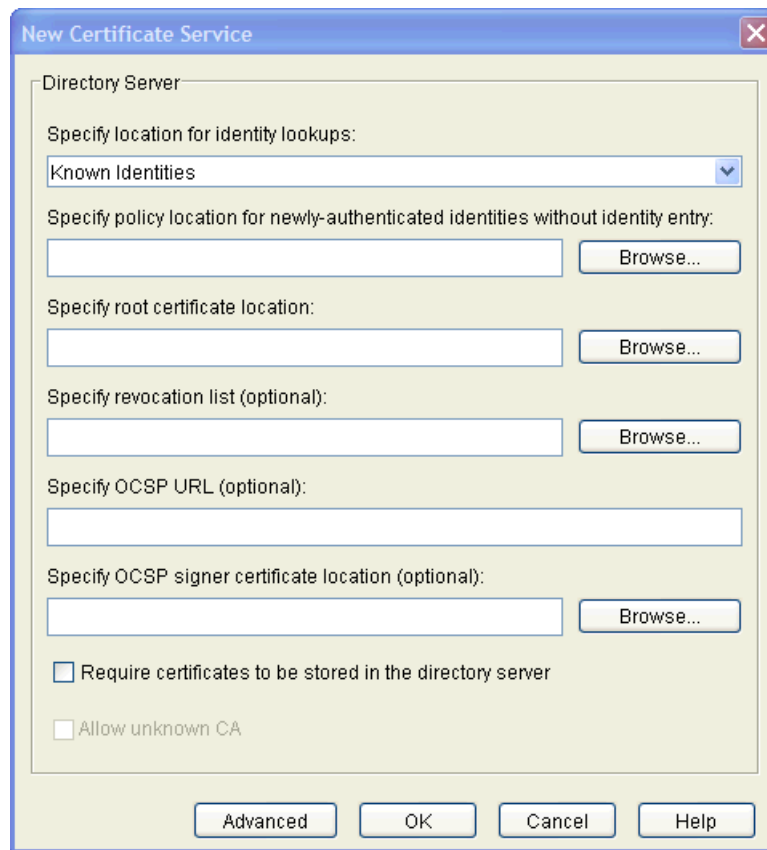


Figure 60 New Certificate Service Dialog Box

- 3 In the **Specify location for identity lookups** drop-down list, select a lookup destination from your global identity location list, for this service. Irrespective of whether the profiles are stored in LDAP, or synthesized as a result of being stored in another data source, select a corresponding location. Depending on whether you select **Known Identities** or a specific identity location, the Policy Validator's behavior varies:
 - **Known Identities:** Search in all identity locations, based on the order specified in the global identity locations list. This option is a good choice when you are unsure of where an identity profile is stored.
 Because DNs for each identity location are unique, you are guaranteed that no authentication ambiguities occur as a result of cached identity profiles on the Policy Validator.
 - **Specific identity location:** Search in this identity location *only*. This option offers faster performance.
- 4 Click **Browse** and select the group or folder in the **Specify policy location for newly authenticated identities without identity entry** field. This location is only used when transient entries are synthesized.
 This group or folder acts as the repository for the access policy *only*. Once an identity is authenticated by this service, the Policy Validator checks this location for the corresponding access policy.
- 5 In the **Specify root certificate location** field, click **Browse** and select the directory server location where your certificates are stored. You must have a root certificate in your directory server before you can select this location.

- 6 If you are using a revocation list, click **Browse** and select the directory server location where the list is stored in the **Specify revocation list** field. This list determines the revocation state of an identified certificate. The Policy Validator issues a status request query to this server, and suspends user access until the server verifies the certificate in question. If the status is not acceptable, the server is rejected and the identity is not authenticated.
- 7 If you are using an Online Certificate Status Protocol server, enter a fully qualified URL in the **Specify OCSP URL** field. This server determines the revocation state of an identified certificate. The Policy Validator then issues a status request query to this server and suspends user access until the server verifies the certificate in question.
- 8 If you require the identity's certificate to be in an identity profile belonging to a specific directory server identity location, check the **Require certificates to be stored on the directory server** check box.
- 9 If you check the **Require certificates to be stored on the directory server** check box, you can also check the **Allow unknown CA** check box. This means that a CA that is not known to you can issue user certificates.
- 10 If you want to configure advanced certificate properties, click **Advanced**. This displays the **Advanced Certificate Configuration** dialog box, which allows you to configure CRL and OCSP checking behavior. For details on how to configure this dialog box, see [To configure advanced certificate properties](#) on page 122.
- 11 Click **OK** to write these configuration details to the Policy Store.

[To configure advanced certificate properties](#)

- 1 Display the **Advanced Certificate Configuration** dialog box. Do this by:
 - Clicking **Tools** → **Authentication Services**.
 - Adding a new, or modifying an existing certificate service. For details, see [To configure a new or existing certificate service](#).
 - In the **New Certificate Service** or **Edit Certificate Service Properties** dialog box, clicking **Advanced**.

The **Advanced Certificate Configuration** dialog box appears.

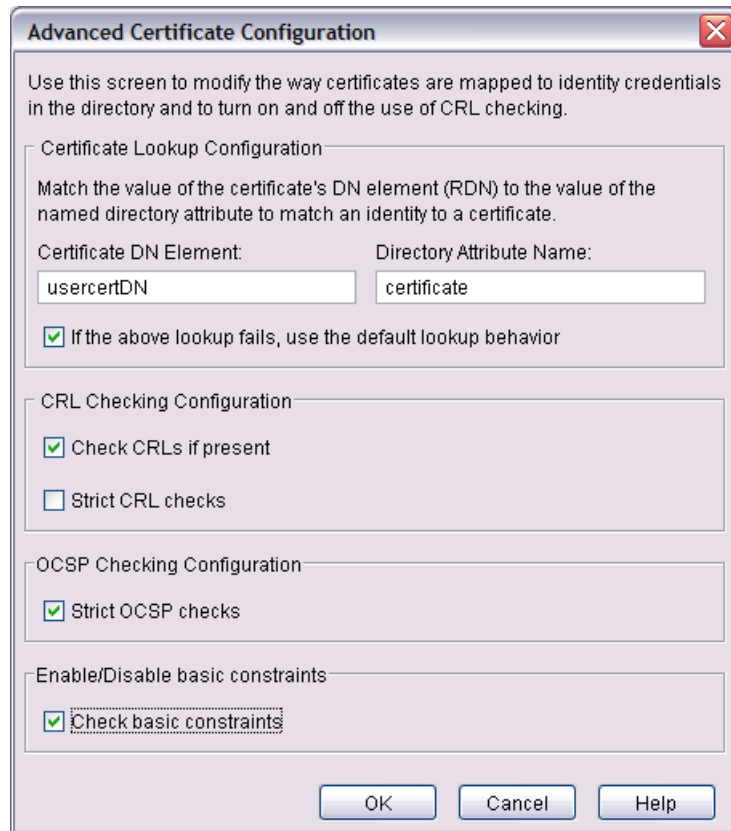


Figure 61 Advanced Certificate Configuration Dialog Box

Advanced certificate configuration consists of two things:

- **How to map the certificate's DN as an identity attribute's value:** This facilitates the way the Policy Validator looks up certificates when authenticating identities.
 - **Whether or not to check CRLs and or OCSP responders:** If you have a CDP mechanism, this feature ensures your CRL is always current by checking the certificate entries on this list.
- 2 To configure **Certificate Lookups**, enter the name of the **Certificate DN Element** that is to be mapped to a **Directory Attribute Name**.

For example, if you map the CN of the Certificate DN to the `surname` LDAP attribute, then the Policy Validator matches the CN of the certificate to the identity's `surname` on the directory server.
 - 3 If you want to use the Policy Validator's normal lookup method (if the method described in Step 2 fails), check the **If the above method fails, use default lookup behavior** check box. The Policy Validator's default behavior is to search for the CN of an identity.
 - 4 To check the CRLs in the CDP mechanism, check the **Check CRLs if present** check box.
 - 5 To enable strict CRL checking with your certificate service, click the **Strict CRL checks** check box. This affects Policy Validator's behavior in that it cannot authenticate identities when:
 - The Policy Validator cannot find the CRL.
 - The Policy Validator compares the current time with the date of the next update timestamp in the CRL. If the current time exceeds that timestamp, the CRL is deemed out-of-date and therefore cannot be trusted.

- 6 To enable strict OCSP checking with your certificate service, click the **Strict OCSP checks** check box. This affects Policy Validator's behavior in that it cannot authenticate identities when:
 - The Policy Validator cannot contact the OCSP responder.
 - The Policy Validator cannot verify the reply received from the OCSP responder in question.
 - The reply that Policy Validator receives is classified as "unknown".

➤ If your Enforcer plugin's configuration uses a value for its **Wait for Validator Reply** (a **Tuning** parameter) is less than OCSP 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.
 - 7 To determine whether basic constraints of a certificate should be checked and enforced, check the **Check basic constraints** check box.
- Basic constraints are one of the extensions that control the processing of a certificate path for a specific certificate. Basic constraints control whether or not a certificate can be used to sign other certificates. If you uncheck this box, the Policy Validator ignores errors from not seeing `basic constraint:true` in the root certificate.
- If you check this box, and errors are reported, certificate validation fails. In this case, the Policy Validator cannot authenticate the identity.

Password Authentication Service

The **New Password Service** dialog box allows you to set up a new service to be used by the Policy Validator to authenticate identities requesting a resource with a password, as shown in [Figure 62](#).

The password an identity enters must match the password stored in the directory server's database.

- If you intend to allow identities to change their passwords (either via a profile-self management terminal point, or as a result of a corporate password policy), note that only password authentication and registration methods use this updated password. This is because only the password for the identity profiles are changed, not those used by other authentication methods. For details, see [The Profile Self-Management Terminal Point](#) on page 193 and [Configuring Password Policies](#) on page 145.

To configure a new or existing password service

- 1 Click **Tools** → **Authentication Services**. The **Authentication Services** dialog box appears, displaying a list of available services.
- 2 Do one of the following:
 - Click **Add** to display the **Authentication Method** dialog box. Enter a service name and click the **Password** option before clicking **OK**. This displays the **New Password Service** dialog box.
 - Select a Password service in your list and click **Properties** to display the **Password Service Properties** dialog box.

Both dialog boxes appear similar to the one shown in [Figure 62](#).

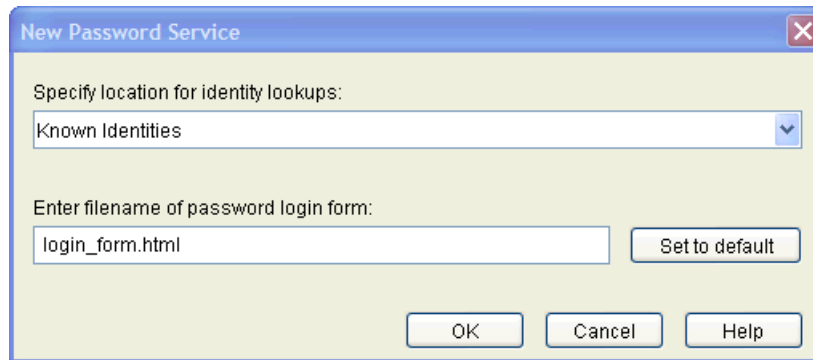


Figure 62 New Password Service Dialog Box

- 3 In the **Specify location for identity lookups** drop-down list, select a lookup destination from your global identity location list, for this service. Depending on whether you select **Known Identities** or a specific identity location, the Policy Validator's behavior varies:
 - **Known Identities:** Search in all identity locations, based on the order specified in the global identity locations list. This option is a good choice when you are unsure of where an identity profile is stored.

Because DNs for each identity location are unique, you are guaranteed that no authentication ambiguities can occur as a result of cached identity profiles on the Policy Validator.
 - **Specific identity location:** Search in this identity location *only*. This option offers faster performance.
- 4 In the **Enter filename of password login form** field, type the name of the password login form to be used for user authentication. You can use the default form, `login_form.html`, or you can specify an alternative name for a form you have customized.
 - If you need to revert to the default form name at any time, simply click **Set to default**.
- 5 Click **OK** to write these configuration details to the Policy Store.

Kerberos Authentication Service

Kerberos authentication services use a Windows domain Kerberos authentication service to authenticate identities. Not only does this allow Select Access to leverage the security features of the Windows operating system, but it also allows you to treat native Windows identities as Select Access identities without duplicating user data and credentials in the directory server(s) acting as your identity location.

- Kerberos authentication is available to Windows 2000/2003 Domain Controllers only.
- If you are using NTLM or Kerberos authentication, and want the identity to be able to modify her Windows domain password, then you must meet the following conditions: you must be using an Active Directory server, and the Policy Validator and the Windows 2000/2003 domain controller must be using the exact same identity location.

To configure a new or existing Kerberos service

- 1 Click **Tools** → **Authentication Services**. The **Authentication Services** dialog box appears, displaying a list of available services.
- 2 Do one of the following:
 - Click **Add** to display the **Authentication Method** dialog box. Enter a service name and click the **Kerberos** option before clicking **OK**. This displays the **New Kerberos Service** dialog box.
 - Select an Kerberos service in your list and click **Properties** to display the **Kerberos Service Properties** dialog box.

Both dialog boxes appear similar to the one shown in [Figure 63](#).

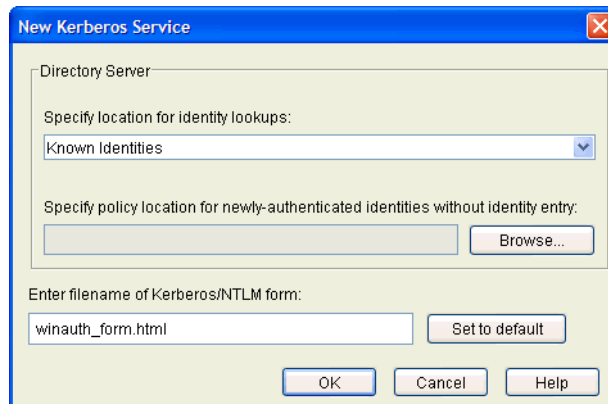


Figure 63 New Kerberos Service Dialog Box

- 3 In the **Specify location for identity lookups** drop-down list, select a lookup destination from your global identity location list, for this service. Depending on whether you select **Known Identities** or a specific identity location, the Policy Validator's behavior varies:
 - **Known Identities:** Search in all identity locations, based on the order specified in the global identity locations list. This option is a good choice when you are unsure of where an identity profile is stored.

Because DNs for each identity location are unique, you are guaranteed that no authentication ambiguities occur as a result of cached identity profiles on the Policy Validator.
 - **Specific identity location:** Search in this identity location *only*. This option offers faster performance.
- 4 Click **Browse** and select the group or folder in the **Specify policy location for newly authenticated identities without identity entry** field. This location is only used when transient entries are synthesized.

This group or folder acts as the repository for the access policy *only*. Once an identity is authenticated by this service, the Policy Validator checks this location for the corresponding access policy.

- 5 In the **Enter filename of Kerberos/NTLM login form** field, type the name of the registration form to be used for user registration and authentication. You can use the default form, `winauth_form.html`, or you can specify an alternative name for a form you have customized.



If you need to revert to the default form name at any time, simply click **Set to default**.

- 6 Click **OK** to write these configuration details to the Policy Store.

Avoiding Incorrect Service Setup for Groups and Dynamic Groups

Because of the way in which dynamic group and group logic is implemented, setting up authentication services incorrectly makes it seem as if the Policy Validator is not evaluating groups and dynamic groups correctly. For more information on setting up your groups and dynamic groups, see [Creating and Modifying a Group](#) on page 69 and [Creating and Modifying a Dynamic Group](#) on page 73.

Symptoms of an Incorrect Setup

When you configure a specific authentication service for a specific branch of the Identities Tree, only identities, groups, and dynamic groups on that branch are authenticated by that service. So, if you created a dynamic group on another branch, it may seem like the Policy Validator was not authenticating and/or evaluating this dynamic group, even though the identity may be part of the branch in question.

Select Access is implemented in this way with the intention of giving you the ability to segment your identities, which allows you to authenticate different user segments with different authentication services. This implementation allows the identity to be authenticated by the authentication service, but not the dynamic group of which the identity is a member.

To correctly set up authentication in the Policy Builder

Do one of the following:

- Add the dynamic group under each branch that you want the authentication service to authenticate.
- OR
- Set the authentication service to authenticate identities higher up on the Identities Tree.

Setting Up Authentication Forms Used by Authentication Services

Depending on your authentication service, you need to configure and customize an authentication support form deployed by the Enforcer plugin. These forms collect information from the identity via their web browser, which is sent to either the Policy Validator or the authentication service for validation.

By default, support forms templates are installed in the `<install_path>/content` folder. For additional details on how the Enforcer plugin uses these forms, or how you can customize the form templates for your own use, see [Chapter 3, Transparently Supported Web Server Integrations](#), in the *HP OpenView Select Access 6.2 Network Integration Guide*.

7 Controlling Network Access

This chapter describes the concept of access management. How you control identity access to sensitive resources depends on how you apply a correct combination of allow/deny/conditional policies against specific identity/resource combinations.

Chapter Overview

This chapter includes the following topics:

- [Understanding Authorization](#) on page 129
- [Using the Policy Matrix to Set Policy](#) on page 130
- [About Access Policy Inheritance](#) on page 133
- [Priority Given to Access Policies](#) on page 136
- [Tips for Administering Access Policies](#) on page 139
- [Administering Access Policies For Known or Unknown Identities](#) on page 130

Understanding Authorization

Once an identity has been authenticated, an access policy determines if an identity can access a specific resource. This is known as authorization and the Policy Builder gives a single administration point for both web and wireless access management.

With Select Access, you can apply and/or create three types of access policy values that work with wired and wireless access, as described in [Table 21](#).



Good practice dictates that identity access ultimately be determined by an access policy, not an authentication method. Setting the proper access policy is the only way to guarantee consistent access behavior.

Using the Policy Matrix to Set Policy

You can apply access policies to all possible identity/group and resource combinations. The access policy for each combination is shown where the identity profile and the resource entry intersect on the Policy Matrix, as shown in [Figure 64](#).

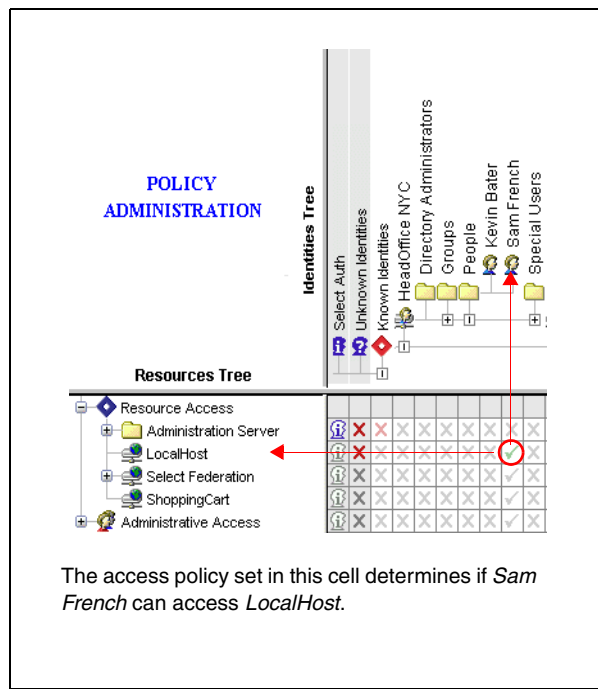


Figure 64 Setting Policy for a Specific Identity and Resource Pair

Administering Access Policies For Known or Unknown Identities

You apply access policies for both known and unknown identities the same way, using the Policy Matrix. When administering access policies for unknown identities, remember the following:

- Unknown identities include identities you cannot reasonably identify. Enable Select Auth in the **Select Auth** column if you want to try to authenticate all unknown identities. For example, Michael Fox is an identity profile in the directory server with his own set of access policies applied to his profile. However, if he is requesting resources remotely, he is not recognized as Michael Fox and therefore becomes an unknown identity. By enabling Select Auth, Michael Fox is given the opportunity to identify himself and gain access to resources he might not otherwise have.
- If an identity cannot be identified using Select Auth, apply a deny policy at the Network level for all unknown identities and allow access to those specific resources to which authentication is not required.
- Create a conditional policy that invokes a conditional rule that you can use to authenticate unknown identities. If the unknown identity becomes known (via an authentication decision point), then the rest of the conditional rule is abandoned. Instead, the policy for the identified user is used instead. If the policy is conditional, then that rule is evaluated instead.

To apply an access policy to a known or unknown identity

- 1 On the Policy Matrix, right-click the square where an identity profile and a resource entry intersect, as shown in [Figure 65](#).

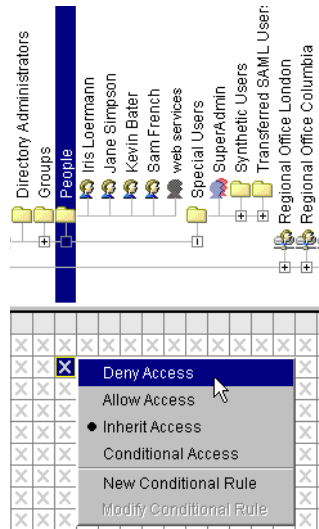


Figure 65 Shortcut Menu for Policy

- 2 Select an access policy. You can choose from the options described in [Table 21](#).

Table 21 List of Access Policy Options








Option	Description
Deny Access 	Deny access to the resource. A red X is shown in the square. The entry (folder, group, or identity) in the Identities Tree is denied access to the entry (folder, service, or resource) in the Resources Tree.
Allow Access 	Allow access to the resource. A green check mark is shown in the square. The entry (folder, group, or identity) in the Identities Tree is allowed access to the entry (folder, service, or resource) in the Resources Tree.
Inherit Access    	Inherit the access policy used by the parent entry. Any gray icon is shown in the square. The entries in the Identities Tree (folder, group, or identity) and the Resources Tree (folder, service, or resource) use the same access policy as their parent entry in the Policy Matrix. Note: The “+” icon appears when an identity inherits to multiple policies from groups to which she is a member. In this case, all rules are evaluated until one returns an allow decision.

Table 21 List of Access Policy Options (cont'd)

Option	Description
Conditional Access 	<p>Use a policy that points to a conditional access rule, which ultimately determines whether access is allowed or denied. To set this policy:</p> <ol style="list-style-type: none"> 1 Right-click the square and select Conditional Access. 2 In the Access Policy Rule Selection dialog box, select a rule and click OK. The rule is applied to the square and a key icon is shown. <p>If you have not yet created any rules, a message appears asking if you want to create one. Click Yes.</p> <p>For details on how to create a rule, see Creating a Rule on page 161.</p>
New Conditional Rule	<p>Create a new rule by launching the Rule Builder. For details on how to create a rule, see Creating a Rule on page 161.</p> <p>When you exit Rule Builder you can select the rule and click OK. The rule is applied to the square and a key icon is shown.</p>
Modify Conditional Rule	<p>Modify an existing rule by launching the Rule Builder. For details on how to create a rule, see To modify a rule on page 163.</p> <p>When you exit Rule Builder you can select the rule and click OK. The rule is applied to the square and a key icon is shown.</p>

About the Access Policy Icons

The icons in the Matrix indicate the type of access policy for an identity and resource pair, as shown in [Figure 66](#).

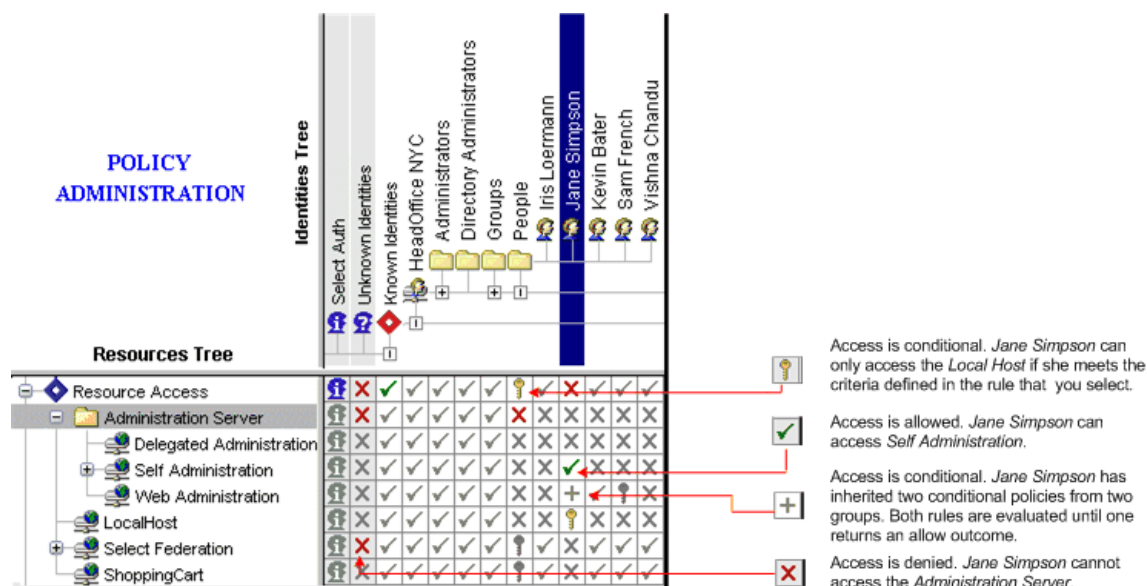


Figure 66 Access Policy Icons Defined

A colored icon indicates that the access policy was applied specifically to a profile, while a gray icon indicates that an access policy is inherited.

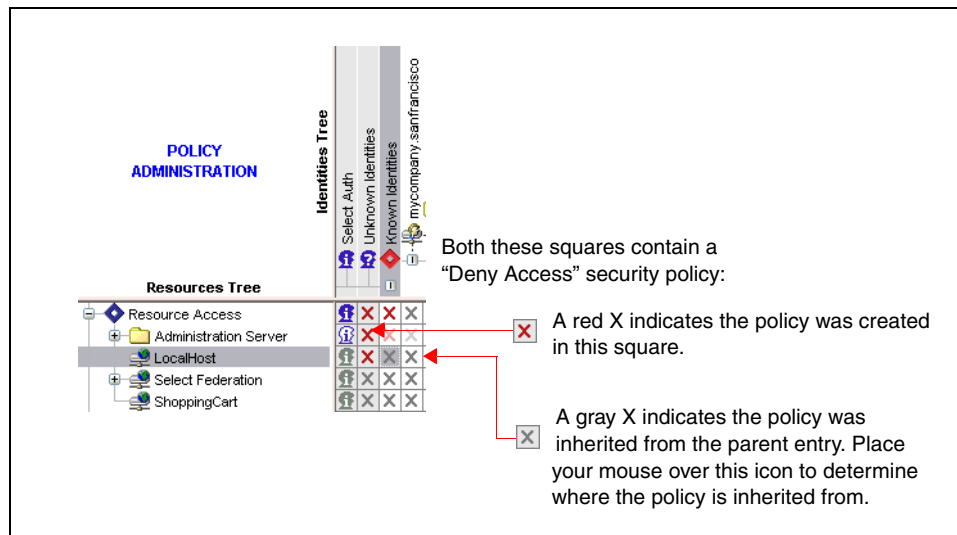


Figure 67 Inheritance Laws Overview

About Access Policy Inheritance

The Policy Matrix allows you to apply access policies for every possible identity and resource combination. This can result in hundreds, thousands, or even millions of combinations. To facilitate the creation of access policies for such large numbers of identities, Select Access uses inheritance. Inheritance allows you to quickly distribute access policies from high-level entries on the Identities Tree like root identities, folders, and groups, as shown in [Figure 67](#).

Increasing Scalability

Policy inheritance also makes Policy Builder extremely scalable. When you add new identities and groups to the Identities Tree, or new services and resources to the Resources Tree, they automatically inherit the access policies applied to their parent entry in the tree. This allows you to quickly add new identities and resources to Policy Builder and automatically apply access policies for them.

Inheriting Access Policies

Administering access policies for all your identity and resource combinations is streamlined because policies are inherited across the Policy Matrix in the following ways:

- The access policy applied to the root of the Identities Tree and the root of the Resources Tree is inherited by all entries on both trees, as shown in [Figure 68](#).
- Enforcer-protected services that you have not added to the Policy Matrix also inherit this root policy. Therefore, to ensure that the Policy Validator applies the right access decision to a resource request, ensure that you add all Enforcer-protected services to the Resources Tree. This allows you to apply an explicit policy against it.

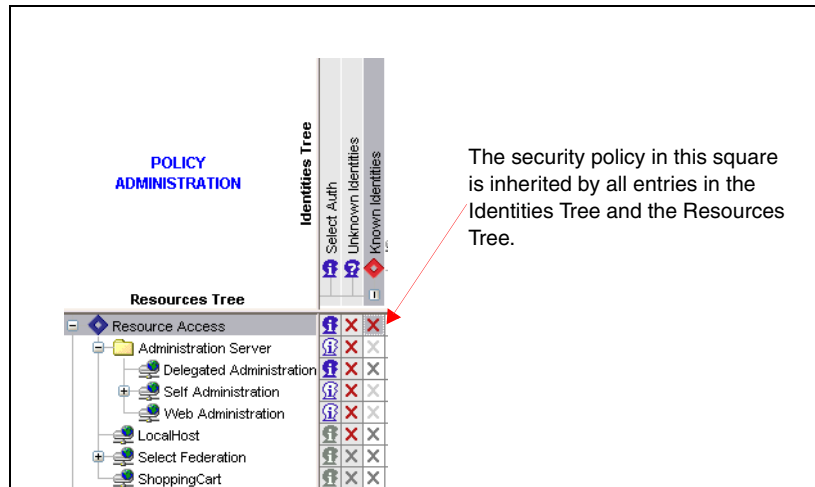


Figure 68 Inheritance Description

- Policies applied to a folder are inherited by all identities and groups in the folder, as shown in [Figure 69](#).

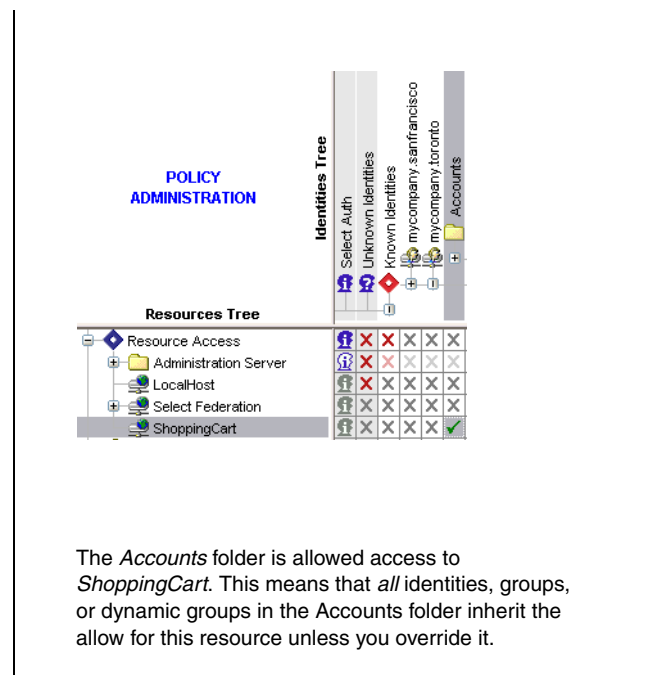


Figure 69 Inheritance Description

- Policies applied for a folder, group, or dynamic group are inherited by all folder, group, or dynamic group members.

This lets you quickly assign the same access policies to multiple identities, as shown in [Figure 70](#). For example, assume you want all members of your administrators group to have access to all Self Administration resources. You therefore create a group called Administrators, add all your corporate administrators to this group, and apply access policies for that group. All the members of the Administrators group automatically inherit the access policies applied for the group. This same inheritance logic applies to dynamic groups as well.

- If the identity belongs to multiple groups to which multiple conditional policies are set against a given resource, the “+” icon appears. In this case, all rules are evaluated until one returns an allow decision.

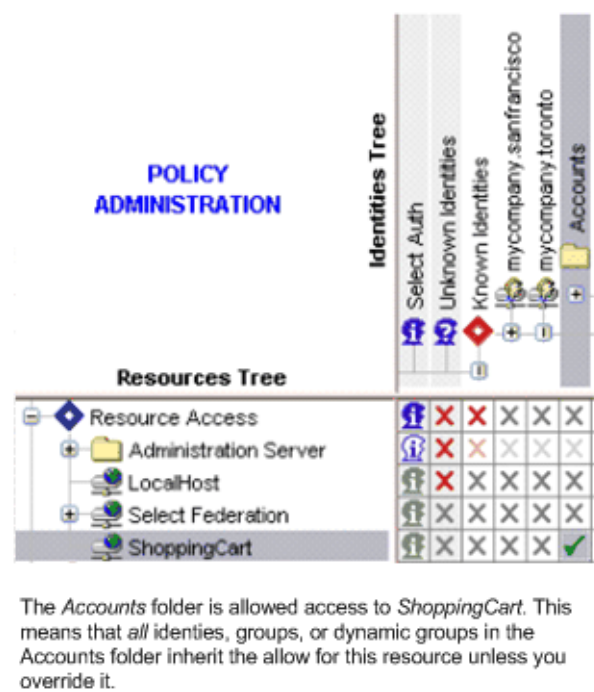


Figure 70 Inheritance Description

- Policies applied to a service (🌐), directory (📁), or folder (📁) are inherited by all of its resources.

For example, if an identity is given access to Corporate intranet, the identity automatically gets access to all resources under that URL, as shown in [Figure 71](#) (such as Index.html and Login.asp). If you want, you can then change the identity’s access to any specific resource. For example, only allow access to the login page, and make remaining pages conditional based on whether or not that identity has been authenticated.

Overriding an Inherited Access Policy

An access policy applied specifically to an entry (such as a folder, group, identity, or resource) always overrides the access policy inherited from the parent entry, as shown in [Figure 73](#).

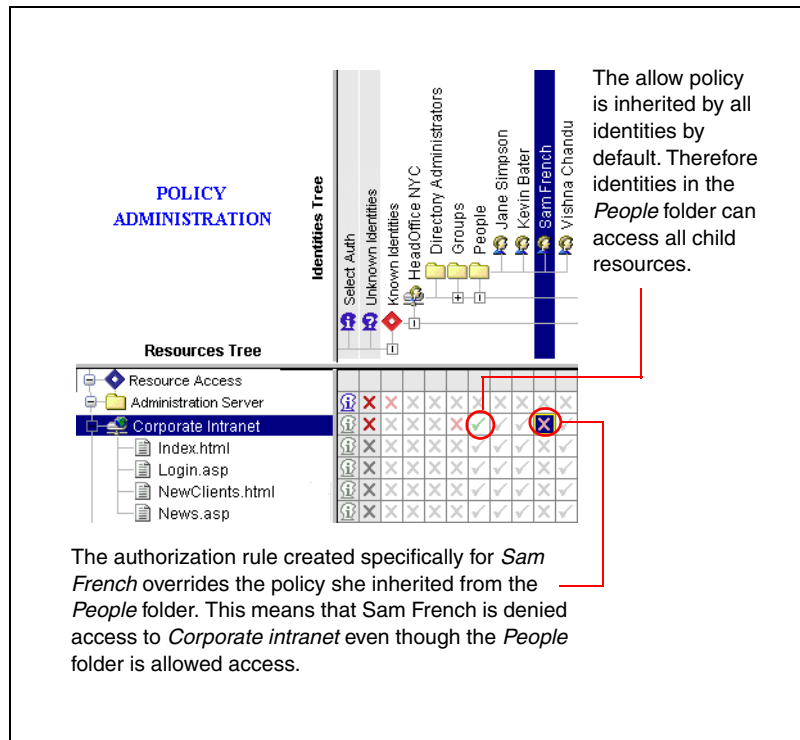


Figure 73 Override Description

When a Pairing Inherits Multiple Access Policies

There are occasions when an identity and resource pairing inherits two or more different access policies. The most permissive of the access policies is always given priority. This means that an access policy allowing an identity access to a resource always overrides an access policy denying the identity access to the same resource.



This rule only applies when inheriting from multiple parents. It does not apply when you create rules specifically for a given identity and resource pairing.

For example, suppose Jane Simpson belongs to both the Employees group and the Senior Executive group. The Senior Executive group is allowed access to the NewClients page, but the Employees group is denied access to the NewClients page.

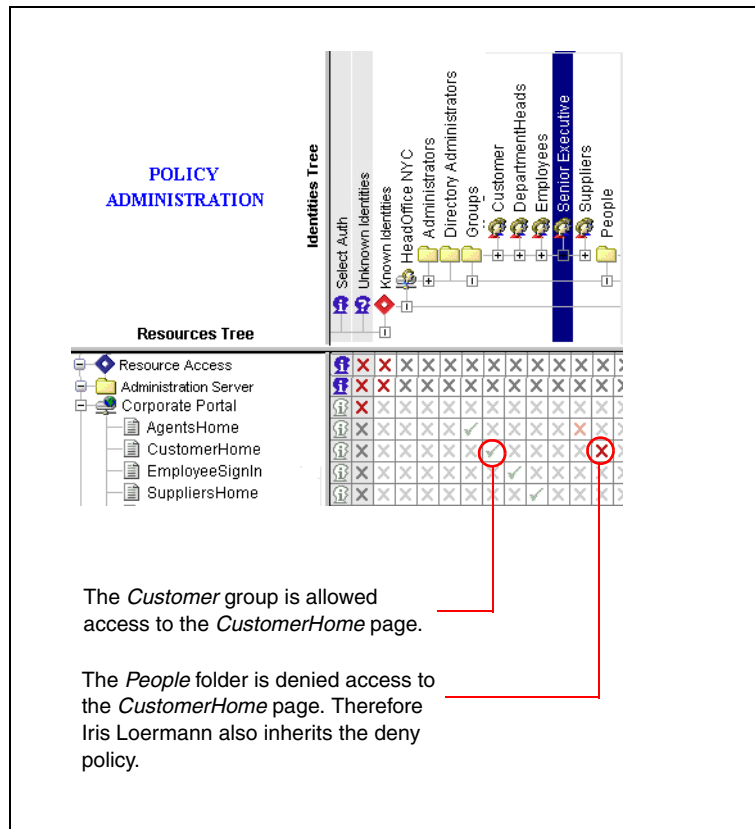


Figure 75 Inheritance Description

Iris Loermann is allowed access to the CustomerHome page because the access policy allowing her access (inherited from the Customer group) overrides the access policy denying her access (inherited from the People folder), as shown in [Figure 75](#).

Tips for Administering Access Policies

When administering your access policies, it is best to apply Deny access policies for top-level entries (such as folders, groups, the root of the Identities Tree, and the root of the Resources Tree), and then apply Allow or Conditional access policies to specific groups or identities. This ensures that inherited Allow access policies do not override inherited Deny access policies. [Figure 76](#) and [Figure](#) illustrate this.

For example, suppose you only want employees to be able to have access to your Corporate intranet. Start by denying everyone access to the web site, then grant access to specific groups.

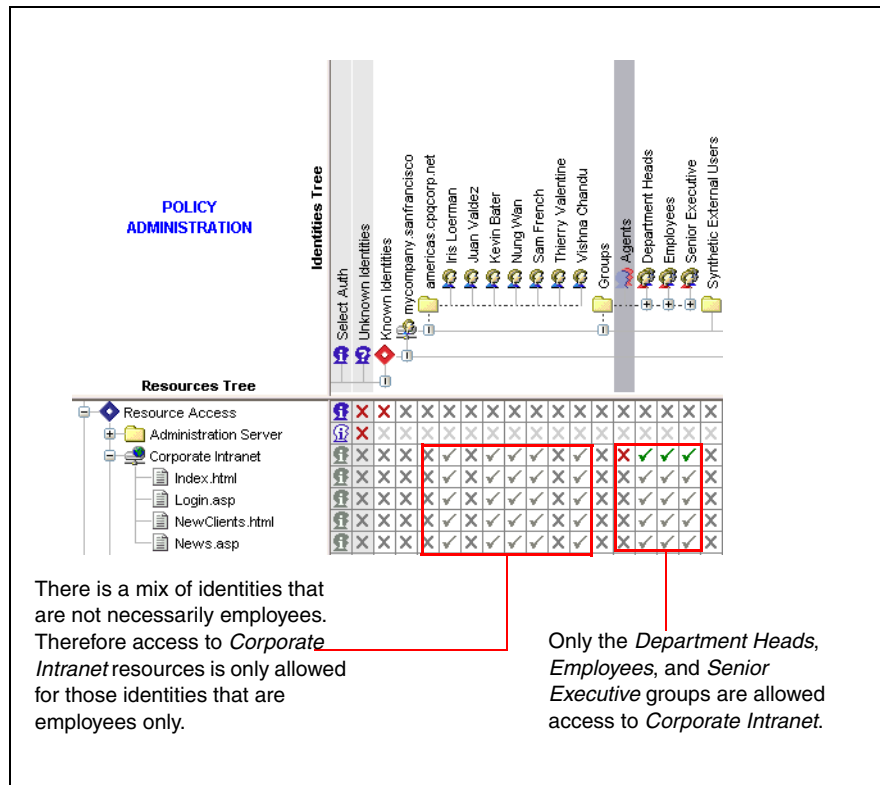
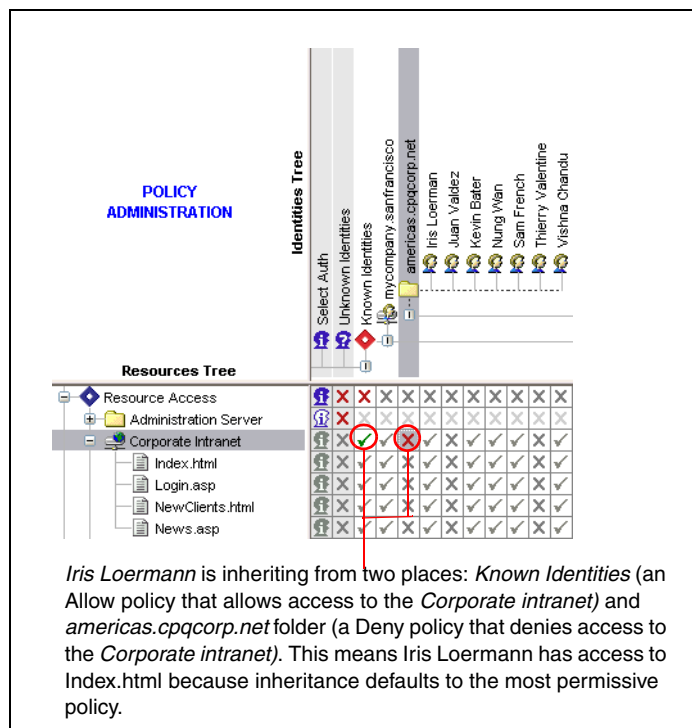


Figure 76 Good Form For Setting Policy

Otherwise, if you initially allow everyone access to the Corporate intranet and then try to deny access to certain groups, the Allow access policies override the Deny access policies.



Bad Form for Setting Policy

8 Managing Identity Profiles

Keeping identity data current is not necessarily the domain of identity administrators alone. Select Access allows end users to manage their own profile data via its profile self-management features.

Chapter Overview

This chapter includes the following topics:

- [Introducing Select Access Management Features](#) on page 141
- [Managing Identities Profiles](#) on page 142
- [Managing End User Passwords](#) on page 144

Introducing Select Access Management Features

Select Access includes features that mitigate administrative expenses by allowing identities to directly manage their own profiles and password. For a summary of these features, see [Table 22](#).

Table 22 Managing User Data Overview

Feature	Details
Identity Profiles : Allows you to create a profile and define preferences against a <i>specific</i> identity.	Managing Identities Profiles on page 142
Password Management : Allows you to manage two levels of password policy: <ul style="list-style-type: none">• The organization-wide password policy• The password preferences you have for a profile	Configuring Password Policies on page 145
Profile Self-Management : Allows you to determine which attributes in the identity profile the end user can self-manage. Whether or not an end user can self-manage these profile attributes is determined by the Profile Self-Management terminal point.	The Profile Self-Management Terminal Point on page 193

Managing Identities Profiles

An identity's profile includes the directory elements that help define the identity of the individual. These directory elements define the types of activities an end user can perform on their own profile.

An identity's profile consists of two things:

- A set of activated attributes that create a profile of that user. If you create a rule with the Profile Self-Management terminal point, you can determine which of these attributes the end user can self-manage. For details, see [The Profile Self-Management Terminal Point](#) on page 193.
 - ▶ Because the identity's password attribute (`userPassword`, `password_id`, etc.) can vary depending on which directory server she is using, you need to change the attribute defined for the **Change Password** button in the `profile_mgmt_form.html` form. For details on the Profile Self-Management form, see [To customize the Profile Self-Management form](#) in the *HP OpenView Select Access 6.2 Network Integration Guide*.
- A subset of the corporate password policy that sets specific self-management preferences for the identity's profile.

To activate the identity's profile and specify password preferences

- 1 Do one of the following:
 - Create a new identity.
 - Modify the properties of an existing identity profile.

For details, see [Manually Adding or Modifying an Identity Profile](#) on page 40.

- 2 In the corresponding **New Identity/Identity properties** dialog box, click the **Profile Management** tab. The tab appears as shown in [Figure 77](#).

Figure 77 New Identity Dialog Box

- 3 Configure the **Password Expiry** settings by clicking any of the following options. Depending on which options you enable, the system automatically determines which combinations are logically allowed.

- **Identity must change password at next login:** The end user must create a new password when he first logs in. The new password must meet the password policy in effect. If you enable this option, the subsequent two options are disabled automatically.

For example, you might set all new identities' passwords to initially be the end users' first initial and full last name (for example, `bjones`). This makes it easy for end users to guess their predefined password when they first log in. However, for security purposes this is not a well-defined password, and is not one that you want them to keep. Therefore, after identities log in for the first time, Select Access ensures that they change the password before they can do anything else on the network. For details on creating a password policy, see [Managing Identities Profiles](#) on page 142.

- **Identity cannot change password:** The end user cannot voluntarily or randomly change the password. Select Access ignores this check box if an involuntary change is pending. The involuntary change happens when at least one of the following scenarios occur:

- You check the **Identity must change password at next login** option.
- You set one or more of the options of **Expiry** tab in the **Password Policy Configuration** dialog box. For details, see [Configuring Password Policies](#) on page 145.

➤ If you enable this option, the **Identity must change password at next login** option is disabled automatically.

- **Password never expires:** Select Access does not force the end user to alter the existing password.
 - If you enable this option, the **Identity must change password at next login** option is disabled automatically.
 - If you enable this setting, it overrides any of the settings of the password expiry policy. For details on creating a password policy, see [To configure password expiry](#) on page 149.
- 4 In the **Password Change** group, type and confirm the default password the end user must enter before accessing the network in the corresponding fields. Depending on what you configured in the **Password Expiry** group in [step 1](#), it is possible the end user will be required to change this password upon login.
- 5 Configure any of the **Profile Status** settings by clicking any of the following:
 - **Profile disabled:** Disables the identity's profile [permanently](#), until the box is unchecked.
 - If the identity's profile is permanently disabled, no one can access the network using this userID and password combination, even if the profile has been reenabled after a number of failed login attempts. For details, see [To configure password expiry](#) on page 149.
 - **Disable profile after idle for:** Disables the identity's profile temporarily if it becomes idle for the configured length of time. Set the idle period in:
 - **Hours:** The allowable range is any numerical value between 0-596523.
 - **Days:** The allowable range is any numerical value between 0-24855.
 - **Weeks:** The allowable range is any numerical value between 0-3550.
 - This box is checked by the system if the session has been idle, or if someone exceeds the number of invalid password entry attempts.

To disable an identity's profile

- 1 Right-click the corresponding identity profile in the Identities Tree and click **Properties**. This displays the **Identity Properties** dialog box.
- 2 Select the **Profile Management** tab.
- 3 Ensure that the **Disable Profile** option in the **Profile Status** group is checked.
 - To enable an identity's profile, ensure that the **Disable Profile** option in the **Profile Status** group is not checked.

Managing End User Passwords

Protecting your network with elaborate security schemes means little if your most basic security scheme (passwords) are ineffectual. The majority of passwords your end users use often do not follow the most tried-and-true password guidelines. But paper-based policies rely heavily on the honor system, and the honor system is destined to fail for a simple reason: user habit. When people have passwords they like, they keep them because they are easy to remember and simple to use. But, habits for your end users equates to vulnerability for your business, because poorly implemented passwords make unauthorized access that much easier.

In recognizing that your overall network security is only as good as your password management policy, Select Access allows you to define robust password policies and provide an enforcement method that guarantees the way end users implement their passwords.



If you have checked the **User cannot change password** box in the **Profile Management** tab of the **Identity Properties/New Identity** dialog for a given user, the identity cannot change his password. None of the policies you create apply to any user who has this setting enabled. For details, see [Managing Identities Profiles](#) on page 142.

Managing user passwords involves performing the following tasks:

- [Setting Up and Maintaining Password Management](#) on page 145
- [Configuring Password Policies](#) on page 145
- [Enabling Password Resets](#) on page 152

Setting Up and Maintaining Password Management

If you intend to enable the password management feature, ensure that you check these two boxes in your Enforcer plugin's **Tuning Parameters** setup screen (they are checked by default when you first install an Enforcer plugin):

- **Login via fill-in form**
- **Enable Web session cookies**

For details, see [Chapter 8, Configuring the Enforcer Plugins](#) in the *HP OpenView Select Access 6.2 Installation Guide*.

If you are disallowing the use of real words, create a text file that acts as your password dictionary:

- Ensure your password dictionary is saved on the same computer as your Policy Validator.
- If your passwords are not ASCII-based, HP recommends that you use a tool like NKF to create a dictionary file.
- Ensure you configure your Policy Validator to use this file via the **Password Dictionary** setup screen.

For details, see [Chapter 7, Configuring the Policy Validator](#) in the *HP OpenView Select Access 6.2 Installation Guide*.

Configuring Password Policies

You can create password policies that allow end users to self-manage their own passwords. Policies can be as rudimentary or robust as you need them to be, by setting policy for password age, size, and uniqueness, and expiry as well as selecting the HTML forms the Enforcer plugin displays to support your policy. The settings you configure combine to enforce strict password policies while allowing your end users the freedom to self-manage their password selection.



Because the identity's password attribute (`userPassword`, `password_id`, etc.) can vary depending on which directory server she is using, you need to change the attribute defined for the **Change Password** button in the `profile_mgmt_form.html` form. For details on the Profile Self-Management form, see [To customize the Profile Self-Management form](#) in the *HP OpenView Select Access 6.2 Network Integration Guide*.

- Identities can only self-manage passwords on Microsoft ADS if the server is running over SSL. Additionally, password lengths must meet the requirements of the directory unless you disable ADS' password policy. For details, see [Active Directory 2003 and Profile Password Setup Problems](#) on page 300.

To enable a company-wide password policy

- 1 Click **Tools** → **Password Policy Configuration**. The **Password Policy Configuration** dialog box appears, displaying four tabs you can configure, as outlined in [Table 23](#):

Table 23 Password Policy Configuration Overview

Password Tab	Details
Strength: This tab allows you to determine rules surrounding the passwords that end users create. If a password does not meet the criteria you set, it is rejected.	To configure password strength on page 147
Expiry: This tab allows you to determine when and how you need to renew passwords.	To configure password expiry on page 149
Failure: This tab allows you to determine why profiles are disabled or re-enabled.	To configure password failure on page 150
Forms: This tab allows you to define the names of the fill-in forms that allow end users to manage their passwords.	To set password policy forms on page 151

- 2 Select any combination of these tabs and configure your preferences for these settings.

- If you are setting password policy for the Administration server Self Administration resources, not all of the settings available in the **Password Policy Configuration** dialog are applicable. The Administration server only recognizes the following settings:

- The **Strength** tab, excluding the **Password must not match identity's last ___ passwords** option.
- The **Expiry** Tab.

In addition, the Administration server does support a password policy dictionary file which lists string combinations that may not be used in a valid password. This file must be named `dictionary.txt`, and must be located in the `<install_path>\bin` directory.

- 3 When you have finished configuring all four tabs that combine to make your single corporate password policy, click **OK**. This stores the password policy in the directory server. All Policy Validators use this password policy from the directory server to evaluate passwords end users submit. If the password provided does not match the criteria of the policy, the Enforcer plugin displays the corresponding form.

➤ If you want the password policy to take effect immediately, flush the Policy Validator's cache. Otherwise, the policy takes effect automatically after the cache refresh interval expires.

To configure password strength

- 1 In the **Password Policy Configuration** dialog box, click the **Strength** tab, as shown in Figure 78.

➤ If you are setting password policy for the Administration server Self Administration resources, the **Password must not match identity's last __ passwords** option is not applicable.

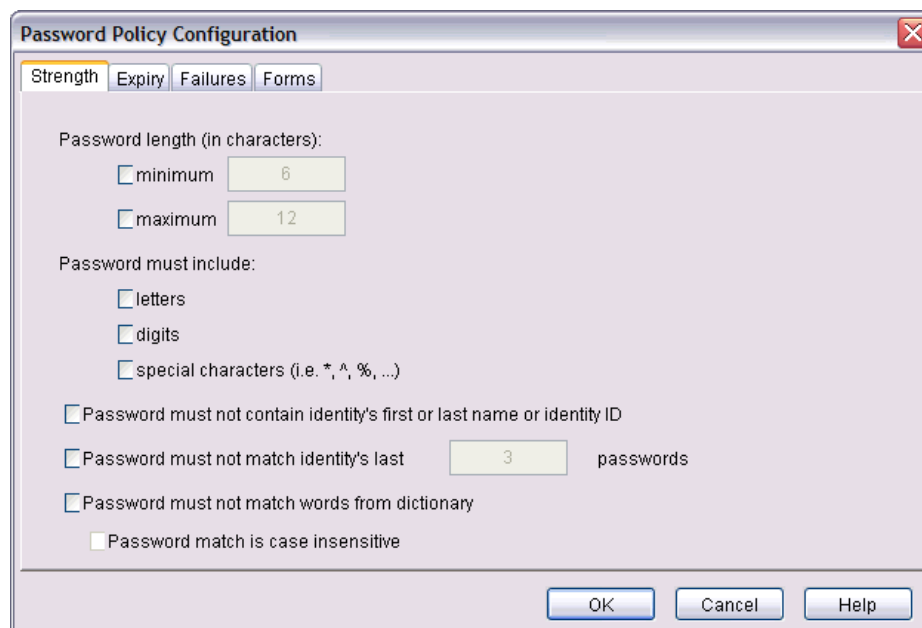
The image shows a screenshot of the 'Password Policy Configuration' dialog box with the 'Strength' tab selected. The dialog has four tabs: 'Strength', 'Expiry', 'Failures', and 'Forms'. Under 'Password length (in characters):', there are two options: 'minimum' with a value of 6 and 'maximum' with a value of 12. Under 'Password must include:', there are three checkboxes: 'letters', 'digits', and 'special characters (i.e. *, ^, %, ...)'. Below these are three more checkboxes: 'Password must not contain identity's first or last name or identity ID', 'Password must not match identity's last' followed by a text box containing '3' and the word 'passwords', and 'Password must not match words from dictionary'. At the bottom, there is a checkbox for 'Password match is case insensitive'. The 'OK', 'Cancel', and 'Help' buttons are at the bottom right.

Figure 78 Password Policy Configuration Dialog Box

- 2 Specify the password's minimum and maximum length in characters. To set a minimum or maximum length, check the corresponding box and enter a numerical value:
 - **Minimum length:** The lowest allowed character limit of a password. If you do not check minimum length, or set minimum length to 0, then no minimum length is required.

For example if you set a password's minimum length to four, and the end user submits "Me2" as the password, Policy Validator evaluates the password as being too short, therefore the password generates an error indicating it has fallen below the allowed lower limit. In this case, the end user needs to resubmit an alternative password that meets the configured criteria.



The longer the password, the more difficult it is for a potential intruder to guess it. However, if you set the password's minimum length to a value higher than seven, the more difficult it becomes for end users to remember. The more difficult it is for them to remember, the more likely it is that they might record it.

- **Maximum length:** The highest allowed character limit of a password. If you do not check maximum length, or set maximum length to 0, then no maximum length is required.

For example, if you set a password's maximum length to 8, and the end user submits "\$\$Talks2MeNU" as the password, Select Access evaluates the password as being too long. Therefore, the password generates an error indicating it has exceeded the allowed upper limit. In this case, the end user needs to resubmit an alternative password that meets the configured criteria.

- 3 Configure the password's uniqueness preferences. To enable any password uniqueness settings, click the corresponding box and enter a value as needed:

- **Password must include letters/digits/special characters:** The alphanumeric character types that must be combined within a password: letters (aA to zZ), digits (1 to 9), special characters (dependent upon the locale of your network. US English special characters include characters like #, @, or ?). If you disable any of these options, the end user does not need to create a password using those characters.

For example, if you create a policy for password uniqueness that requires end users to combine all three character types, and the end user submits "MonKeY", the Policy Validator evaluates the password as being invalid. Therefore, the password generates an error indicating it requires special characters before it is valid. In this case, the end user needs to resubmit an alternative password that meets the configured criteria.



The more diverse character mix you require, the more secure user passwords are generally perceived to be.

- **Password must not include identity's first or last name or identity ID:** The end user's given name, family name, UID, CN, or `samaccountname` are not allowed within a password.

For example, if you enable this setting, and an identity named Jane Doe submits "KnowJDoe?", the password is not accepted. In this case, the end user needs to resubmit an alternative password that meets the configured criteria.



Select Access only enforces this restriction case sensitively. That is, if you check this box and an identity's `givenname` attribute is set to Jane, the end user cannot use "Jane" within her password. However, the Policy Validator does allow the end user to use "jane" instead. For example, "aJanetor" is disallowed while "ajanetor" is.



ADS directories have a maximum string limit of 64 unicode characters for the `givenname` attribute.

- **Password must not match identity's last passwords:** The password must not match the configured number of passwords stored in the password history for that user. The end user cannot re-use passwords in that history.

- **Password must not match words from dictionary:** Check this box if you want a password dictionary file to validate user passwords. Words included in the dictionary text file are prohibited words that are not allowed as a password. You can add words to the dictionary or create a new dictionary file.

For example, if the word “doctor” and the end user submits “doctor”, the password is rejected. In this case, if the end user resubmits the password as “DRiiii”, it is accepted because nothing in that password exists as a word in the dictionary.

- **Password match is case insensitive:** Check this box if you want password dictionary word matching to be case-insensitive.

➤ The password dictionary is configured when you set up your Policy Validator. For details, see [Chapter 7, Configuring the Policy Validator](#), in the *HP OpenView Select Access 6.2 Installation Guide*.

To configure password expiry

- 1 In the **Password Policy Configuration** dialog box, click the **Expiry** tab.

- When the password expires, the Enforcer plugin displays an HTML form that forces the end user to change her password. The password that the end user changes is the password that corresponds to the one stored in his identity profile on the directory server.
- If you are using NTLM or Kerberos authentication, and want the end user to be able to modify her Windows domain password, then you must meet the following conditions: you must be using an Active Directory server, the Policy Validator and the Windows 2000 domain controller must be using the exact same identity location, and use SSL to connect.

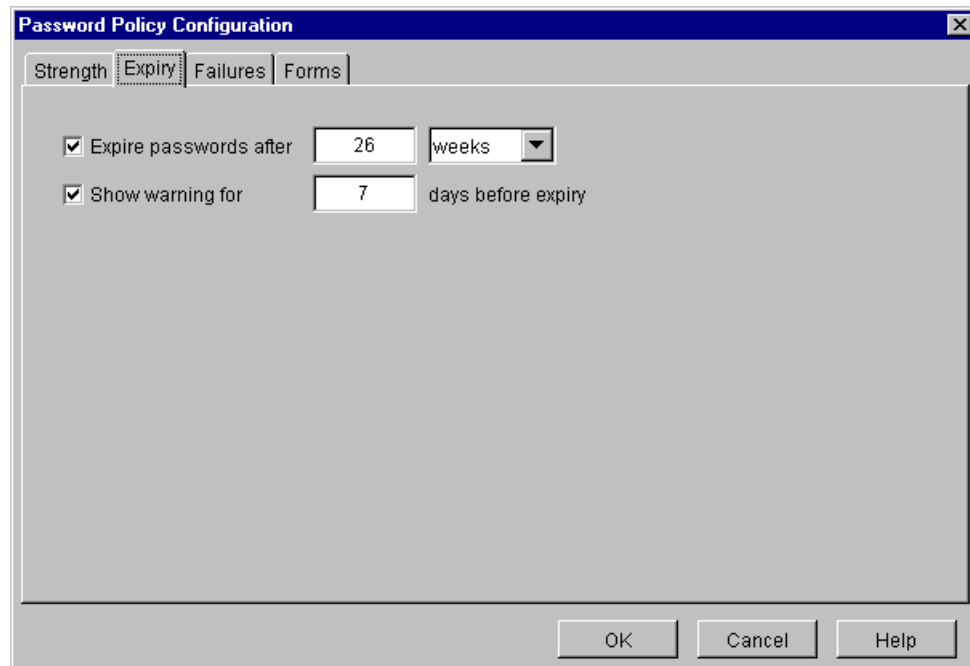


Figure 79 Password Policy Configuration Dialog Box

- 2 Set the maximum age of the password, click the **Expire passwords after** box, and set the age of the password. Password expiry takes effect from the last time the end user has modified a password. You can set the age of the password in:

- **Days:** The allowable range is any numerical value between 1-24855 days.
 - **Weeks:** The allowable range is any numerical value between 1-3550 weeks.
- You must enter a value greater than 0. You cannot use 0 to disable failed login limits. To disable password expiry, uncheck this box. HP recommends you always enable this option; otherwise, end users are allowed to use their original password indefinitely, which can increase the security risk to your network.
 - If the password has expired and the end user has not supplied a new password, she is not able to authenticate herself, and consequently is not able to access the network.
- 3 If you want to warn end users that their current password is about to expire, click the **Show warning for** box, and specify the number of days that the end user is given advance notice.
- If you do not check this box, or set the value in days to 0, end users are not warned of impending expiry dates.

To configure password failure

- 1 In the **Password Policy Configuration** dialog box, click the **Failure** tab, as shown in [Figure 80](#).
- If you are setting password policy for the Administration server Self Administration resources, this tab is not applicable.

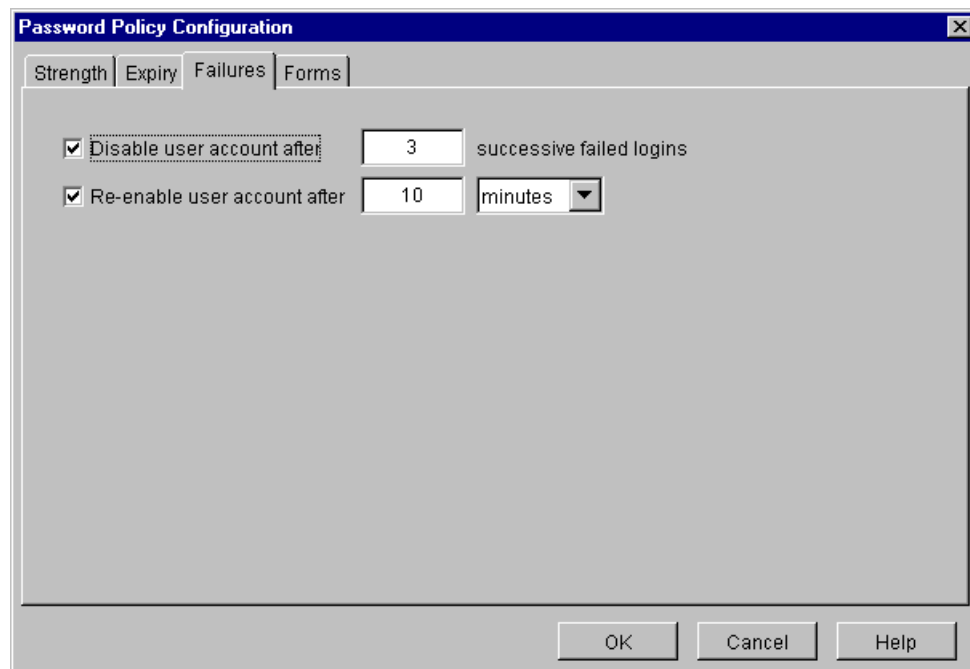


Figure 80 Password Policy Configuration Dialog Box

- 2 Specify the number of failed logon attempts that can occur before the profile is locked out, by selecting the **Disable user profile after** check box and setting a reasonable numerical value.
 - You must enter a value greater than 0. You cannot use 0 to disable password expiry. To disable password expiry, uncheck this box. HP recommends you always enable this option; otherwise, anyone can have unlimited login attempts, which can increase the security risk to your network.
- 3 Specify the amount of time that must pass before a profile that has been disabled by the configured number of login attempts is enabled once more. Select the **Re-enable user profile after** check box and set the window in which a profile remains locked out. Set the lockout period in:
 - **Minutes:** The allowable range is any numerical value between 1-35791394.
 - **Hours:** The allowable range is any numerical value between 0-596523.
 - **Days:** The allowable range is any numerical value between 0-24855.
 - **Weeks:** The allowable range is any numerical value between 0-3550.
 - If you do not check this box, or set the reenabling time to 0, you permanently disable all profiles with failed login attempts.
 - If the profile is reenabled and the end user cannot log in, check to see that her profile has not been permanently disabled.

To set password policy forms

- 1 In the **Password Policy Configuration** dialog box, click the **Forms** tab, as shown in [Figure 81](#). The password forms you configure are needed to support the policy you have set using the other tabs of the **Password Policy Configuration** dialog box.
 - If you are setting password policy for the Administration server Self Administration resources, this tab is not applicable.

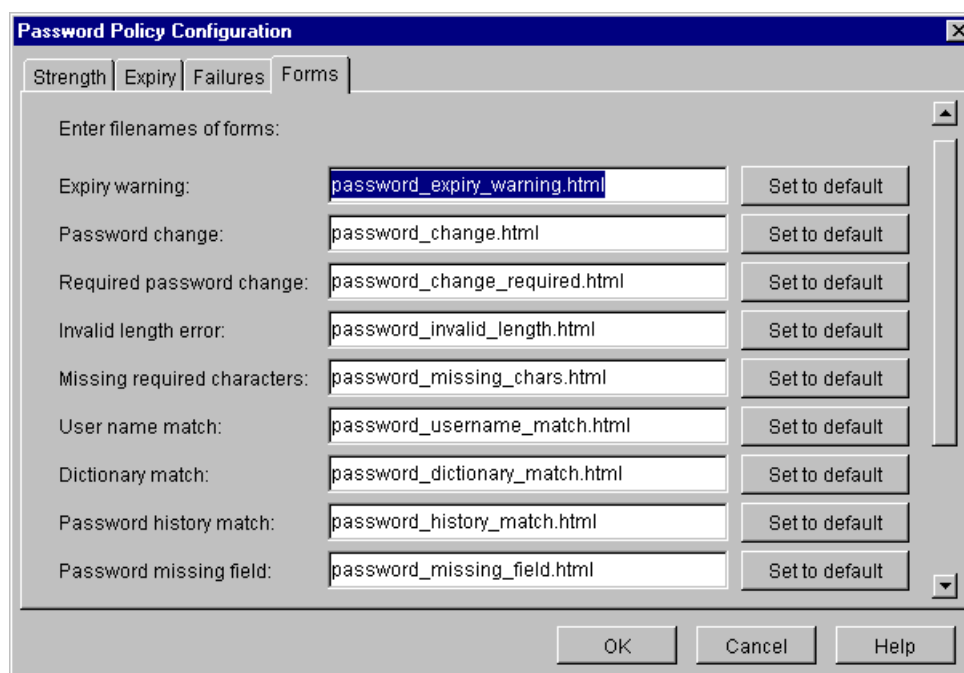


Figure 81 Password Policy Configuration Dialog Box

- 2 Type the name of the password login form used to authenticate identities. You can use the default form, or you can specify an alternative name for a form you have customized.
- 3 Revert to the default form at any time, by clicking **Set to default**.
 - Save a copy of these forms on your web server. Otherwise, the Enforcer plugin is unable to display the forms your configured forms. The original templates for these forms are installed to the following directory by default: `<install_path>/content/`. For more details on customizing these forms, see [Customizing Select Access Forms and Messages](#) in the *HP OpenView Select Access 6.2 Network Integration Guide*.

To disable company-wide password policies

- 1 Disable all settings and/or set all values in the dialog box to 0 (or delete them).
- 2 Click **OK** to save these settings.
 - Ensure this new policy is updated on all Policy Validators. For details, see [Configuring Password Policies](#) on page 145.

Enabling Password Resets

The Password Reset function allows administrators to determine when and how end users can change passwords if they are forgotten. Because it is an administrative mechanism, Password Reset appears as a new function on Resources Tree as part of the Administrative Access – Functions branch.

The responsibility of configuring and managing passwords via the reset function is shared between administrators and end users. Once an administrator sets up the policy, the end user can self-manage:

- **Answers:** to the secret questions that authenticate the identity from a list defined by the administrator. The Administration server randomly chooses which questions are displayed to the end user. Only the authenticated user can modify answers as part of profile attributes in their user profile.

The questions that appear to the end user may be shared across your all identities in your identity data location. However, the answers the end user provides are unique the user's individual profile. Note that Select Access prevents administrators from modifying answers themselves.

- **The password:** that logs the end user onto the system. End users can only change the password after they authenticate themselves via a series of secret questions and answers and only if the administrator gives the end user the required entitlement to self-manage the password in their profile.

➤ The Password Reset policy also can enable disabled profiles. For example, if a user's identity profile is disabled because of too many failed login attempts, and the end user successfully resets the passwords in that profile, the profile is automatically re-activated.

➤ An administrator with the appropriate entitlement delegated to them can configure a Password Reset policy. If there are workflow rules for this function, changing the configuration will trigger the workflow rules as well.

However, workflow is not triggered by changes made by end users on the registration and/or profile self-management pages. This is because the directory attributes used are internal attributes and cannot be used with workflow rules.

To use the Password Reset feature, you must follow the procedure listed in [Table 24](#).

Table 24 Enabling the Password Reset Feature

Setup Task	Details
1 If you have not already done so, configure the Administration server to display the appropriate resource to end users who can reset their passwords. You configure the Administration server with the Setup Tool.	Chapter 5, Configuring the Administration Server in the <i>HP OpenView Select Access 6.2 Installation Guide</i>
2 To manage password reset properties, create the Password Reset policy that controls what the end user sees in that resource. End users cannot manage Password Reset properties until the administrator configures and thereby activates the function.	To configure the password reset policy on page 154

Table 24 Enabling the Password Reset Feature

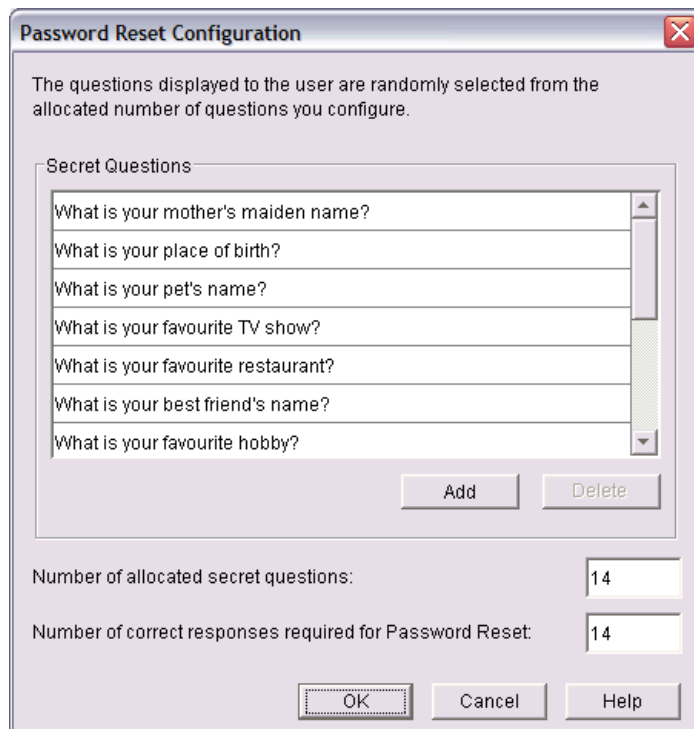
Setup Task	Details
3 Manually add a link to the Password modify password login and/or portal pages to include a link for password resets, using the URL you configured.	<p>The URL for the password reset JSP uses the following syntax:</p> <pre>https://<admin_server>:9992/ password_reset/reset.jsp</pre> <p>Note: Only after the identity is authenticated, does the person get redirected to the reset page.</p>
4 Modify the password reset JSP page to include any business-driven requirements. For example, adding redirect back to your Home page.	Site-specific
5 Because you cannot configure workflow on password resets themselves, you may want to modify your Audit Settings to capture any events or messages you require.	A new audit Component , Password Management, is available in the Audit Entry dialog box. Set the appropriate severity level for this component as needed. For details, see Chapter 13, Changing Audit Settings .

To configure the password reset policy

The Password Reset configuration provides a list of secret questions and other options related to resetting a password.

- 1 Run the Policy Builder and click **Tools** → **Password Reset Configuration**. The **Password Reset Configuration** dialog box appears.

► You can only configure a single reset policy for all user passwords.



Password Reset Configuration

The questions displayed to the user are randomly selected from the allocated number of questions you configure.

Secret Questions

- What is your mother's maiden name?
- What is your place of birth?
- What is your pet's name?
- What is your favourite TV show?
- What is your favourite restaurant?
- What is your best friend's name?
- What is your favourite hobby?

Add Delete

Number of allocated secret questions: 14

Number of correct responses required for Password Reset: 14

OK Cancel Help

Figure 82 Password Reset Configuration Dialog Box

- 2 Define a pool of questions by adding them to or deleting them from the editable **Secret Questions** list box. Use the corresponding buttons provided for this task.

These secret questions are randomly selected by the Administration server and displayed to the end user in the JSP page for resets. The number of questions must be equal to or greater than the number of questions to be displayed to the individual.

- a In the **Number of allocated secret questions** box, enter the number of questions you want to display to the end user. The number of questions must be equal to or greater than the number of correct answers you will be configuring in [step b](#).
- b In the **Number of correct responses required for password reset** box, enter the number of correct answers the end user must supply before the password they give is reset by the system. The number of correct responses must be less than or equal to the number of questions displayed to the individual, which you configured in [step a](#).

➤ Select Access prevents administrators from altering the answer to the questions the end user provides. Administrators can only alter the secret questions.

- 3 Click **OK** to commit your changes.

Understanding End Users' Answer Requirements

Depending on whether or not the end user is a new identity or a previously-registered one, the individual must meet specific criteria as described below:

- New (unknown) users initially set up the answers to the secret questions in the registration page. They can use any combination of characters or numbers to create their answer.
 - ▶ Empty answers cannot be submitted to the identity's profile. Because, asterisks (*) (or asterisks with spaces) are treated as an empty field, they are also not accepted by Select Access.
- Existing (known) users with a profile can set up the answers to the secret questions in the profile self-management page. Like new users, existing users can use any combination of characters or numbers to create their answer. Pre-existing answers are masked by a series of asterisks; known users can indicate "no change" by leaving the masked entry unchanged.
 - ▶ However, if users add another character like "A" to a masked answer, they permanently change the answer to something like "A*****" -- not "A<old_answer>". Ensure you communicate this risk to your identities.

9 Creating Conditional Access Rules with the Rule Builder

A conditional access rule is a way of graphically describing the logic flow of evaluation criteria or behavior. This chapter describes how you can use the Rule Builder to create these conditional rules.

Chapter Overview

This chapter includes the following topics:

- [Introducing the Rule Builder](#) on page 157
- [What Can Conditional Policy Rules Do?](#) on page 158
- [How Do Conditional Policy Rules Work?](#) on page 158
- [Before You Begin](#) on page 161
- [Creating a Rule](#) on page 161

Introducing the Rule Builder

You can display the Rule Builder by:

- Clicking **Tools** → **Rule Builder** in the Policy Builder.
- Right-clicking a cell in the Policy Matrix, and choosing select **Create/Modify Conditional Rule** or **Create/Modify Workflow Rule**.



The cookie used to save the last configuration of the Policy Builder includes details on the Rule Builder's frame size. To reset frame sizes, we recommend you delete this cookie.



Do not open multiple instance of the Rule Builder utility from the Policy Builder applet. This can cause the Policy Builder freeze or behave unpredictably.

[Figure 83](#) describes the different elements of the Rule Builder.

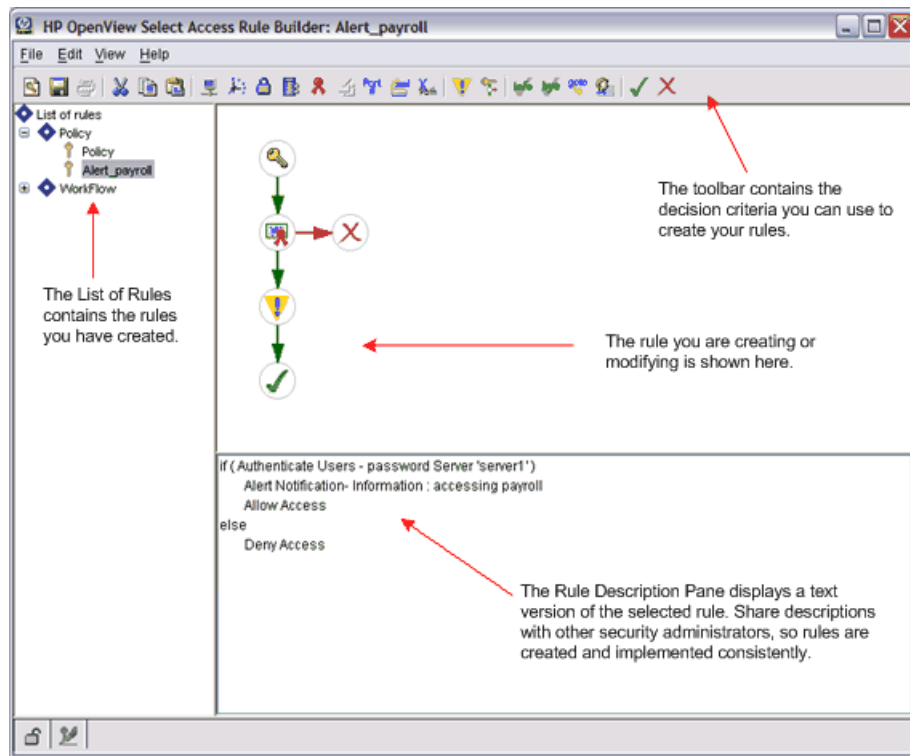


Figure 83 Rule Builder Overview

What Can Conditional Policy Rules Do?

Conditional policy rules are a way of:

- Creating and defining a specific set of conditions that a known user must meet, before a decision is made to allow or deny access to a resource.
- Triggering a certain action to be performed, such as self-manage profiles, redirect to a new URL, and so on.
- Specifying an alternate authentication method when:
 - Select Auth is disabled.
 - There is insufficient information to determine an identity.

How Do Conditional Policy Rules Work?

When an identity requests access to a resource, the Enforcer plugin intercepts the request and forwards it to the Policy Validator. The Policy Validator checks to see what policy is assigned to that resource and user combination. If the policy is a conditional access, the Policy Validator evaluates the request to see whether it meets the criteria for access.

Figure 84 summarizes the components of a rule and how they work together to create an entire decision tree.

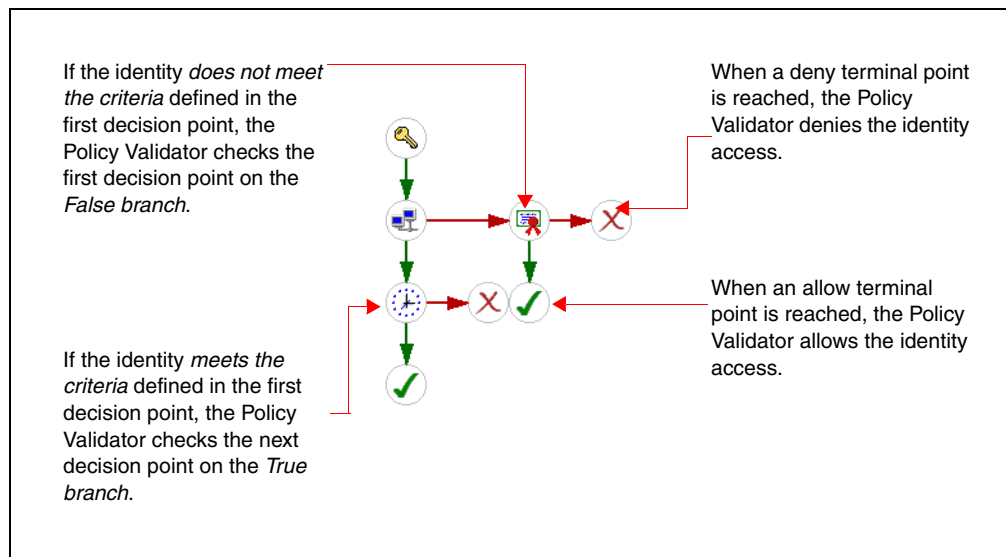


Figure 84 How Rules Are Processed

When a resource request reaches a decision point, it is checked against the criteria you have configured for that point. There are two results:

- **If the request matches the criteria:** It is considered true and follows the true branch of the access rule to the next decision point. True branches can contain other decision points containing criteria to an allow terminal point or to a deny terminal point.
- **If the request does not match the criteria:** It is considered false and follows the false branch of the access rule to the next decision point. False branches can contain other decision points containing criteria to an allow terminal point or to a deny terminal point.

Depending on how you have built your rule, access is ultimately allowed, denied, or redirected.

What is a Decision Point?

A decision point is the Rule Builder counterpart to the Policy Validator decider plugin. It is displayed as a graphical “node” that represents criteria to be evaluated this Policy Validator plugin. The Policy Validator uses each configured plugin to evaluate specific criteria until a terminal point is reached. You can add decision points to the Rule Builder by creating your own plugins and uploading them to the directory server. For details, see the *HP OpenView Select Access 6.2 Developer’s Tutorial Guide*.

At any decision point, you have two decisions to make:

- What happens after the decision point evaluates true?
- What happens after the decision point evaluates false?

You can use any of the following decision points, as described in [Table 25](#).

Table 25 Decision Points Overview

Decision Point Description	Configuration Details
 Evaluates the identity's network address or domain name.	The Networks and Domains Decision Point on page 165
 Evaluates the time of day when the identity is attempting to access the resource.	The Time of Day Decision Point on page 167
 Evaluates the identity's encryption level.	The Encryption Level Decision Point on page 169
 Evaluates identity's directory attributes.	The Directory Attributes Decision Point on page 170
 Evaluates the identity's authentication credentials.	The Authentication Properties Decision Point on page 173
 Evaluates the port the identity is attempting to access.	The Ports Properties Decision Point on page 174
 Evaluates the Policy Validator's query attributes.	The Query Attributes Decision Point on page 176
 Evaluates the Policy Validator's query elements via an XPath expression.	The XPath Decision Point on page 180
 Sends an alert notification to the administrator when an identity reaches this point in a rule.	The Alert Notification Decision Point on page 183
 Inserts another rule within the current rule.	The Insert Subrule Decision Point on page 184
 Evaluates and forwards user attributes, so the Citrix NFuse server can determine which personalized content to display.	The Citrix Decision Point on page 186
 Evaluates when administrative changes the Policy Matrix must be approved other administrators. You can add multiple workflow decision points to a single rule.	The Workflow Decision Point on page 187

What is a Terminal Point?







A terminal point determines the end of the rule and provides an outcome for the evaluated branch. Terminal points control whether or not the resource request is allowed or denied.



You can use all terminal points on either true or false branches.

You can use any of the following terminal points, as described in [Table 26](#).

Table 26 Terminal Points Overview

Terminal Point Description		Configuration Details
	A Custom response. It enables you to provide customized resources to identities, regardless of whether they are authenticated or unknown identities.	The Custom Response Terminal Point on page 189
	An allow with logout. It indicates that the identity meets all evaluation criteria and has been authorized for access, and is explicitly logged out.	The Logout Identity Terminal Point on page 190
	Redirect an identity to an alternate URL based on the identity's level of authentication.	The Redirect Terminal Point on page 191
	Enables profile self-management to allow an end user to self-manage their identity profile.	The Profile Self-Management Terminal Point on page 193
	An allow indicates that the request meets all evaluation criteria and has been authorized for access.	The Allow and Deny Terminal Points on page 195
	A deny indicates that the request has not met one or more evaluation criteria and has been denied access.	The Allow and Deny Terminal Points on page 195

Before You Begin

Before you begin creating your rules, you need to think about your security needs, and answer the following questions:

- What number of rules do you need to create so they define decision criteria clearly? This is important so that Policy Validator can evaluate identities accurately based on your business needs.
- Under which conditions will one rule be used over another?
- How do you create rules so they include an authentication properties decision point logically?

Creating a Rule

To create a rule, begin with an empty tree and add decision points to it. There are two types of rules you can create:

- A single branch rule, where false branches are immediately terminated with the appropriate terminal point
- A multibranch rule, where decision points and action points are placed on both the true and false branches to help you capture more advanced decision-making logic

The figures below illustrate the differences between these two rules.

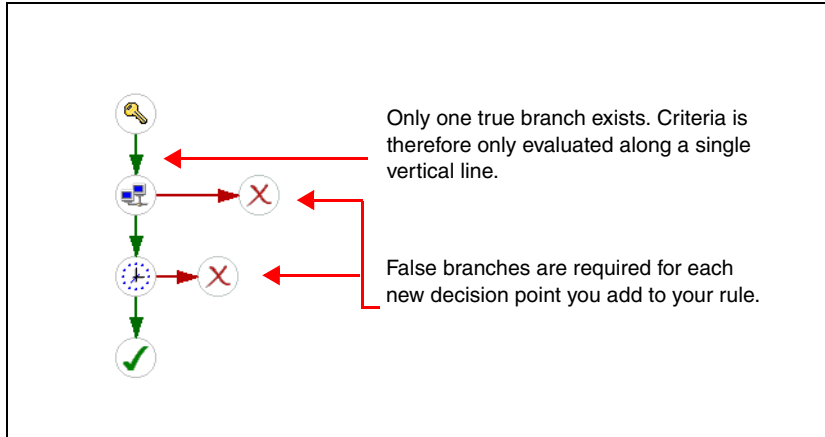


Figure 85 Single Branch Rule Overview

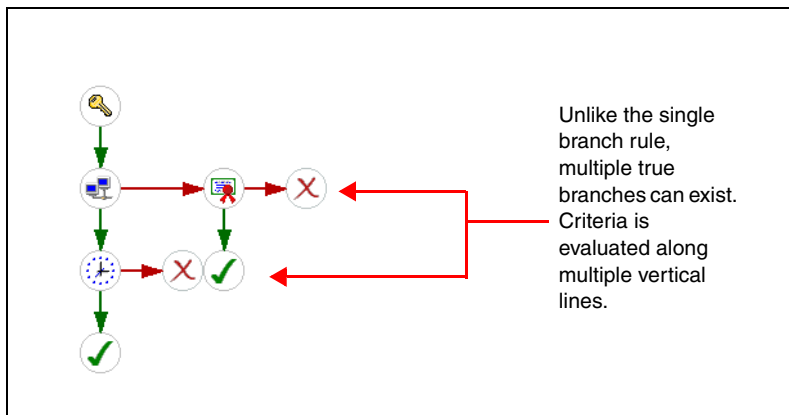


Figure 86 Multibranch Rule Overview

Working with Rules


You can either create a new rule that captures your specific business logic, or modify one you already created. Typical actions you can perform in the Rule Builder include:

- Creating a new rule to capture new business logic.
- Copying an existing rule and changing it to capture slightly different business logic you require.
- Modifying a rule when the business logic it contains is no longer sufficient.
- Saving a rule after it has changed.
- Printing a rule to create a hardcopy record of it.

➤ If one or more administrators are adding, modifying, and deleting rules, refresh your Policy Builder regularly to ensure the list of current rules are correct. For details, see [To refresh data](#) on page 42. If you do not refresh your data regularly, the Policy Builder prompts you to do so when needed.

➤ You cannot name a rule “Allow” or “Deny”. These names are reserved by Select Access.

To create a new policy rule

- 1 Click **File** → **New Rule**. The **Create New Rule** dialog box appears.
- 2 Select the **Policy** rule type and enter a name for the rule and click **OK**.
 You cannot use a comma (,), semi-colon (;) or double quotes (“ ”) in a rule name. They are invalid characters, and Rule Builder does not accept them.
- 3 Select a decision or terminal point from the Rule Builder toolbar by clicking its respective icon. A properties dialog for the selected decision point appears.
- 4 Configure the properties for it. For details, see:
 - To configure a [networks and domains decision point](#) on page 166
 - To configure a [Time of Day decision point](#) on page 168
 - To configure an [Encryption Level decision point](#) on page 169
 - To configure a [Directory Attributes decision point](#) on page 171
 - To configure an [Authentication Properties decision point](#) on page 173
 - To configure a [Ports Properties decision point](#) on page 175
 - To configure a [Query Attributes decision point](#) on page 177
 - To configure an [XPath decision point](#) on page 180
 - To configure an [Alert Notification decision point](#) on page 184
 - To configure an [Insert Subrule decision point](#) on page 185
 - To configure a [Citrix decision point](#) on page 186
 - To configure a [Workflow decision point](#) on page 187
- 5 Add the decision point to the a branch of the rule. To add any decision or terminal point to a branch:
 - a Move your cursor to the insertion point of your rule. When you have moved the decision point to a valid insertion location, the branch arrow is highlighted.
 - b Click to insert the decision point or terminal point at that location.
- 6 Repeat [Step 3-Step 5](#) to add any additional decision or terminal points.

To copy an existing rule

You can create a new rule by copying an existing rule.

- 1 In the **List of rules**, right-click a rule, then click **Save As**. The **Save Rule As** dialog box appears.
- 2 Enter a name for the rule and click **OK**.
- 3 Add decision points and terminal points as required.

To modify a rule

- 1 In the **List of rules** list, click the rule you want to modify. The rule tree is shown on the right side of the window.

- 2 Add, modify, or delete decision points and terminal points as required.



You can also double-click a key icon in the Policy Matrix to launch Rule Builder and modify the rule.

To delete a rule

- 1 If necessary, start Rule Builder by clicking **Tools** → **Rule Builder** in Policy Builder.
- 2 In the **List of rules** list, right-click a rule, then click **Delete**.

To save a rule

- To save the current rule:
 - a In the **List of rules** list, select a rule.
 - b Click **File** → **Save**. This saves the rule on the directory server being used as the Policy Store.
- To save all rules, select **File** → **Save All**. This saves all rules to the directory server being used as the Policy Store.
- To save a rule with a different name:
 - a In the **List of rules** list, select a rule.
 - b Click **File** → **Save As**. The **Save Rule As** dialog box appears.
 - c Enter a name for the rule and click **OK**. This saves the rule on the directory server being used as the Policy Store.



You cannot name a rule “Allow” or “Deny”. These names are reserved by Select Access.

To print a rule

- 1 In the **List of rules** list, click the rule.
- 2 Click **File** → **Print**.

Working with Decision Points

Like rules, you can modify the logic of a decision point you have already created. Typical actions you can perform on a decision point include:

- Creating a new decision point to capture new business logic.
- Copying and pasting an existing decision point and changing it to capture slightly different business logic you require.
- Modifying a decision point when business logic it contains is no longer sufficient.
- Deleting a decision point that is no longer needed.

To create a decision point

- 1 Click the toolbar icon that corresponds to the decision point you want to add. For details, see [What is a Decision Point?](#) on page 159.

- 2 Configure the properties for it.
- 3 Click **OK** and drag the cursor to a suitable place in the rule you want to add it to.

To copy and paste decision points

- 1 Right-click a decision point, then click **Copy**.
- 2 Right-click the arrow where you want to paste the new decision point, then click **Paste**.

To modify a decision point

- 1 Right-click the decision point and then click **Properties**. Alternatively, double-click the decision point.
- 2 Modify the decision point and then click **OK**.

To delete a decision point

- 1 Right-click the decision point, then click **Delete**. If the decision point has subordinate decision points attached to the true and false arrows, a confirmation dialog box appears.
- 2 Do one of the following:
 - To delete only the selected decision point, select **Delete only this decision point?** and click **OK**.
 - To delete all subordinate decision points as well, select **Delete this decision point and all sub-decision points?** and click **OK**.

The Networks and Domains Decision Point

A Networks and Domains decision point allows you to check the identity's network address to ensure the identity is coming from an allowed location. You can enter one of the following:

- You can enter a specific hostname. For example:
`www.mycompany.com`
`trial.mycompany.com`
 - You can use a wildcard (*) as the first part of a domain name. For example, to check the entire `mycompany.com` domain, you enter `*.mycompany.com`. This ensures all hosts in the domain (`www.mycompany.com`, `sales.mycompany.com` and `trial.mycompany.com`) are checked.
 - You can enter an exact IP address. For example:
`10.10.10.10`
 - You can enter a network address by entering an IP address and netmask. For example:
`10.10.10.0/255.255.255.0`
- The network address you enter must exactly match the address sent to Policy Validator. Domain name resolution is not performed on IP addresses.
 - This decision point does not work on all platforms. This is due to performance issues when doing reverse DNS lookups for Enforcer plugins.

For example, an administrator might choose to combine this decision point with a time of day decision point to restrict access to the company intranet to computers on the company network and only during regular business hours, as shown in [Figure 87](#).

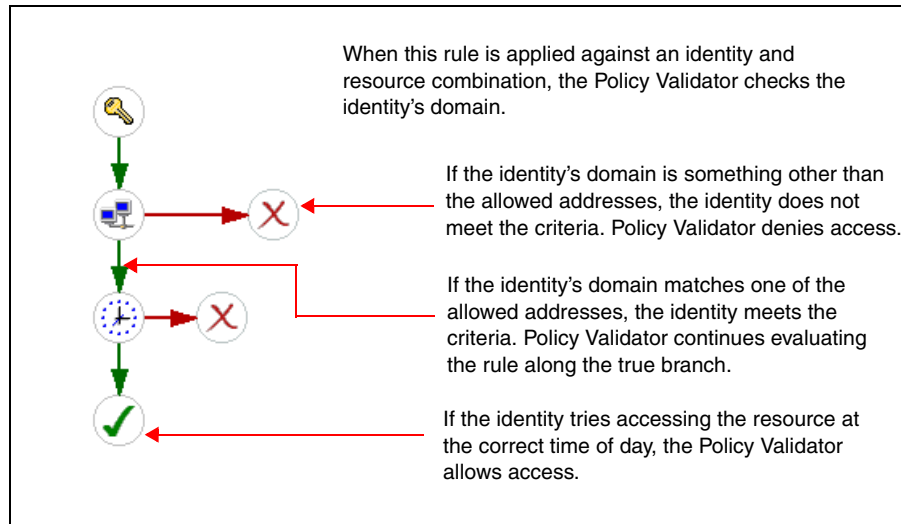



Figure 87 Example Networks and Domains Rule

To configure a networks and domains decision point

1 Do one of the following:

- To add a Networks and Domains decision point, select  from the toolbar.
- To modify a Network and Domains decision point that already exists, right-click the existing Network and Domains decision point and select **Properties**.

The **Networks and Domains Properties** dialog box appears, as shown in [Figure 88](#).

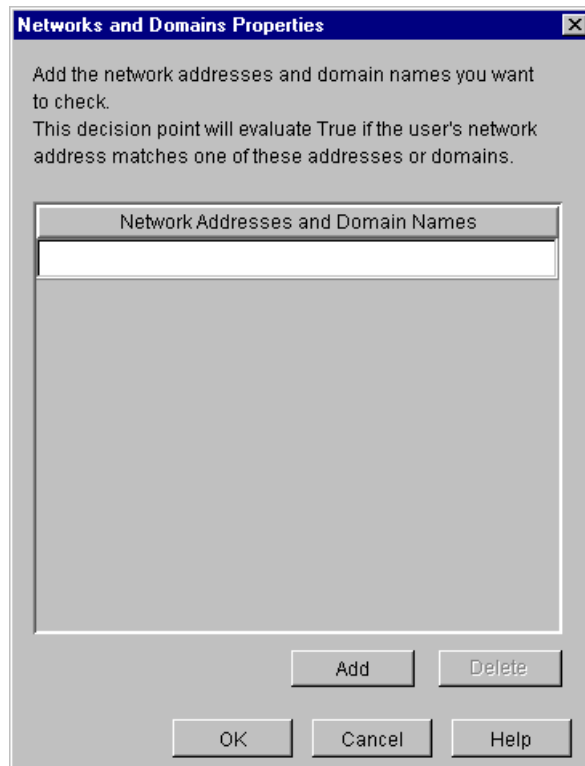


Figure 88 Networks and Domains Properties Dialog Box

- 2 Enter a network address in the row provided.
- 3 If you need to create multiple addresses, click **Add** and then enter an address for each row you have added.
- 4 To delete a network address, select the corresponding row for the address you want to delete, and click **Delete**.
- 5 Click **OK**.

The Time of Day Decision Point

A Time of Day decision point allows you to specify the time of day that an identity can access a resource and when they cannot.

For example, an administrator might want to prevent the identity who arrives to work unusually early from accessing company assets on their extranet. In this case, because the resource request falls outside of permissible hours, the identity receives a deny, even though he satisfies other parts of a rule, as shown in [Figure 89](#).

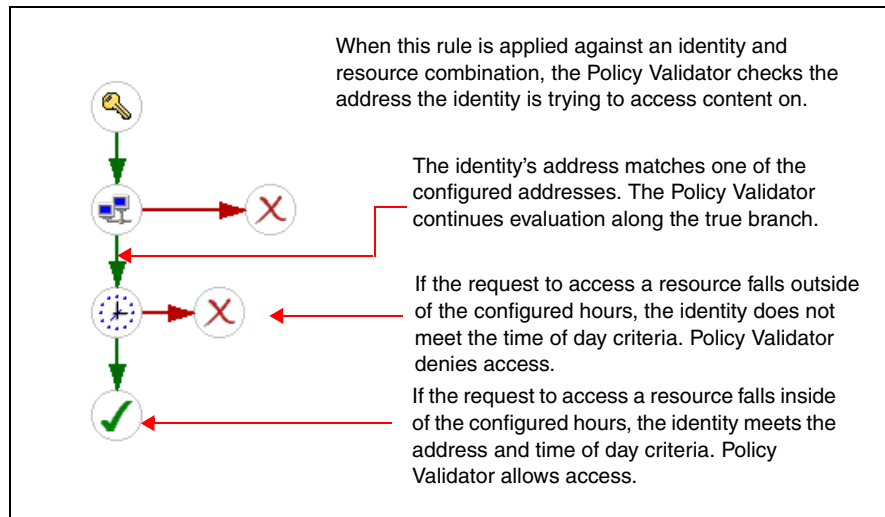



Figure 89 Example Time of Day Rule

To configure a Time of Day decision point

- 1 Do one of the following:

- To add a Time of Day decision point to the rule, select  from the toolbar.
- To modify a Time of Day decision point that already exists, right-click the existing Time of Day decision point and select **Properties**.

The **Time of Day Properties** dialog box appears, as shown in [Figure 90](#).

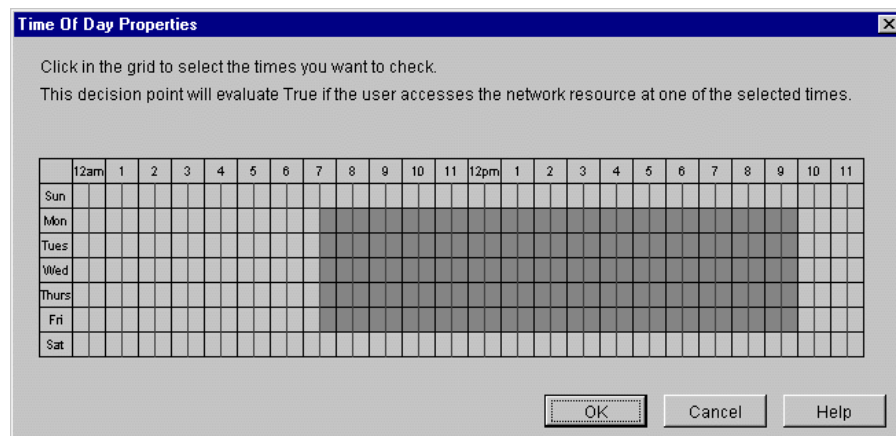


Figure 90 Time Of Day Properties Dialog Box

- 2 To select the times you want to check, click the squares on the grid. For example, you can check if the identity is trying to access the resource on a weekend, or after 6 p.m. during the week.
- 3 Click **OK**.

The Encryption Level Decision Point

An Encryption Level decision point allows you to check the identity's encryption level to ensure it is at an adequate standard for the resource they are requesting. The more restricted a resource is, the higher the encryption level typically required.

For example, if you are an administrator working at a financial institution, you might create an encryption rule requiring 128-bit encryption for all customers accessing their sensitive information over the Internet. An example rule is shown in [Figure 91](#).

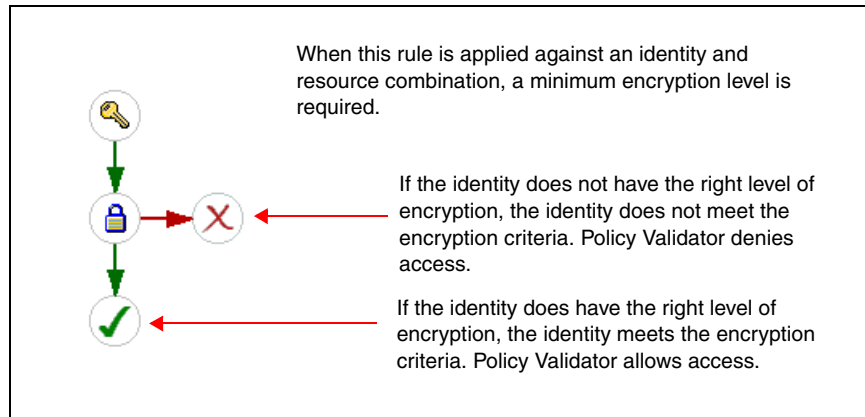



Figure 91 Example Encryption Level Rule

To configure an Encryption Level decision point

- 1 Do one of the following:
 - To add an Encryption Level decision point, select  from the toolbar.
 - To modify an Encryption Level decision point that already exists, right-click the existing Encryption Level decision point and select **Properties**.

The **Evaluate Encryption Level Properties** dialog box appears, as shown in [Figure 92](#).

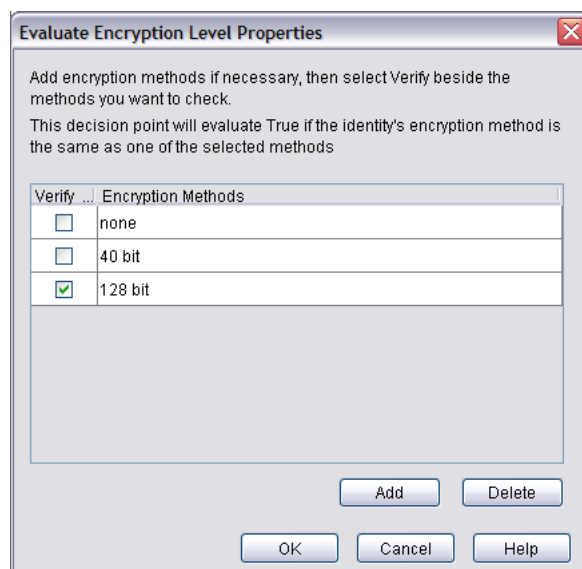


Figure 92 Evaluate Encryption Level Properties Dialog Box

- 2 To add an encryption method:
 - Click **Add** to create a new row.
 - In the **Encryption Methods** column, enter the encryption level string that appears in the tag forwarded to the Policy Validator.
 - ▶ The exact string must be used, otherwise the identity fails to meet this criteria. For example, if you type none, this matches both the string “none” in the query *and* the absence of encryption method.
- 3 To determine which of the encryption levels are required, check the corresponding box for the method in the **Verify** column.
- 4 To delete an encryption level, select a row and click **Delete**.
- 5 Click **OK**.

The Directory Attributes Decision Point

A Directory Attributes decision point allows you to check the identity’s attributes via an LDAP search expression. This ensures the identity’s attributes meet required characteristics designated for that resource. A search expression consists of the following elements:

- The type of directory entry to be checked
- An attribute type and value
- A boolean operator to define how to evaluate attributes

This decision point is typically used to target content to a specific category of customer. For example, a large multinational department store might launch a special promotion targeted to customers who make a large number of purchases throughout the course of one year. To that end, you might have a profile attribute with the value “platinum client” that identifies those customers who can access details surrounding that promotion.



This decision point performs case-insensitive matches and numerical matches.



Before you configure a directory attributes decision point, use the Policy Builder to activate the attributes you want this decision point to use. For additional details on attributes, see [About Directory Attributes](#) in the *HP OpenView Select Access 6.2 Concepts Guide*.

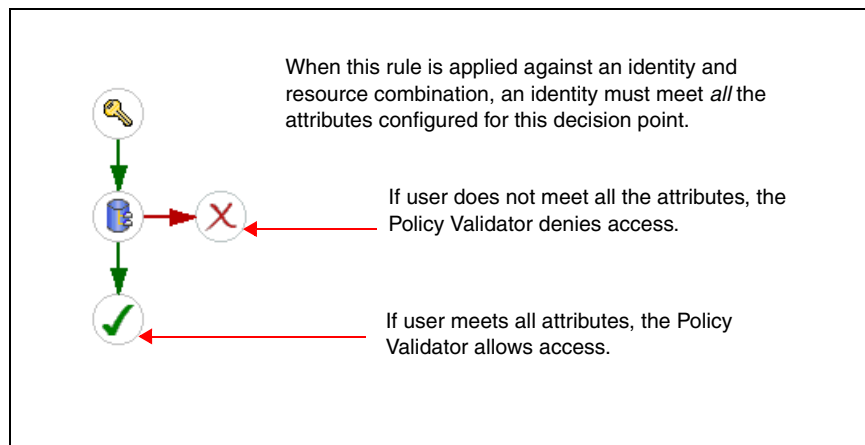



Figure 93 Example Directory Attributes Rule

To configure a Directory Attributes decision point

1 Do one of the following:

- To add a Directory Attributes decision point, select  from the toolbar.
- To modify a Directory Attributes decision point that already exists, right-click the existing Directory Attributes decision point and select **Properties**.

The **Evaluate Directory Attributes Properties** dialog box appears, as shown in [Figure 94](#).

Evaluate Directory Attributes Properties

Create a comparison expression with one or more attribute type and value pairs. This decision point compares the values in the expression against identity's entry and/or identity's group and dynamic group entries. If all the values match, the decision point returns true.

	Scope	Attribute Type	Attribute Value
Match:	User	uid, userid	= ASchulz
AND	User	c, countryName	= Canada

Buttons: Add, Delete, OK, Cancel, Help

Figure 94 Evaluate Directory Attributes Properties Dialog Box

- 2 To create a new expression, select a row and click **Add**. A row is added below the selected row. If you do not select a row, the new row gets appended to the bottom of the list.



Due to the way in which comparison operators in LDAP searches are implemented on DirX and Critical Path directories, dynamic groups and the LDAP attribute decision point behave in a manner inconsistent with other supported directory servers. In particular, less than (<), greater than (>), less than or equal to (<=), and greater than or equal to (>=) tend to be the most inconsistent operators.

- 3 If you are adding more than one row, you need to define how to match attributes:
 - **AND**: Requires the search to match all defined attributes.
 - **OR**: Requires the search to match any attributes.
- 4 Select the type of directory entry in which the Policy Validator performs lookups by choosing a value from the **Scope** menu:
 - **Identity**: Limits lookups to identity profiles only.
 - **Groups**: Limits lookups to groups and dynamic groups that the identity is currently a member of.
 - **Any**: Checks any Tree entry.



When you set **Scope** to **Any**, all Identities Tree entries (that is, groups, dynamic groups, folders, and so on) are evaluated, including those the identity entry inherits from. Depending on your situation, this affects the outcome of this decision point.

- 5 Select the types of attributes to check for in the entry, by selecting the attribute from the **Attribute Type** menu. You must activate attributes before using them.

To learn more about attributes, see [What a Directory Attribute Consists Of](#) in the *HP OpenView Select Access 6.2 Concepts Guide*.
- 6 Select the boolean operator that defines how the attribute is evaluated from the corresponding menu. For details on these boolean operators, see the table in [Appendix C, Writing LDAP Expressions](#).



Ensure you check the type of the attribute you are creating a filter for. For example, if you assume the attribute is an integer, when it in fact is a string, the results of your dynamic group filter expression might be unexpected.



Each directory server implements comparison operators differently, and operators can therefore act differently than expected. Only the Equal to comparison operator behaves consistently among all directory servers.

- 7 Enter a value that the attribute is evaluated for in the **Attribute Value** field. If you are using the ! * or =* operators, you cannot enter a value.



All attribute values must exactly match (case sensitive) before the decision point evaluates to true. Meeting only one condition does not allow access.

- 8 To delete an attribute, select a row and click **Delete**.
- 9 Click **OK**.

The Authentication Properties Decision Point

An Authentication Properties decision point allows you to define which authentication service you want to use to identify an identity. You can use an authentication properties decision point when:

- Select Auth is disabled.
- There is insufficient information to validate the identity.

For example, perhaps your password service already identified an identity as Yanla Singh. However, the nature of the resource also requires that a RADIUS service be configured and used to confirm Yanla's identification further. This further guarantees that Yanla is who she claims to be. Until Yanla enters the correct secret for user YSingh, the RADIUS service denies her access, as shown in [Figure 95](#).

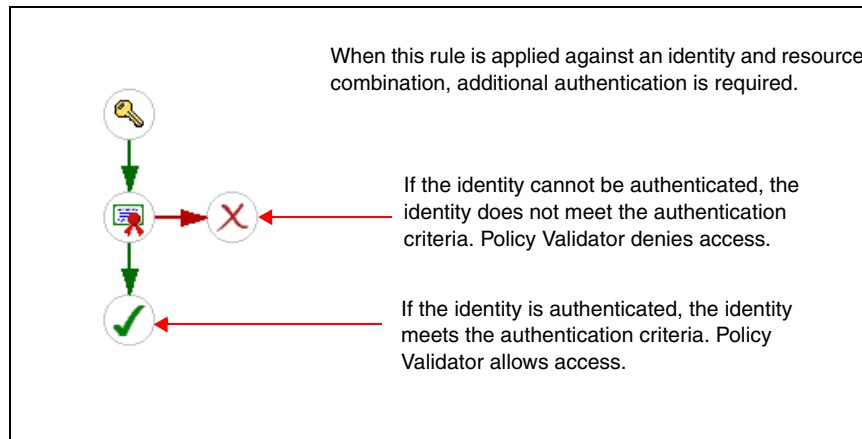



Figure 95 Example Authentication Rule

To configure an Authentication Properties decision point

- 1 Do one of the following:
 - To add an Authentication Properties decision point, select  from the toolbar.
 - To modify an existing Authentication Properties decision point, right-click the existing Authentication Properties decision point and select **Properties**.

The **Authentication Properties** dialog box appears, as shown in [Figure 96](#).

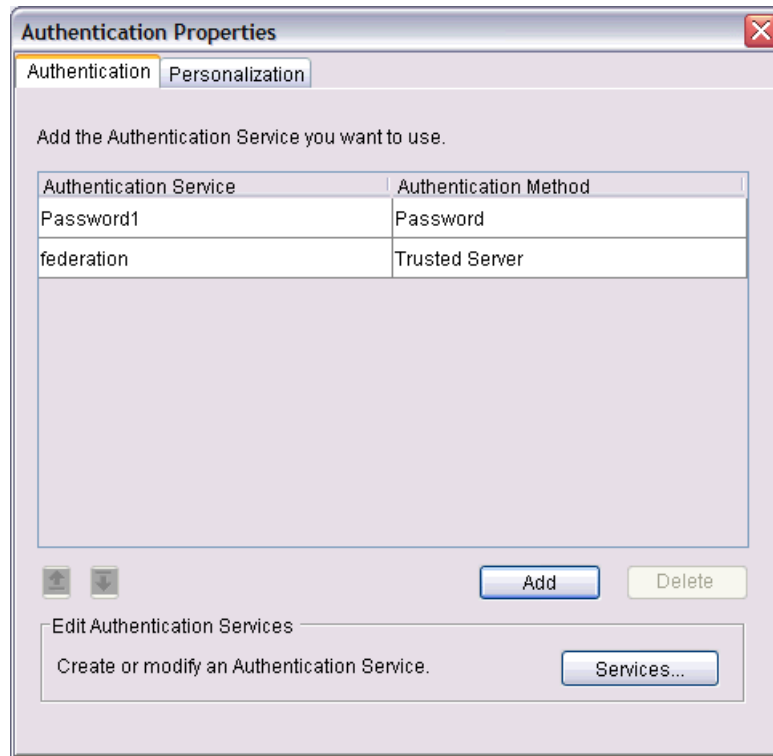


Figure 96 Authentication Properties Dialog Box

- 2 Configure the **Authentication** and **Personalization** tabs as needed. This dialog is the same dialog used to configure Select Auth. For configuration details, see [To enable Select Auth](#) on page 89.
 - If you are configuring an authentication method that requires you to browse to a folder that contains a large number of profiles that exceed the Tree threshold you have set, the **Quick Search** dialog box appears. For details, see [To perform a quick search](#) on page 78. For details on how to change the Tree threshold, see [To set tree thresholds](#) on page 83.
- 3 Click **OK**.

The Ports Properties Decision Point

A Ports Properties decision point allows you to check the port the identity is attempting to access. This decision point is typically used when you have different content available on publicly visible ports versus that which is only available on a private port.

For example, a multinational pharmaceutical company might have a large extranet. Some content on that extranet might be accessible through the web server on port 80 (the public port) and other content might be accessible only through port 8000 (a private port). Therefore if an identity wants to gain access to this content, the identity must be intending to use the port for the private content, as shown in [Figure 97](#).

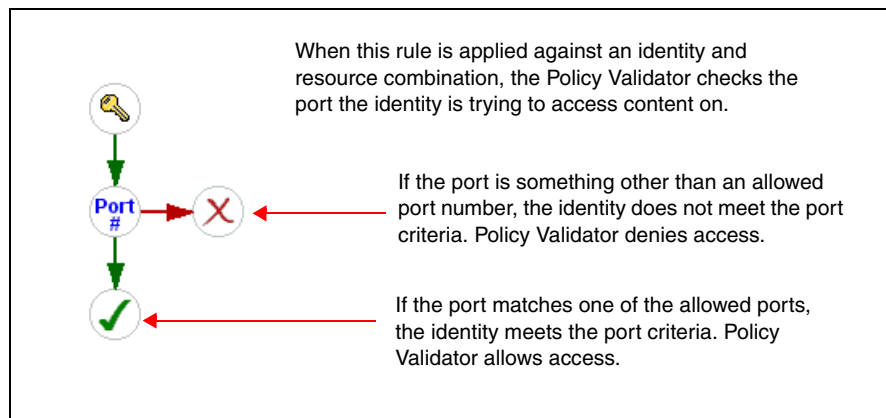



Figure 97 Example Port Rule

To configure a Ports Properties decision point

- 1 Do one of the following:
 - To add a Ports Properties decision point, select  from the toolbar.
 - To modify an existing Ports Properties decision point, right-click it and select **Properties**.

The **Ports Properties** dialog box appears, as shown in [Figure 98](#).

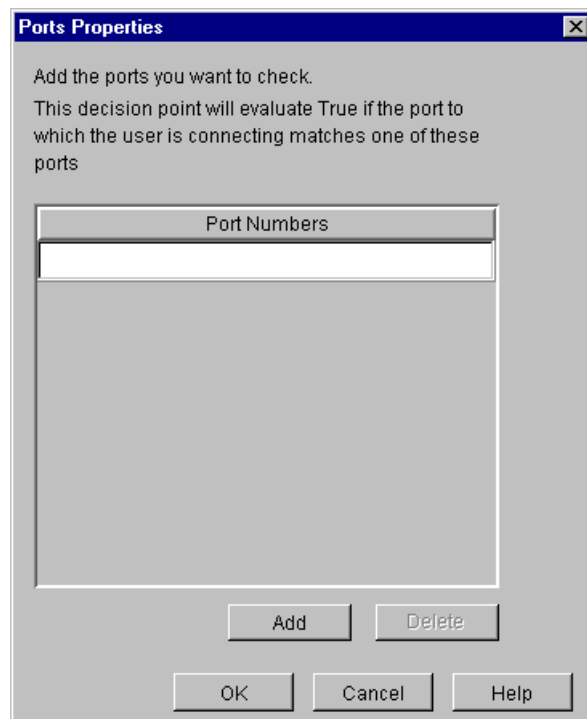


Figure 98 Port Properties Dialog Box

- 2 To add a port number, click **Add** and enter the port number. You can enter a single number or a range of numbers separated by a hyphen (for example, 80-120).
- 3 To modify a port number, type a new port number over an existing one.

- 4 To delete a port number, select a row and click **Delete**.
- 5 Click **OK**.

The Query Attributes Decision Point

A Query Attribute decision point allows you to check:

- The identity information embedded in a Policy Validator query XML tags.

For example, your corporate web site, which has two sets of content, is optimized for different types of web browsers. So, if an identity is accessing resources using a Netscape web browser, pages are displayed in a suitable way for that web browser.

- The identity information described by an LDAP user attribute.

For example, your corporate web site, which has two user categories based on spending habits, is personalized for each different category. So, if an identity belongs a category that is designated as a frequent purchaser, pages are displayed in a much different way than if the identity was an infrequent purchaser.

► If you are performing a query-based comparison, ensure that you configure your Enforcer plugin's **Query Details** (on the **Tuning** setup screen) to be either **Regular** or **Maximal**. Otherwise the query may not contain the data you require.

A search expression consists of the following elements:

- The query property list name and/or property name
- A value
- A boolean operator

For example, your corporate web site has two sets of content that are optimized for different types of web browsers. So if an identity accesses resources with a Netscape web browser, resources are subsequently displayed in an optimized format for that web browser.

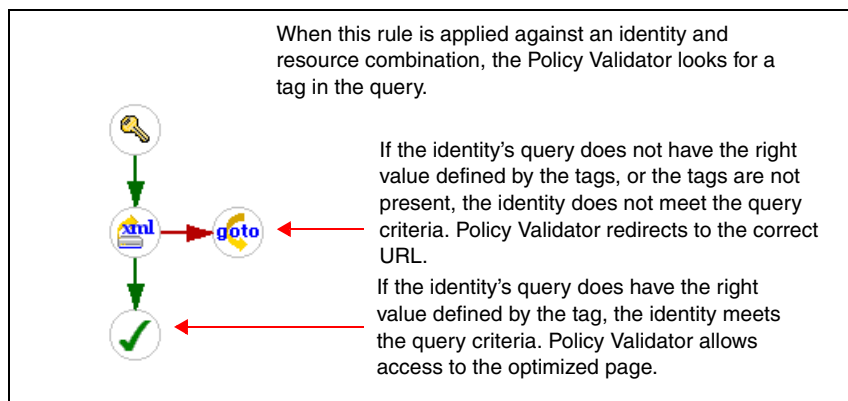



Figure 99 Example Rule with Query Attributes Decision Point

To configure a Query Attributes decision point

1 Do one of the following:

- To add an evaluate Query Attributes decision point, select  from the toolbar.
- To modify an existing evaluate Query Attributes decision point, right-click it and select **Properties**.

The **Evaluate Query Attributes Properties** dialog box appears, as shown in [Figure 100](#).

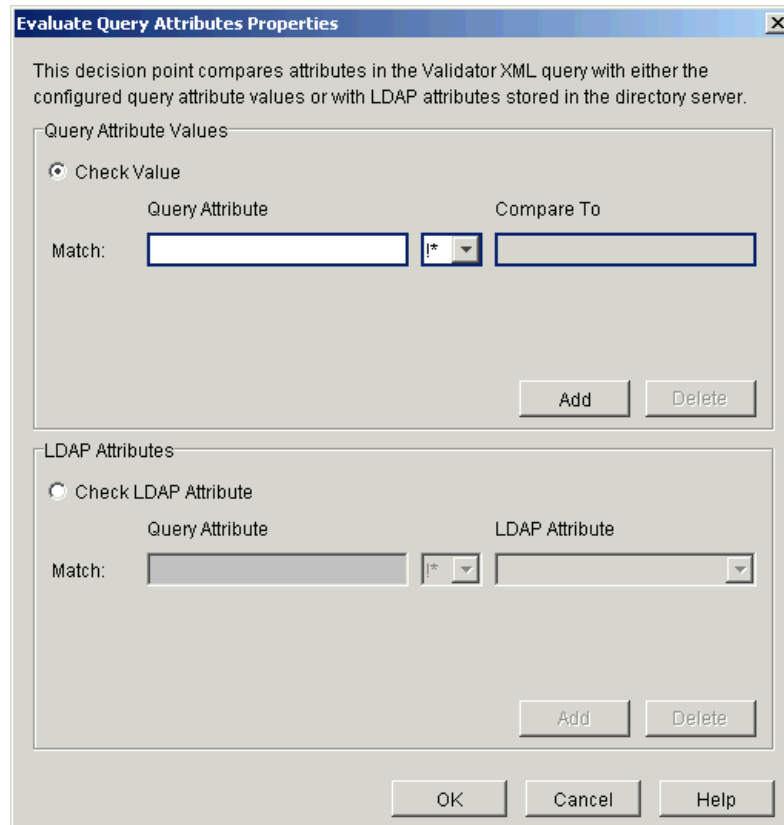


Figure 100Evaluate Query Attributes Properties Dialog Box

2 Decide what you want to evaluate:

- To compare a configured value against a fixed constant value in the Policy Validator query, click **Check Value**. The Policy Validator then evaluates user values in the property or property lists for each XML query it receives.
- To compare a configured value against a directory attribute, click **Check LDAP Attribute**. The Policy Validator then evaluates user attributes on the directory server for each query it receives.

3 Enter the name of the query property or property list tags to be evaluated by entering the appropriate string in the **Query Attribute** field. To name a specific property list element, use the forward slash (/) to separate it from the property. For example:

```
<PropertyList_name>/<Property_name>
```



If you are just naming a property, then the configuration of this field does not change with Patch 3.

- 4 Select the comparison operator that defines how the attribute is to be evaluated from the corresponding menu.
- 5 Depending on whether or not you are creating an expression for an XML search or an LDAP search, do one of the following:
 - For an XML search, enter a value that the query property tag will be evaluated for in the **Compare To** field. If you are using the ! * or =* operators, do not enter a value.
 - ▶ The name/value pairs you create must exist in the query sent to the Policy Validator.
 - For an LDAP search, choose an LDAP attribute from the list in the **LDAP Attribute** drop-down list.

For example, if you wanted to create a search expression that searches the `http_query_list` property list tag for the `SWECmd` property to see if it contains a value of `Logoff`, configure the fields in the **Query Attribute Values** group box, as shown in [Figure 101](#).

Figure 101 Example Values for Query Attributes

In this case, the following URL would then meet the search expression configured for this decision point:

```
http://www.mycompany.com?swecmd=Logoff
```

However, if you wanted to create a search expression that searches the `http_query_list` property list tag for the `givenname` property to see if the value in that property matches the value in the directory server attribute `cn`, configure the fields of the **LDAP Attributes** group box as shown in [Figure 102](#).

Figure 102 Example Values for Directory Server Attributes

- 6 Click **OK**.

Available Query Attributes

The table below outlines those query property tags that can be evaluated using string operations. If you frequently use one of these query properties and would like a custom decision point plugin for it, Select Access' extensible architecture allows you to build your own plugin. For details, see the *HP OpenView Select Access 6.2 Developer's Tutorial Guide*.

Table 27 Query Properties Syntax

Property	Description	Value
cert	A property that sends information required by the certificate decision point.	A PEM-encoded X.509 digital certificate.
client	A property that sends information from the client software. <i>Note:</i> This data is not used by any of the standard server decision points.	The name and version number of the client software that initiated the request.
dstHost srcHost	A property that makes the host name explicit, when a single physical machine supports multiple virtual host names. <i>Note:</i> This data is not used by any of the standard server decision points.	The name of the host to which the request was sent.
dstIP srcIP	A property that retrieves destination IP information.	The IP address to which the request was sent.
dstPort srcPort	A property that retrieves destination port information. This data is required by the ports decision point.	The port to which the request was sent.
protocol	A property that describes which format is used for transmitting data between the browser and server.	Any accepted protocol. For example, http, https.
method	A property that describes what HTTP header command was used to encapsulate the data.	Any valid HTTP header command. For example, GET, POST, HEAD.
server	A property that describes what kind of web server is used.	Any supported web/application server. For example, iPlanet web server.

The XPath Decision Point

An XPath decision point allows you to evaluate any arbitrary XML within a Policy Validator query with an XPath expression. When the Policy Validator receives a query from an Enforcer plugin that protects a web service, this plugin evaluates the data in the SOAP envelope against a criteria you configure.



If you intend to use this decision point, you must have an advanced knowledge of XPath and how to write syntactically correct XPath expressions. Describing XPath terminology and syntax is beyond the scope of this document.

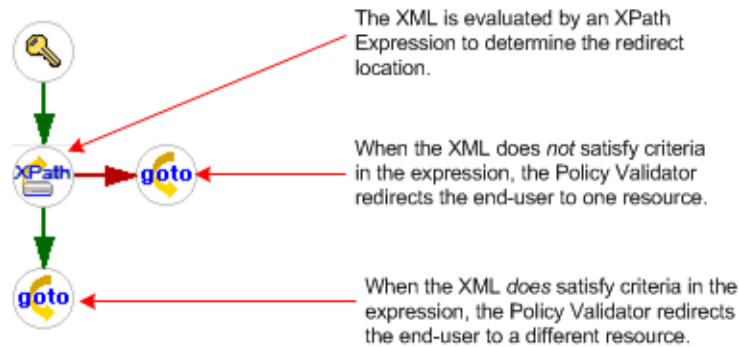



Figure 103 Sample Rule with an XPath Decision Point

To configure an XPath decision point

- 1 Do one of the following:
 - To add an XPath decision point, select  from the toolbar.
 - To modify an existing XPath decision point, right-click the existing XPath decision point and select **Properties**.

The **XPath Expression Properties** dialog box appears, as shown in [Figure 104](#).

Evaluate XPath Expression Properties

Create a decision point that evaluates Policy Validator XML queries with the XPath expression you create.

Namespaces

Map prefixes to their corresponding namespace as required. XPath expressions can use prefixes to identify the namespace that an element or attribute belongs to.

Namespace	Prefix
http://schemas.xmlsoap.org/soap/envelope/	soap

Add Delete

XPath Expression

The Policy Validator begins evaluating an XPath expression from the Root Context. The XPath Expression can include either fixed constant values or LDAP attributes. The Policy Validator only searches for LDAP attributes delimited with curly brackets as in "\${LDAP_attribute}". To auto-populate an attribute name, right-click the XPath Expression text box and choose 'Insert LDAP attribute'.

Root Context:

/PolicyValidatorQuery/PROPERTYLIST[@NAME='soap']/soap:Envelope

XPath Expression:

OK Cancel Help

Figure 104 Evaluate XPath Expression Properties Dialog

2 Map the namespace to an appropriate prefix, if required:

➤ You only need to define a Prefix, if the XML you are evaluating uses **Namespaces**.

- The **Namespace** is any Uniform Resource Identifier (that is, a URL or URN) contained in the anticipated Policy Validator query that is sent by an Enforcer plugin.
- The **Prefix** is a short form of the Namespace that you can then use in your XPath Expression.

For example, assume your Policy Validator query contained the following SOAP envelope:

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <soap:Header></soap:Header>
  <soap:Body>
    <comp:GetEmployeeInfo comp:employeeNumber="194567"
comp:type="manager" xmlns:comp="http://www.company-x.com">
      <comp:EmployeeName>Tom Carter</comp:EmployeeName>
    </comp:GetEmployeeInfo>
  </soap:Body>
</soap:Envelope>
```

In this case, you might have mapped the following prefixes and namespaces as shown in the figure below:

Namespace	Prefix
http://schemas.xmlsoap.org/soap/envelope/	soap
http://www.company-x.com	x-co

Figure 105 Example Namespaces Configuration

- 3 To narrow the evaluation scope, define a **Root Context**. The fixed node you define is the point from which the Policy Validator begins evaluating the XML.
 - If you do not know the absolute path to the appropriate context, type “/” as the **Root Context**. Then all elements in the query meet the criteria even if they are on different levels of the XML tree.
 - You can only configure one **Root Context** for a single XPath decision point. If you need to evaluate XML from various root nodes, you must configure a new decision point for each new starting point.

To continue the example introduced in [Step 2](#), if you used the default **Root Context**, the Policy Validator only begins filtering XML once it locates a `PROPERTYLIST` query tag type with the name of `soap:Envelope`. [Figure 106](#) illustrates this example.

Root Context:

Figure 106 Sample Root Context Configuration

- 4 Type the **XPath Expression** you want the Policy Validator to evaluate queries with. The expression can include static values as well as LDAP attributes. In the case of the latter, the Policy Validator checks the value stored in the identity’s profile. For details on how to write an XPath Expression, see [To write a valid XPath Expression](#) on page 183.
 - Remember, XML is case-sensitive. However LDAP attribute names are not. Ensure you type the expression carefully to avoid the Policy Validator returning an incorrect result.
 - 🚩 For LDAP attributes, you can right-click the expression text box and click **Insert LDAP attribute**. This allows you to auto-populate the expression with the correct attribute name and casing.

For example, you can write a simple expression as follows:

```
x-co:GetEmployeeInfo[@x-co:type="manager"]
```

In this case, the XPath decision point evaluates the SOAP envelope introduced in [Step 2](#) as true (it meets the criteria).

However, to expand upon the example introduced in [Step 2](#), assume you have the following identity profile with the following LDAP attributes:

```
sn=Carter
cn=Tom Carter
uid=TCarter
employeeType=manager
employeeNumber=194567
```

With this profile data, you can write an expression that searches for identities that meet the following criteria:

```
x-co:GetEmployeeInfo/ns:EmployeeName='{$cn}' AND  
x-co:GetEmployeeInfo[@ns:type!="{$employeeType}"]
```

In this case, however, the identity for Tom Carter would evaluate to false, because the second condition of (that is, does *not* have an `employeeType` attribute) is not met.

- 5 Click **OK**. You may be prompted to correct any syntax errors in the **Root Context** or the **XPath Expression**, if any exist.

To write a valid XPath Expression

- 1 Ensure the expression meets the following criteria:
 - That values use the correct case
 - For LDAP attributes, that you delimit names the following characters: “\${” and “}”
- 2 Meet the syntactical requirements for XPath. The Rule Builder attempts to examine the expression to determine if there are any errors. However, HP cannot always catch all errors.
- 3 If your expression includes prefixes, ensure you have mapped them to the appropriate URI.

The Alert Notification Decision Point

An Alert Notification decision point triggers an email message to the administrator when an identity passes or fails a specific criteria in the rule.

For example, an administrator places an Alert Notification decision point before an allow terminal point, and then applies this rule against every extremely sensitive resource on a network. That way, administrators are notified of which authenticated user accessed the resource and when, so they can track those resources more closely. This rule is illustrated in Figure 107.

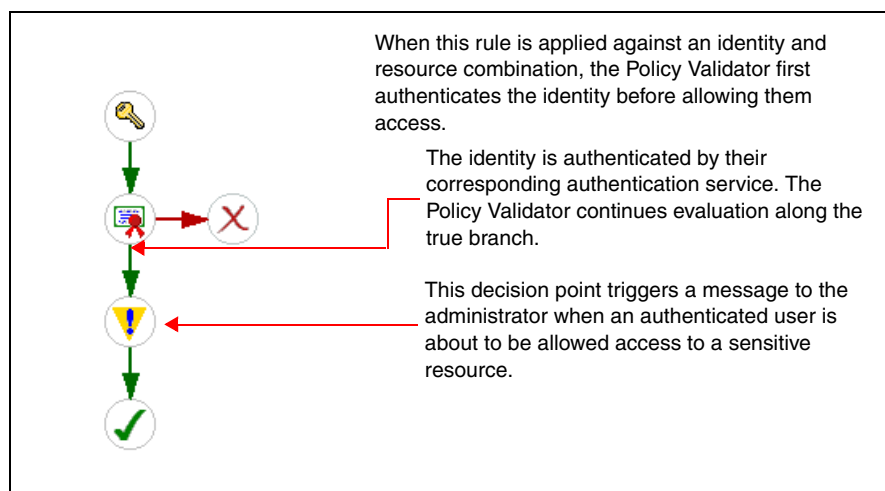



Figure 107Example Rule with an Alert Decision Point

To configure an Alert Notification decision point

- 1 Do one of the following:
 - To add an Alert Notification decision point to a rule, click  from the toolbar.
 - To modify an existing Alert Notification decision point, right-click it and select **Properties**.

The **Alert Properties** dialog box appears, as shown in [Figure 108](#).

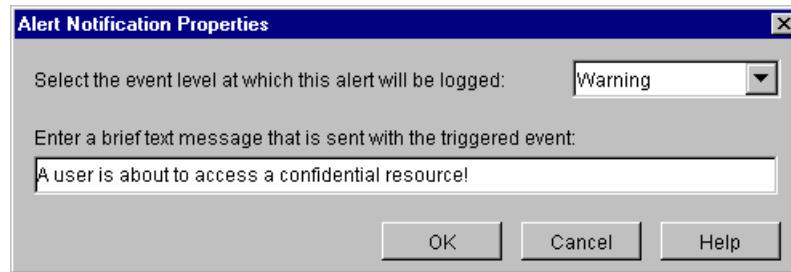


Figure 108 Alert Properties Dialog Box

- 2 To filter messages based on their severity level, select the severity from the **Select the event level at which this alert will be logged** menu. For details on event level options, see [Configuring an Audit Policy](#) in the *HP OpenView Select Access 6.2 Installation Guide*.
- 3 Enter your message in the **Enter a brief text message to be sent with the alert** field. The message is used to introduce the alert and what has happened.
- 4 Click **OK**.

The Insert Subrule Decision Point

An Insert Subrule decision point allows you to insert an existing rule as part of the rule you are creating. This allows you to create a single rule for common elements of the evaluation elements you need on a regular basis, which you can insert into a different rule to customize the logic for different user and resource combinations.

For example, an administrator might create a rule that captures the evaluation logic required for a global human resources portal. Since each regional office can have its own authentication service, you can insert the human resources portal rule inside a unique authentication rule for each region, as shown in [Figure 109](#).

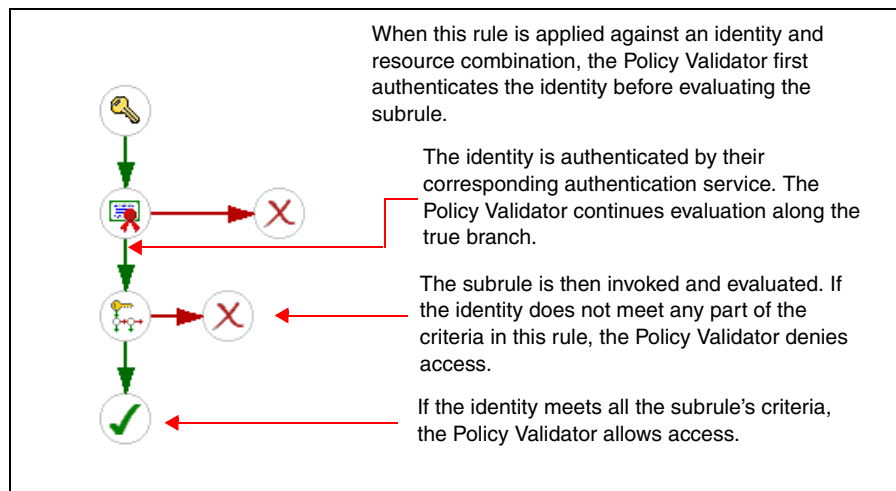



Figure 109Example Rule with Insert Subrule Decision Point

To configure an Insert Subrule decision point

- 1 Do one of the following:

- To insert a Subrule to an existing rule, select  from the toolbar.
- To modify an existing Insert Subrule decision point, right-click it and select **Properties**.

The **Insert Subrule Properties** dialog box appears, as shown in [Figure 110](#).

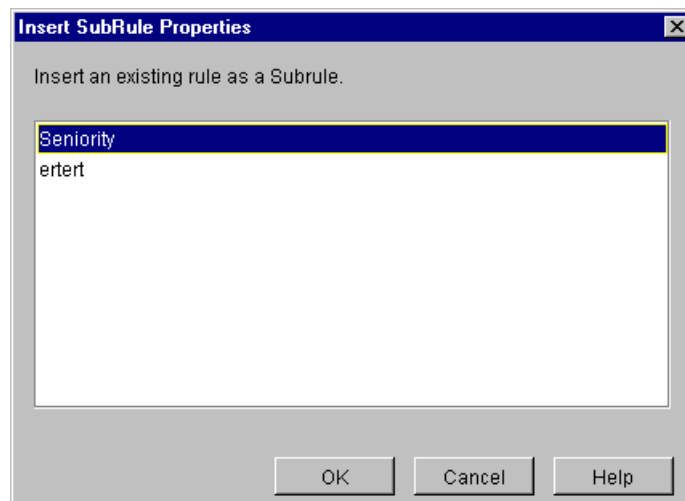


Figure 110Insert Subrule Properties Dialog Box

- 2 From the list of rules, select the rule you want to use as the subrule.
- 3 Click **OK**.

The Citrix Decision Point

The Citrix decision point allows you to verify identities' credentials and then, if authenticated, deliver personalized content to them. This decision point uses usernames, passwords, and domains to evaluate the type of content it is to deliver:

- If you configure a common username, password, and domain, Citrix delivers generic content for all identities.
- If you configure the corresponding attributes that hold the unique values, Citrix uses this data to deliver personalized content.

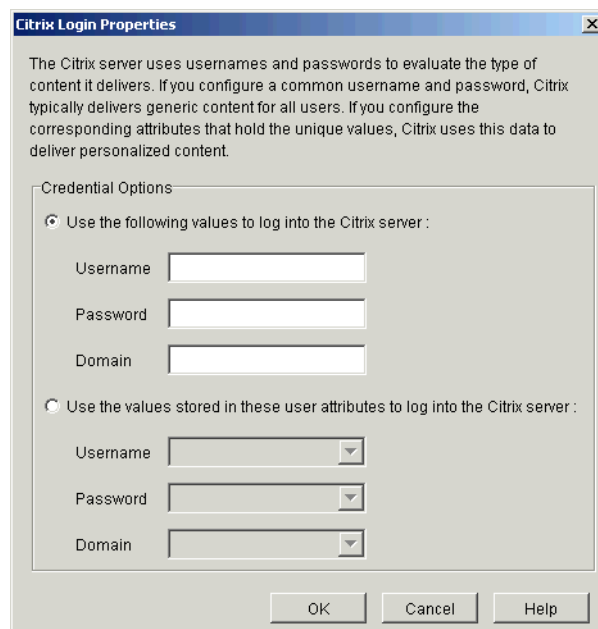


Only upload this decision point if you use Citrix as part of an integrated Select Access solution.

For example, an administrator using Citrix might want to create a rule that ensures Citrix delivers personalized content to all identities. In this case, the administrator clicks the **Use the values stored in these user attributes to log into the Citrix server** radio button and then fills out the fields below it. The administrator also has to make sure there are username, password, and domain credentials for each user in the directory server.

To configure a Citrix decision point

- 1 Upload the Citrix decision point to the Rule Builder toolbar. For details, see [To upload a custom Decision Point or Authentication plugin](#) on page 289.
- 2 Click  on the toolbar. The **Citrix Login Properties** dialog box appears.



The Citrix Login Properties dialog box is shown. It has a title bar 'Citrix Login Properties' with a close button. The main text area contains the following text: 'The Citrix server uses usernames and passwords to evaluate the type of content it delivers. If you configure a common username and password, Citrix typically delivers generic content for all users. If you configure the corresponding attributes that hold the unique values, Citrix uses this data to deliver personalized content.'

Below the text is a section titled 'Credential Options' with two radio buttons:

- ☒ Use the following values to log into the Citrix server :
- ☐ Use the values stored in these user attributes to log into the Citrix server :

Under the first radio button, there are three text input fields: 'Username', 'Password', and 'Domain'.

Under the second radio button, there are three dropdown menu fields: 'Username', 'Password', and 'Domain'.

At the bottom right, there are three buttons: 'OK', 'Cancel', and 'Help'.

Figure 111Citrix Login Properties Dialog Box

- 3 To authenticate Citrix identities with shared credentials, do the following:
 - Click the **Use the following values to log into the Citrix server** radio button (common credential configuration) to configure a common username, password, and domain. Citrix uses this data to deliver generic content for all identities.

- Configure the **Credential Options** by typing a **Name**, **Password**, and **Domain** in the corresponding fields.

➤ These credentials must correspond to a valid Windows account. The information you configure on a Windows account becomes a shared passport for all of your identities to the content on your Citrix server.

4 To deliver personalized content to identities, do the following:

- Click the **Use the values stored in these user attributes to log into the Citrix server** radio button (unique credential configuration) to configure the corresponding attributes that hold the unique values. Citrix uses this data to deliver personalized content.
- Configure the **Credential Options** by typing a **Name**, **Password**, and **Domain** in the corresponding fields. You can use existing attributes or create new ones.

➤ Attributes vary from one directory server to the next. Consult your directory server's documentation for details on which attributes it handles.

Example attribute names are listed in [Table 28](#).

5 Click **OK**.

The Workflow Decision Point


Each Workflow decision point defines the following information:

- The list of administrators capable of approving the change request
- The minimum number of administrators who must approve a change in order for it to be executed
- The minimum number of administrators who must reject a change in order for it to be cancelled
- Whether alerts will be sent to the approvers
- Whether alerts will be sent to the submitting administrator

➤ For a comprehensive discussion on how to use and set up workflow, see [Chapter 12, Using Administration Workflow](#).

To configure a Workflow decision point

1 Do one of the following:

- To add a new Workflow decision point, select  from the toolbar.
- To modify a Workflow decision point that already exists, right-click the existing Workflow decision point and select **Properties**.

The **Workflow Properties** dialog box appears, as shown in [Figure 112](#).

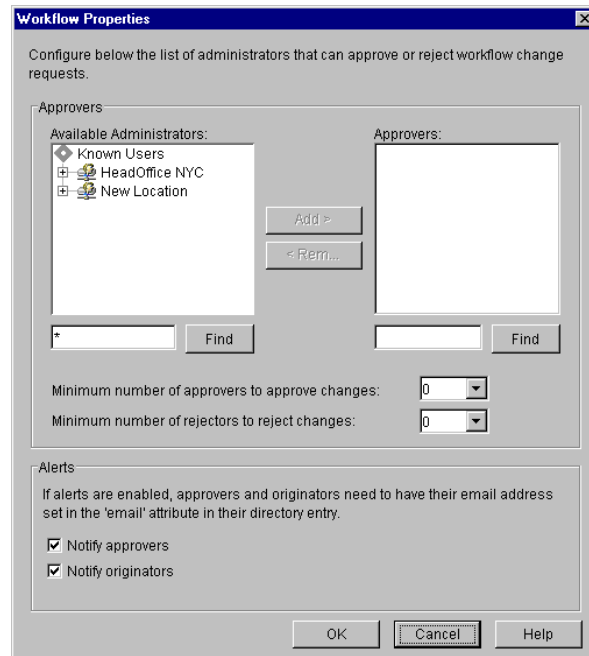


Figure 112 Workflow Properties Dialog Box

- 2 Create a list of identities who can approve changes. Select one or more identities in the **Available Approvers** list and click **Add**. This moves them to the **Approvers** list.
 - A list of approvers may include folders, groups, or dynamic groups, as well as individual identities. In those cases, every user in the folder, group or dynamic group added to the **Approvers** list is notified. Should an administrator be added as an approver more than once (as a member of both a selected group and a selected folder, for example), he is notified only once.
 - Identities added to the **Approvers** list must have an email address configured as part of their identity profiles, or workflow alerts cannot be sent.
- 3 Specify the minimum number of approvals and the minimum number of rejections required to accept or reject a change request.
 - You must specify a value of one or greater, since at least one user must accept a change request in order for it to be processed, and at least one user must reject a change in order for it to be cancelled.

Note that if at least three of six identities are required for an approval, then four rejections is enough to reject the change.
- 4 Set up optional alerts for approvers and/or submitters by checking the **Notify approvers** and/or **Notify originators** boxes. Alerts can be sent when:
 - A node in the workflow rule has been entered
 - A change request has been rejected
 - A change request has been processed

If selected, alerts are sent in addition to the messages notifying approvers of a change request.
- 5 Click **OK** to return to the Rule Builder.

- 6 Add the new decision point to a branch of the rule. To add any decision or terminal point to a branch:
 - a Move your cursor to the insertion point of your rule. When you have moved the decision point to a valid insertion location, the branch arrow is highlighted.
 - b Click to insert the decision point or terminal point at that location.
- 7 Repeat [Step 3-8](#) to add any additional decision or terminal points.

The Custom Response Terminal Point

A Custom Response terminal point allows the identity to access the resource in question, but also displays additional personalized content, which can further depend on the attribute values that exist in the identity's profile.

For example, use a Custom Response terminal point in combination with a time of day decision point to display custom data to an identity. If the identity accesses the stock exchange site during business hours, a stock ticker appears. However, if she accesses the stock exchange site after trading hours, she gets a list of the day's most active stocks. This example is illustrated below.

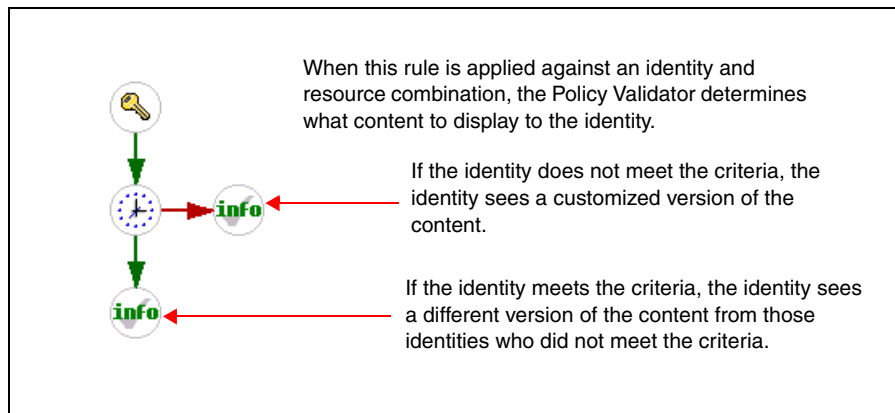



Figure 113Example Custom Response Rule

To configure a Custom Response terminal point

- 1 On the toolbar, select  .
The **Custom Response** dialog box appears.

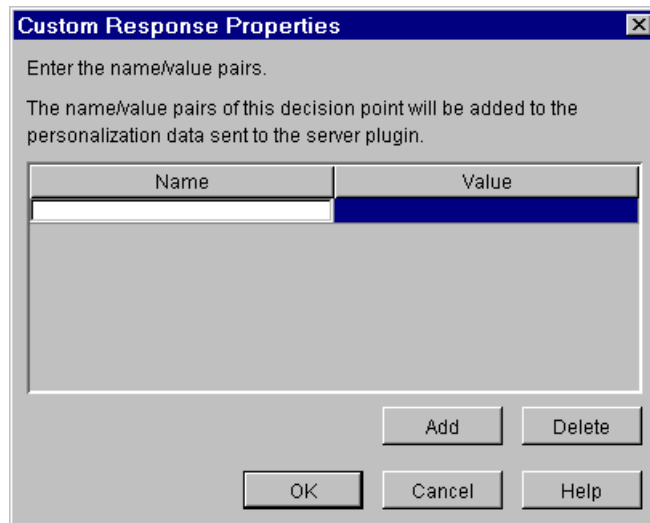


Figure 114 Custom Response Properties Dialog Box

- 2 To define personalization data, enter the name of the tag and value in the corresponding columns. This name is sent to the Enforcer-protected web server, which uses this information to determine which set of customized content to serve to the identity.
- 3 To add multiple name/value pairs, click **Add** then enter the attribute name and value in the corresponding columns.
- 4 To delete a name/value pair, select a row and click **Delete**.
- 5 Click **OK**.

The Logout Identity Terminal Point

A Logout Identity terminal point allows you to explicitly force logout, so that subsequent identities of the shared computer cannot take advantage of the session cookie. The identity must reauthenticate before access is authorized.

If you use this terminal point, we recommend you support it with a web page that displays a message something like “You are now logged off. Subsequent access to this web site requires a new login”.



You cannot use the logout node following an Authentication decision point in uses a Certificate Authentication service. You cannot logout with certificates; the browser always automatically presents the certificate to the web server whenever you connect.

For example, an administrator at a government agency where identities share terminals creates rules where all identities who are allowed access must always log off from the resource they have accessed. An example of this is shown in [Figure 115](#).

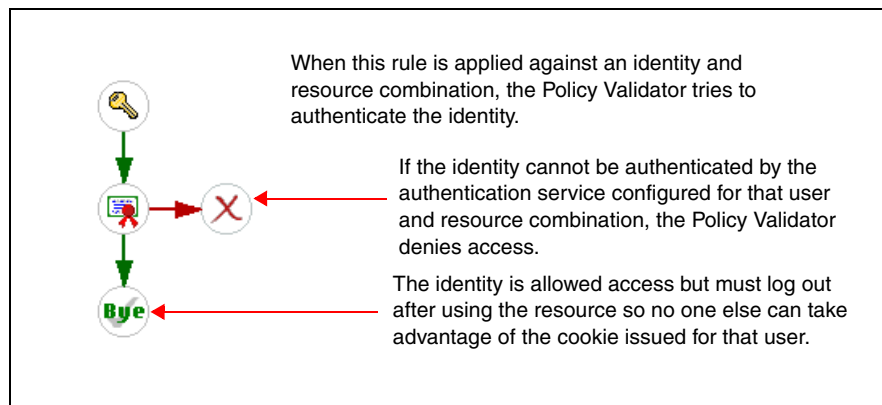


Figure 115Example Logout Identity Terminal Point in a Rule

The Redirect Terminal Point

A Redirect terminal point allows you to redirect an identity to an alternate URL, depending on the outcome of the decision criteria. The redirect to the URL only takes place under the following conditions:

- The identity has not tried to authenticate.

If the identity has not tried to authenticate yet, she is prompted via a form or HTTP basic authentication to authenticate. In this case, the redirect is ignored.

- The identity has tried to authenticate, but authentication failed (for example, their password was incorrect).

For example, you create a redirect decision point that sends these identities to a “Failed Login Attempt” page. To attempt to log in again, the identity can click the **Back** browser button.

For example, if an identity who does not have a certificate tries to access a resource that requires a certificate, you can redirect her to a URL that describes the company’s certificate policy, as illustrated in [Figure 116](#).

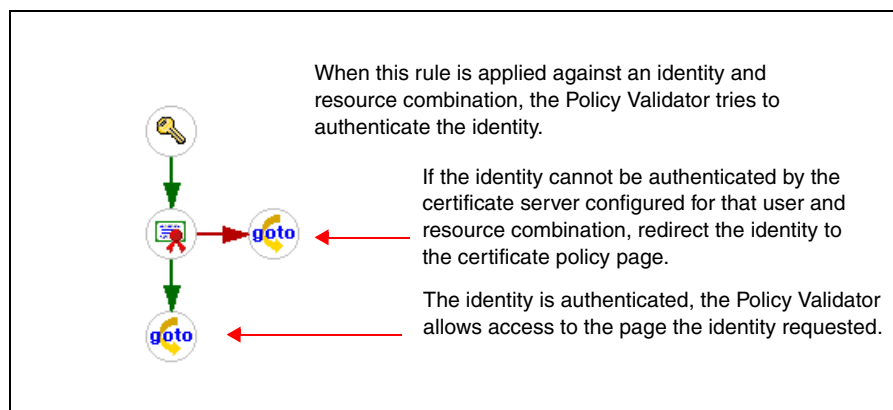



Figure 116Example Redirect Rule

To configure a Redirect terminal point

1 Do one of the following:

- To add a Redirect terminal point to the rule, select  from the toolbar.
- To modify a Redirect terminal point that already exists, right-click the existing Redirect terminal point and select **Properties**.

The **Redirect Properties** dialog box appears, as shown in [Figure 117](#).

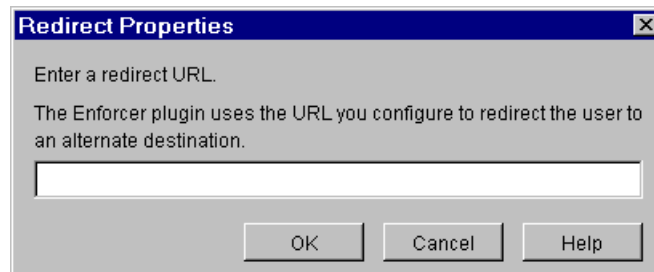


Figure 117 Redirect Properties Dialog Box

2 In the **Please enter a redirect URL** field, type the destination URL. There are two kinds you can enter:

- A fully-qualified URL specifies the entire path to the resource and uses the following syntax:

`<protocol>://<URL>/<path>/<filename>`

For example:

`http://www.mycompany.com/solutions/partners/welcome.html.`

- A relative URL specifies the location of a resource relative to the identity's current location.

Examples of relative URLs appear in [Table 28](#). For demonstration purposes, these examples are relative to the URL listed in the previous example.

Table 28 Relative URLs

Syntax	Example	Redirect
/<filename>	/help.html	http://www.mycompany.com/solutions/partners/help.html
<filename>	default.asp	http://www.mycompany.com/solutions/partners/default.asp
../<path>/	../products/	http://www.mycompany.com/solutions/products/

3 Click **OK**.

The Profile Self-Management Terminal Point

A Profile Self-Management terminal point identifies when and how identities can update their profiles. Modifiable profile information is determined by the attributes you have already activated for this purpose.

- This terminal point can frequently be used as a single node inside its own rule.
 - At a minimum, activate the following end user-editable attributes:
facsimiletelephonenumber, givenname, mail, sn, telephone number, userpassword.
These attributes are required by the fields in `profile_mgmt_form.html`.
- Note that ADS directories have a maximum string limit of 64 unicode characters for the `givenname` attribute.
- Because the identity's password attribute (`userPassword`, `password_id`, etc.) can vary depending on which directory server she is using, you need to change the attribute defined for the **Change Password** button in the `profile_mgmt_form.html` form. For details on the Profile self-management form, see [To customize the Profile Self-Management form](#) in the *HP OpenView Select Access 6.2 Network Integration Guide*.

For example, an administrator might include a profile self-management terminal point as a result of a mandate to reduce administration costs company wide. To reduce the overhead costs required to input and update profile data, you apply a profile self-management action point to your Customers group. This allows identities to update their own data when and if their profile data changes. An example rule is shown in [Figure 118](#).

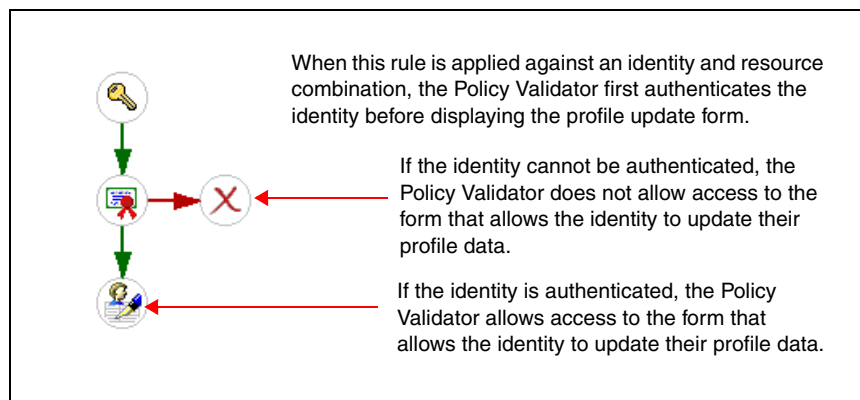



Figure 118Example Profile Self-Management Rule

To configure a Profile Self-Management terminal point

- 1 Do one of the following:
 - To add a Profile Self-Management terminal point to the rule, select  from the toolbar.
 - To modify an existing Profile Self-Management terminal point, right-click it and select **Properties**.

The **Profile Self-Management Properties** dialog box appears as shown in [Figure 119](#).

If you have activated attributes, they appear in the **Available Attributes** list. Of those activated attributes, if you have activated any of our recommended attributes (for example `facsimiletelephonenumber`, `givenname`, `mail`, `sn`, `telephone number`, and `userpassword`, they automatically appear in the **Identity Profile Attributes** list.

▶ Note that ADS directories have a maximum string limit of 64 unicode characters for the `givenname` attribute. Ensure that you communicate this limitation with your end users.

▶ If you choose a `userpassword` attribute, the Enforcer plugin displays an HTML form that allows the end user to change her password. The password that the end user changes is the password that corresponds to the identity's profile on the directory server. Depending on how you use this terminal point, password changes are always directly relevant: that is, you are forcing a password change for an LDAP password that is never to be used.

▶ If you are using NTLM or Kerberos authentication, and want the end user to be able to modify her Windows domain password, then you must meet the following conditions: you must use Active Directory, the Policy Validator and the Windows 2000 domain controller must be using the exact same identity location, and you must connect over SSL.

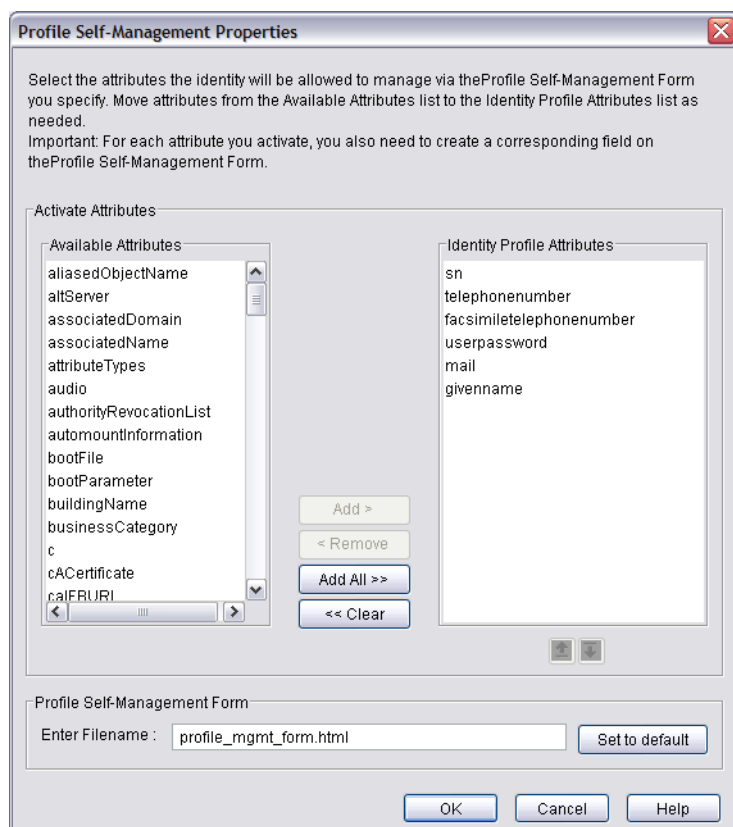


Figure 119 Profile Self-Management Properties Dialog Box

- 2 To allow identities to self-manage any additional attributes in their profile, select one or more attributes in the **Available Attributes** list and click **Add**. This moves the selected attributes to the **Identity Profile Attributes** list.

- 3 To reorder the attributes, select an attribute and use the up and down arrows to shift its position.
- 4 To remove attributes in the **Identity Profile Attributes** list, do one of the following:
 - Select individual attributes and click **Remove**.
 - Click **Clear** to remove all listed attributes.
- 5 To change the name of the profile self-management form, type the new name in the **Enter filename** field. If you need to revert to the default form at any time, simply click **Set to default**.

► Save a copy of this form on your web server. Otherwise, the Enforcer plugin do not allow identities to manage their own profile. The original `profile_mgmt_form.html` template is installed to the following directory by default: `<install_path>/content/`.
- 6 Click **OK**.

The Allow and Deny Terminal Points

The Allow and Deny terminal points indicate the evaluation logic the Policy Validator performs along a specific branch. Either terminal point can come at the end of a true or false branch.

For example, if an administrator were to create a simple rule using just a networks and domains decision point that has only one domain configured for it (`mycompany.com`), the meaning varies depending on how the Allow and Deny terminal points have been placed. The subsequent figures illustrate the subtleties of their placement in a rule.

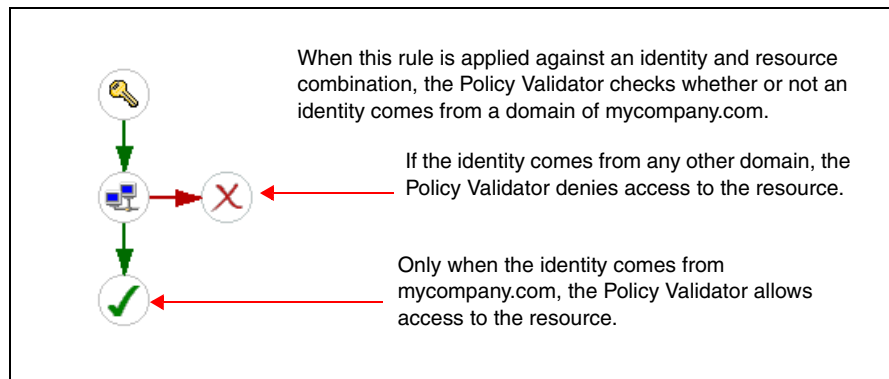


Figure 120 Example Rule with Allow at End of True Branch

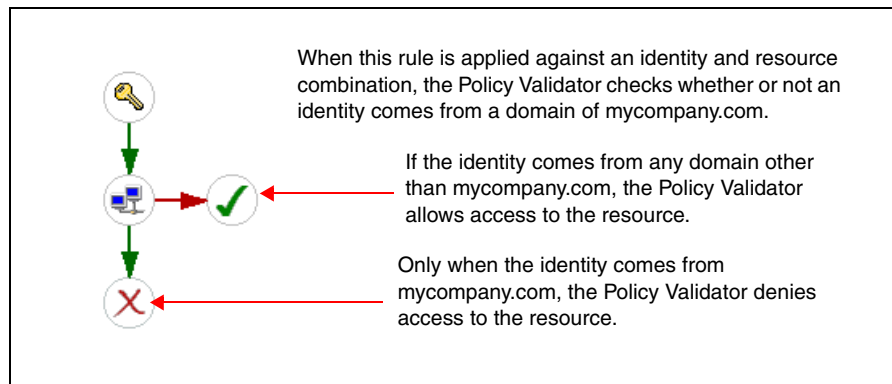


Figure 121 Example Rule with Allow at End of False Branch

10 Controlling Administrative Access

This chapter introduces the levels of administration access an identity can have. It is an overview topic to the more detailed subjects of Delegated Administration management and workflow management described in subsequent chapters of this guide.

Chapter Overview

This chapter includes the following topics:

- [Levels of Administrative Access](#) on page 197
- [Using the Administration Matrix to Delegate Entitlements](#) on page 202

Levels of Administrative Access

The Administration server allows several different levels of administrative access. Each level accesses the server through its own port, which is configured in the Setup Tool's Administration Server wizard. For more information on setting the Administration server service names and ports, see [Using the Setup Tool to Configure the Administration server](#) in the *HP OpenView Select Access 6.2 Installation Guide*.

The Administration server has four service levels:

- Root aAdministration. For more information, see [Root Administration Access](#) on page 197.
- Delegated Administration. For more information, see [Delegated Administration Access](#) on page 198.
- Web Administration. For more information, see [Web Administration Access](#) on page 198.
- Self Administration. For more information, see [Self Administration Access](#) on page 198.

Root Administration Access

This access level allows administrators complete access to the Administration server through the Root Administration mode of the Policy Builder. By default, Root (also known as "Full") Administration accesses the Administration server via port 9986.

By default, the Policy Builder in Root Administration automatically contains entries for each of Administration server service levels described in the following sections. These entries are contained in a folder named, by default, Administration server.

Access to Root Administration mode should be limited to the Select Access super administrators only. HP strongly recommends that the Administration server only be accessed through this mode to:

- Enable and disable the other Administration server services
- Set up initial delegation entitlements to a second tier of administrators
- Resolve Administration server issues

Delegated Administration Access

This access level allows delegated administrators partial access to the Administration server through the Delegated mode of the Policy Builder. By default, Delegated Administration accesses the Administration server via port 9987.

The level of access a delegated administrator has is determined by which entitlements they have been given; a delegated administrator may be permitted to set access policy for only a single resource, or may have administration access to complete Policy Builder functionality, excluding the Administration server resources.

Web Administration Access

The Web Administration access level allows delegated administrators with the appropriate entitlement to manage identity profiles via their browser, without requiring the Policy Builder applet. By default, this service accesses the Administration server via port 9991.

Using this service, administrators can add, modify, rename or delete any identity, group or folder to which they have been given full access, or view those to which they have been given read only access.

For more information on managing identities with the Web Administration service, see [Appendix B, Using Web Administration](#).

Self Administration Access

Self Administration access allows identities to set or modify their own user profile attributes. By default, this service accesses the Administration server via port 9992.

Self Administration is comprised of three resources, each of which is accessed via its own URL on the Self Administration port:

- Self-Management: Allows end users to modify their profile attributes.
- Self-Registration: Allows end users to register themselves as Select Access identities.
- Password Reset: Allows end users to change passwords.

By default, self-management and self-registration uses a JSP resource for each. The Select Access SDK includes a default JSP page for each Self Administration resource. You can modify these pages or create your own using the Web Administration interface. For more information on creating new JSP resources or modifying the template resources, refer to the *HP OpenView Select Access 6.2 Developer's Tutorial Guide*.

Once created, these resources should be copied into their respective folders (specified in the Administration server setup; by default, named `self_management`, `self_registration` and `password_reset` respectively). These folders can be found in:

```
<install_path>/shared/jetty/policy_builder/webadmin
```

Once the JSP pages have been added, you can add links to these pages in other resources where self-administration is required or useful. Adding them as resources in the Policy Builder allows you to set access policy for these resources just as you can for any other network resource.



If you add the registration JSP page as a static resource, you must give Unknown Identities access to it.

Enabling Administration Server Resources

In order for administrators or end users to access any of the Administration server resources, these resources must first be enabled. These resources can only be enabled only in Root Administration mode of the Policy Builder.

To enable an Administration server resource, you must:

- Enable Select Auth on the specific resource. Enabling Select Auth allows identities to connect to Administration server using the selected resource.
- Configure the authentication services. Any identity attempting to access one of the Administration server resources are authenticated with the authentication services you configure for that purpose.



If you are enabling Delegated Administration and you intend to use certificate-based authentication for Delegated Administration, ensure you manually copy your DER or PEM encoded X.509 CA certificates to this location on your Administration server:

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

Otherwise, the delegated administrator does not get prompted for the correct certificate. We recommend that delegated administrators also import their client certificate into their browsers. For details, see [Adding Delegated Administration CA Certificates](#) in the *HP OpenView Select Access 6.2 Installation Guide*.

To enable Select Auth on an Administration server resource

- 1 Right-click the **Select Auth** column beside the entry for the selected Administration server resource. By default, this resource is located in the **Administration Server** folder and is named **Delegated Administration**.
- 2 From the shortcut menu, click **Enable Select Auth**, shown in [Figure 122](#).

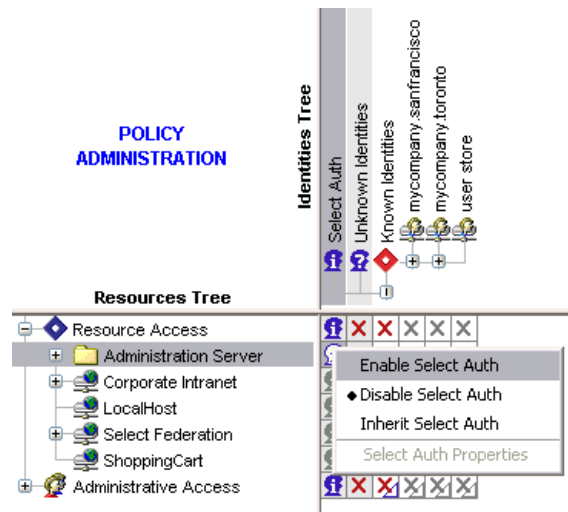


Figure 122Enabling Select Auth for Delegated Administration Resource

The **Authentication Properties** dialog box appears, as shown in [Figure 123](#). This tab allows you to specify which authentication services are to be used to authenticate the user.

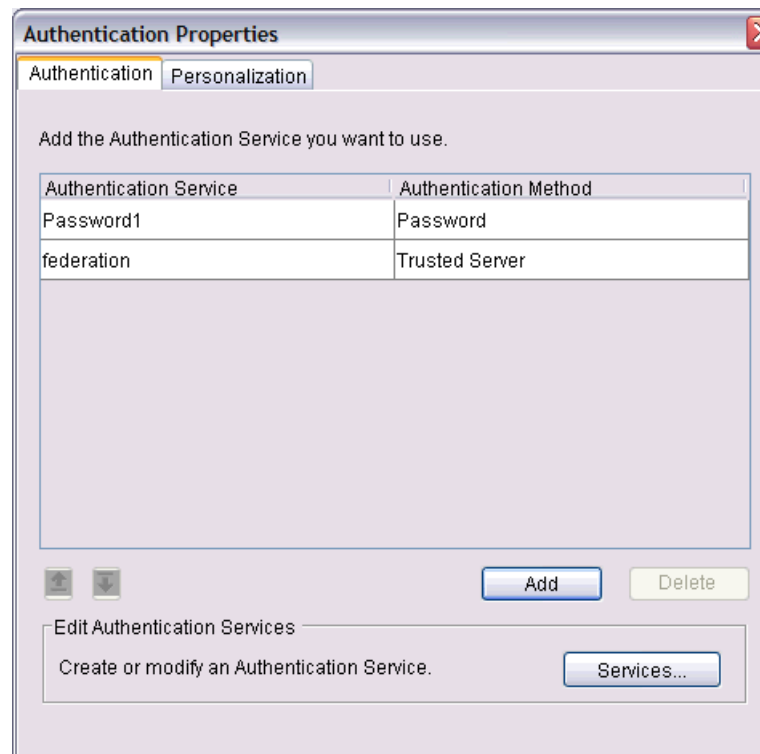


Figure 123Authentication Properties Dialog Box

- 3 Click **Add**. The **Available Authentication Services** dialog box appears, as shown in [Figure 124](#).

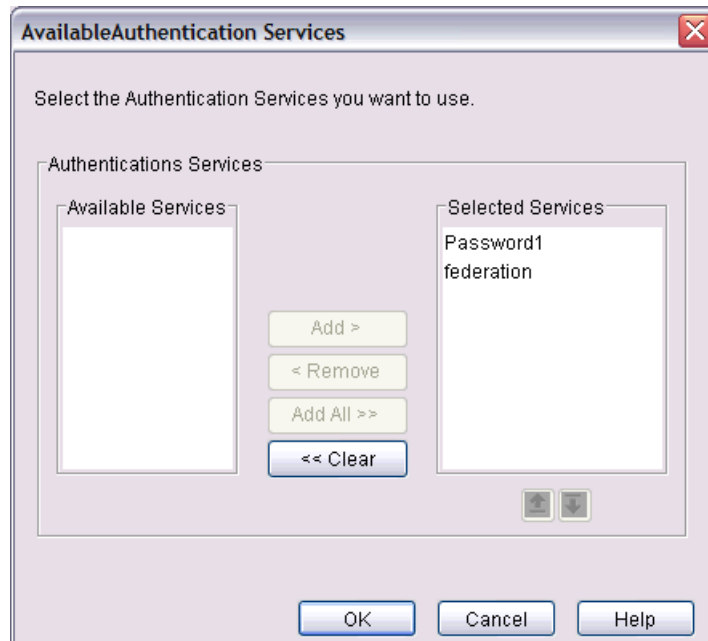


Figure 124 Available Authentication Services Dialog Box

This dialog box contains the following lists:

- The **Available Services** list contains the authentication services you have configured.
 - The **Selected Services** list contains the authentication services that are to be used.
- 4 In the **Available Services** list, select the service you want to use and click **Add**. The service moves to the **Selected Services** list.
 - Use CTRL+CLICK or SHIFT+CLICK to select multiple services.
 - 5 To remove a service, select the service in the **Selected Services** list and click **Remove**.
 - 6 Use the arrows to prioritize the services. The services are used in this order to try to identify an identity. (The arrows are also available on the **Authentication Properties** dialog box.)
 - 7 Click **OK** to close the **Available Authentication Services** dialog box.
 - 8 If you want to create or modify an authentication service, click **Services**. For details on creating an authentication service, see [Setting Up Your List of Authentication Services](#) on page 100.
 - A **Personalization** tab appears when you configure this dialog box. Personalization has no effect on this feature. You do not need to configure this tab.
 - 9 Click **OK** to close the **Authentication Properties** dialog box.

Using the Administration Matrix to Delegate Entitlements

You configure administration entitlements against identity profiles in the Administration Matrix, which is shown in [Figure 125](#).



To facilitate the way you assign entitlements to specific identities, create a centralized repository for all administrative identities. You can centralize administrative identities through any combination of folders, groups, and dynamic groups. For details, see [Building the Identities Tree](#) on page 31.

The Administration Matrix is part of the Resources Tree. You can find the Administration Matrix listed after the Resource Access branch in the Policy Matrix. The Administration Matrix automatically contains entries for four administrative categories: Attributes, Functions, Network Management, and User Management.



When you set the threshold value for the Administrative Access Matrix in the current administration session, the setting is not immediately recognized by the Policy Builder. However, if you exit and then restart the Policy Builder applet, the threshold value you set in the previous session is recognized.

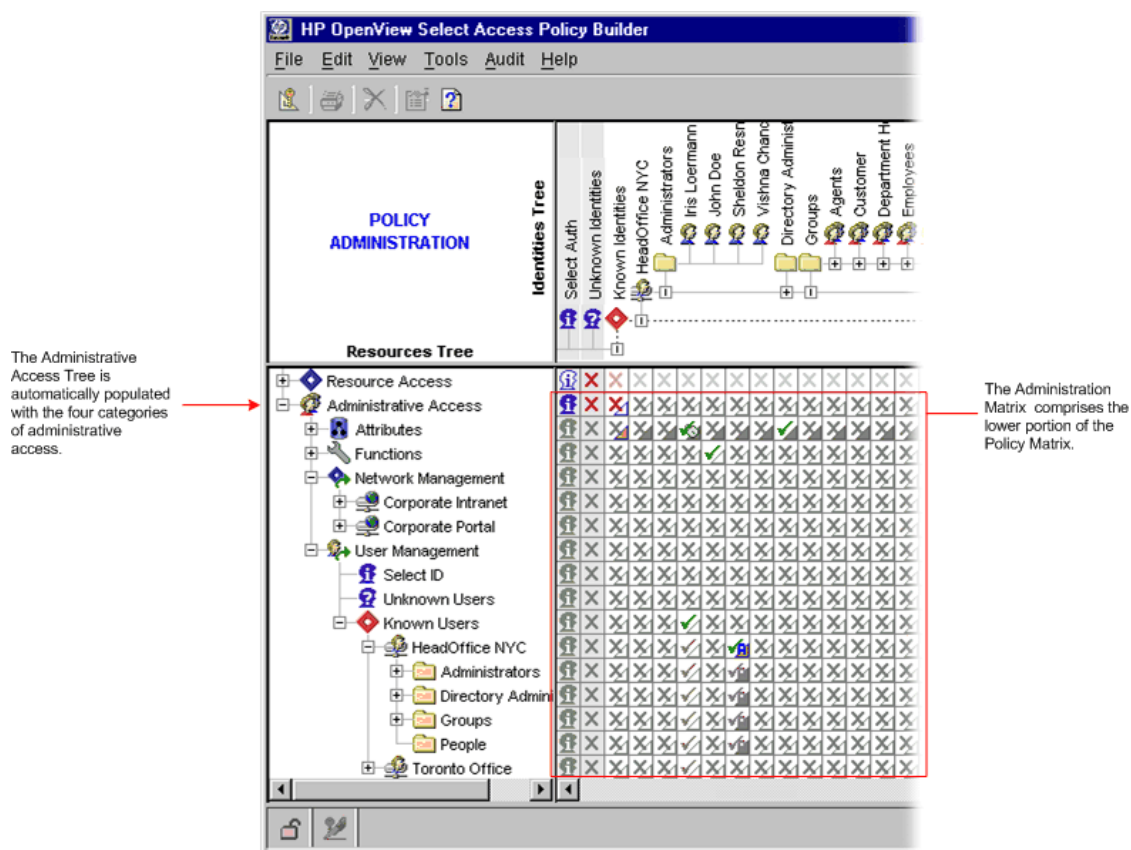


Figure 125Administration Matrix

About Administration Entitlements: Delegation and Workflow

Setting administration entitlements is slightly more complex than setting access policies in that each cell in the Administration Matrix actually stores two types of data:

- **Delegation policy:** Allows you to share administrative responsibilities amongst one or more authorized administrators. The policy sets the degree to which entitlements are granted: for example, full vs. partial control. It also sets what administration resources the identity has access to.

For more information on setting delegation the delegation policy, see [Chapter 11, Managing Delegation Policies](#).

- **Workflow condition:** When the workflow condition is enabled, you apply a workflow rule that restricts any change from taking effect until it has been approved by one or more authorized administrators. The workflow rule defines the list of administrators required to approve or reject any change, and is created with the Rule Builder.

For information on setting workflow policy, see [Chapter 12, Using Administration Workflow](#).

For information on creating workflow rules, see [Creating Workflow Rules](#) on page 221.

Delegation policies and workflow conditions are set independently of one another. However, workflow condition is subordinate to the delegation entitlements; if an identity does not have delegation entitlements for an administrative resource, enabling a workflow condition for that identity on that resource is meaningless.

The ability to set both a delegation entitlements and a workflow condition on a single cell allows administrators to improve efficiency by delegating administrative responsibilities to many administrators and to assure that the integrity of the information in the Policy Store is maintained. To see how workflow conditions and delegation policies are represented, see [How Administration Policies are Represented](#) on page 203.

How Administration Policies are Represented

Information in the Administration Matrix is represented slightly differently than in the Resource Policy Matrix since each cell in the Administration Matrix must represent both the delegation policy and the workflow condition.

The delegation policy and workflow condition share the cell as follows:

The Delegation icon is displayed centrally in the cell.  The Workflow icon is displayed in the lower right corner of the cell.

[Figure 126](#) shows an example of how icons represent administration policy in the Administration Matrix.

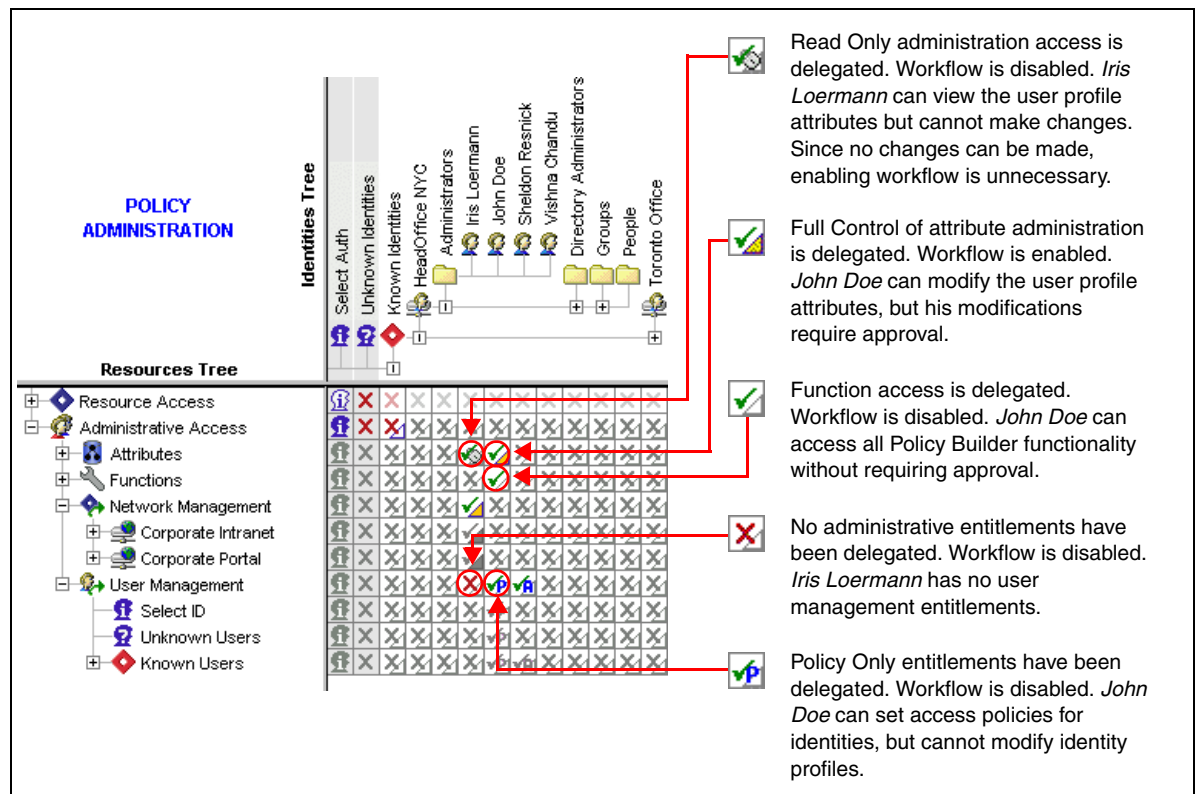


Figure 126 Administration Policy Representation

A colored icon indicates that the access policy was applied specifically to an entry, while a gray icon indicates that an access policy is inherited.

For more information on the icons that may be displayed in the Administration Matrix, see the following tables:

- [Table 30 in Chapter 11, Managing Delegation Policies](#) for a complete list of delegation policies and their associated icons.
- [Table 32 in Chapter 12, Using Administration Workflow](#) for a complete list of workflow conditions and their associated icons.

11 Managing Delegation Policies

This chapter advances the subject of administrative access first discussed in [Chapter 10, Controlling Administrative Access](#). It gives you the implementation details you need to set specific entitlements for identities, thereby granting them administrative responsibilities.

Creating delegation policies consists of a two-part process:

- 1 Enabling the ability to delegate administrative entitlements.
- 2 Setting administration entitlements for an identity.



HP recommends that administrators frequently refresh the Policy Builder by clicking **View** → **Refresh**. Because changes made by different administrators can often overlap, administrators need to refresh the Policy Builder often to ensure that it is displaying the latest data. This command updates information on the Identities Tree and Resources Tree in Policy Matrix and the Rule Builder, and in the authentication services list.

Chapter Overview

This chapter includes the following topics:

- [Enabling Delegation](#) on page 205
- [Assigning Administration Entitlements](#) on page 207
- [About Delegation Entitlement Inheritance](#) on page 213

Enabling Delegation

By enabling delegation in the Policy Builder, you allow identities to login with one or more combinations of credentials stored in the profile.



The Root Administration login should be reserved for the initial setup of Select Access and emergency cases only. If you are the candidate that has been charged with this duty, you should delegate entitlements to your own profile and use this login going forward.



By default, all Delegated Administration session timeouts are tied to the Policy Validator's **Client Idle Timeout** tuning parameter. The default value for this parameter is 10 minutes. If this value is too low, you may want to adjust this parameter accordingly. For details, see [Modifying Group and Override Parameters for the Enforcer Plugin](#) on page 255.

How Views Are Customized

If Select Auth authenticates administrators with the services configured for administration, they are presented with a custom view of the Policy Builder. The view they receive depends on the administration resources assigned to that identity. Not only does this allow Select Access to dynamically control the view of the Policy Builder, but it also allows actions to be audited properly.

Before you set specific delegation entitlements in the Policy Builder, you must enable delegation. By default, delegation is disabled in the Policy Builder. If delegation is disabled, any specific entitlements you may have already configured may appear grayed out.

To enable delegation

- 1 Right-click the cell where the Select Auth column and Administrative Access row intersect.
- 2 From the shortcut menu, click **Enable Delegation**. The **Authentication Properties** dialog appears.
- 3 Configure the Authentication services that are needed to authenticate delegated administrators. For details, see [Enabling Administration Server Resources](#) on page 199.



If you are delegating component configuration entitlements that require the use of the Setup Tool, you are limited to using Password authentication only.

About the Delegated Administration Enforcer plugin

Delegated Administration requires its own Enforcer plugin. Therefore, when you enable and configure Delegated Administration, an Enforcer plugin is automatically created for this mode. This Enforcer plugin appears in the **Component Configuration** window that appears when you click **Tools** → **Component Configuration**. While the Enforcer plugin for Delegated Administration appears in this window, HP strongly recommends that you avoid modifying its configuration. This Enforcer plugin has been configured specifically for Delegated Administration mode. Modifying its configuration parameters can result in unpredictable behavior.

However, if you are using Registration Authentication via the Administration server to register new users, and the Administration server and web server are on different machines or domains, you need to set certain SSO and/or MD-SSO parameters. This is the only exception for modifying this plugin's configuration parameters independently. For more information, see [Registration Authentication Service](#) on page 107.



Every time you reconfigure your Administration server, your Enforcer plugin for Delegated Administration is automatically reconfigured to propagate properties required by the Select Access system. To get this updated configuration information, you should disable and then re-enable Delegated Administration in the Policy Builder. This is particularly important if you have updated the number of Policy Validators deployed on your network. For details, see [To enable delegation](#) on page 206.

Assigning Administration Entitlements

Once you enable delegation, you activate the entitlements that are delegated to identities. You assign entitlements with the Administrative Access branch or the Resources Tree.

- If the cells in the Administration Matrix appear grayed out, you have not enabled Delegated Administration. For details, see [Enabling Delegation](#) on page 205.
- Refreshing your data is particularly important when multiple administrators are making changes simultaneously. However, HP recommends you try to minimize multiple, concurrent changes as much as possible.

To refresh data and ensure you have the most current data, click **View** → **Refresh**. The information currently shown in the Identities Tree, Resources Tree and Policy Matrix is refreshed.

Administration Resources You Can Delegate

To display the Administration Matrix, expand the nodes beneath the Administrative Access entry in the Resources tree. Four administrative categories are automatically displayed as entries:

- **Attributes:** Contains a list of profile attributes.
This list allows you to specify which profile attributes Delegated Administrators can view or modify. You can allow full or read-only access to any available attribute. Attributes can be delegated in varying degrees of granularity; you can delegate the entire list, an attribute group, or an individual attribute.
- **Functions:** Contains a list of the operations you can perform in the Policy Builder.
Entitling functions allows to you to specify which Policy Builder functions an administrator is able to access. Functions you can entitle are listed in [Table 29](#).
 - When you set the threshold value for the Administrative Access Matrix in the current administration session, the setting is not immediately recognized by the Policy Builder. However, if you exit and then restart the Policy Builder applet, the threshold value you set in the previous session is recognized.

Table 29 Policy Builder Functions Available for Entitlement

Function	Descriptions
Authentication Service Configuration	Adds new Authentication Services or modify existing ones.
Component Configuration	Configures the Administration server, Enforcer plugins, audit settings and Policy Validators.
Network Discovery	Runs the Network discovery tool to automatically add HTTP/HTTPS services to your Resources tree.
Password Policy Configuration	Specifies the parameters that all Select Access passwords must adhere to.
Password Reset Configuration	Configures a list of secret questions and other options related to resetting a password.

Table 29 Policy Builder Functions Available for Entitlement (cont'd)

Function	Descriptions
Policy Data Signing	Signs policy data and verify policy data signatures.
Rule Builder	Accesses the Rule Builder to create and modify policy and workflow rules.
Sub-Delegation Ability	Sub-delegates any administrative resources that they have access to. Policy Builder supports multiple levels of delegation. That means any administrator to whom administration has been delegated can, in turn, sub-delegate administration further.
Identity Editor Plugin Configuration	Configures any custom identity editor plugins.
Identity Location Configuration	Add, delete, and modify identity locations. Note: Delegated administrators need component configuration permission to configure this function.
Workflow Alert Template Configuration	Configures the SMTP server and the email templates used for workflow alerts.
Workflow Configuration	Configures the workflow grid. Setting up a workflow on an identity requires access to SMTP server information and the notification email template. Enabling Workflow Configuration grants the user permission to define a workflow in the policy grid. To have the permission to <code>_read_email template config</code> and <code>email server config</code> , a delegated administrator needs permission for the Workflow Alert Template function as well otherwise there is no way to construct email content.

- **Network Management:** Replicates the list of entries in the Resource Access tree.
Delegating network management allows you to specify which network resources delegated administrators can set and manage access policies for. Tasks these delegated administrators can perform include creating, editing, or deleting:
 - Conditional rules
 - Access policies
 - Clearing of Policy Validator's cache
- **Identity management:** Replicates the list of profiles in the Identities Tree.
Allows you to specify which identities in the Identities Tree delegated administrators can manage. Additionally, you can give them policy entitlements (the ability to set policy only), identity administration entitlements (the ability to administer the list of profiles only), or Root Administration entitlements (both policy and identity).

To set a specific delegation entitlement

- 1 In the Administration Matrix, right-click the cell where you want to apply a delegation policy, as shown in [Figure 127](#).

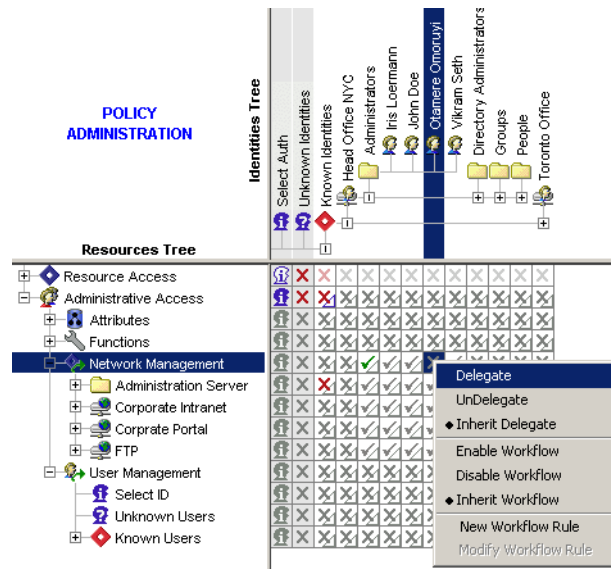


Figure 127Setting a Delegation Policy

- 2 Select a delegation policy. Each administration category has its own set of policies. You can choose from the options described [Table 30](#).
 - You must delegate attribute permissions separately from other categories of Administrative Access permissions. For example, if you want an identity to manage a group, as well as to be able to change a group's name, you need to set two delegation assignments:
 - **Full Control** for the group in question, and
 - **Full Control** for the `cn` attribute.
 - A Delegated Administrator with FULL or ADMIN privileges on a group can modify group membership regardless of the privilege on each group member. Delegating management of a group gives the administrator the ability to change what people can do by adding to or removing from the group, even if the administrator does not have permissions on the individual group members.

Table 30 List of Delegation Policy Options





Category	Option For	Description
Attributes	Full Control 	<p>Delegate the ability to view and modify activated identity profile attributes.</p> <p>A green check mark is shown in the central portion of the square. The entry (folder, group, or identity) in the Identities Tree is allowed access to the attribute or group of attributes in the Resources Tree.</p>
	Read Only 	<p>Delegate the ability to view identity profile attributes, but not to modify them.</p> <p>A green check mark with a padlock is shown in the central portion of the square. The entry (folder, group, or identity) in the Identities Tree is allowed to view, but not modify, the attribute or group of attributes in the Resources Tree.</p>
	Hidden 	<p>Hide identity profile attribute.</p> <p>A red X is shown in the central portion of the square. The entry (folder, group, or identity) in the Identities Tree is not allowed to view or change the attribute or group of attributes in the Resources Tree.</p>
	Inherit Delegation 	<p>Inherit the delegation policy used by the parent entry.</p> <p>A gray check mark or X is shown in the central portion of the square. The entries in the Identities Tree (folder, group, or identity) and the Resources Tree use the same access policy as their parent entry in the Administration Matrix.</p>

Table 30 List of Delegation Policy Options (cont'd)












Category	Option For	Description
Functions	Delegate 	<p>Delegate the ability to access and configure Policy Builder administrative functions.</p> <p>A green check mark is shown in the central portion of the square. The entry (folder, group, or identity) in the Identities Tree is allowed access to the function (for example, authentication service configuration, audit configuration data signing) in the Resources Tree.</p>
	Undelegate 	<p>Undelegate the ability to access and configure Policy Builder administrative functions.</p> <p>A red X is shown in the central portion of the square. The entry (folder, group, or identity) in the Identities Tree is denied access to the entry (for example, authentication service configuration, audit configuration data signing) in the Resources Tree.</p>
	Inherit Delegation 	<p>Inherit the delegation policy that allows or denies access to Policy Builder administrative functions.</p> <p>A gray check mark or X is shown in the central portion of the square. The entries in the Identities Tree (folder, group, or identity) and the Resources Tree use the same access policy as their parent entry in the Administration Matrix.</p>
Network Management	Delegate 	<p>Delegate the ability to manage a network resource.</p> <p>A green check mark is shown in the central portion of the square. The entry (folder, group, or identity) in the Identities Tree is allowed manage to the entry (folder, service, or resource) in the Resources Tree.</p>
	Undelegate 	<p>Undelegate the ability to manage a network resource.</p> <p>A red X is shown in the square. The entry (folder, group, or identity) in the Identities Tree is denied access to the entry (folder, service, or resource) in the Resources Tree.</p>
	Inherit Delegation 	<p>Inherit the delegation policy used by the parent entry.</p> <p>A gray check mark or X is shown in the central portion of the square. The entries in the Identities Tree (folder, group, or identity) and the Resources Tree use the same access policy as their parent entry in the Administration Matrix.</p>

Table 30 List of Delegation Policy Options (cont'd)

Category	Option For	Description
Identity Management	Full 	<p>Delegate the ability to administer security policy to identities as well as Select Access identity properties in the Identities Tree.</p> <p>A green check mark is shown in the central portion of the square. The entry (folder, group, or identity) in the Identities Tree is allowed manage the entry (folder, group, or identity) in the Resources Tree.¹</p>
	Policy Only 	<p>Delegate only the ability to administer security policy to identities.</p> <p>A green check mark with a P is shown in the central portion of the square. The entry (folder, group, or identity) in the Identities Tree is allowed to set policy for the entry (folder, service, or resource) in the Resources Tree.^a</p>
	Admin Only 	<p>Delegate only the ability to administer Select Access identity properties in the Identities Tree.</p> <p>A green check mark with a lock is shown in the central portion of the square. The entry (folder, group, or identity) in the Identities Tree is allowed to modify identity profile information for the entry (folder, group, or identity) in the Resources Tree.^b</p>
	None 	<p>No user management is permitted.</p> <p>A red X is shown in the central portion of the square. The entry (folder, group, or identity) in the Identities Tree is denied access to the entry (folder, group, or user) in the Resources Tree.</p>
	Inherit Delegation 	<p>A gray check mark or X is shown in the central portion of the square. The entries in the Identities Tree (folder, group, or identity) and the Resources Tree use the same access policy as their parent entry in the Administration Matrix.</p>

- a. If you have a Folder of administrators to whom you are delegating **Policy Only** privileges, but then delegate **Admin Only** privileges to a single identity, the profile for that identity temporarily disappears from the Administration Matrix. However, it does reappear when you refresh the Matrix.
- b. To delegate the ability to rename a profile (that is, modify the `cn` attribute), ensure you assign either the **Full** or **Admin Only** privileges as well as assign privileges over the user profile as well.

About Delegation Entitlement Inheritance

Delegated Administration entitlements are inherited differently than policies set in the Resource Access branch of the Policy Matrix; primarily because you cannot expand groups and dynamic groups under the Identity Management function of the Administrative Access branch. Therefore, you should note the differences documented in the subsequent sections.



The same logic used to evaluate delegation entitlements is also used by workflow evaluation.

Inheritance Restrictions on Groups and Dynamic Groups

If you set a delegation policy for a single administrator over a group or dynamic group on the Identity Management branch, the administrator can *only* set policy against the group. The policy does not get inherited by the individual identity profiles that are members that group or dynamic group. However, the policy would be inherited if the policy was set against a folder and groups and dynamic groups were organized within that folder.

For example, Annette Bater is delegated with Full control over the Administrators group as well as the Executive folder, as illustrated in [Figure 128](#) on page 214. Notice how delegation is inherited by identities in the folder but not by members of the group.

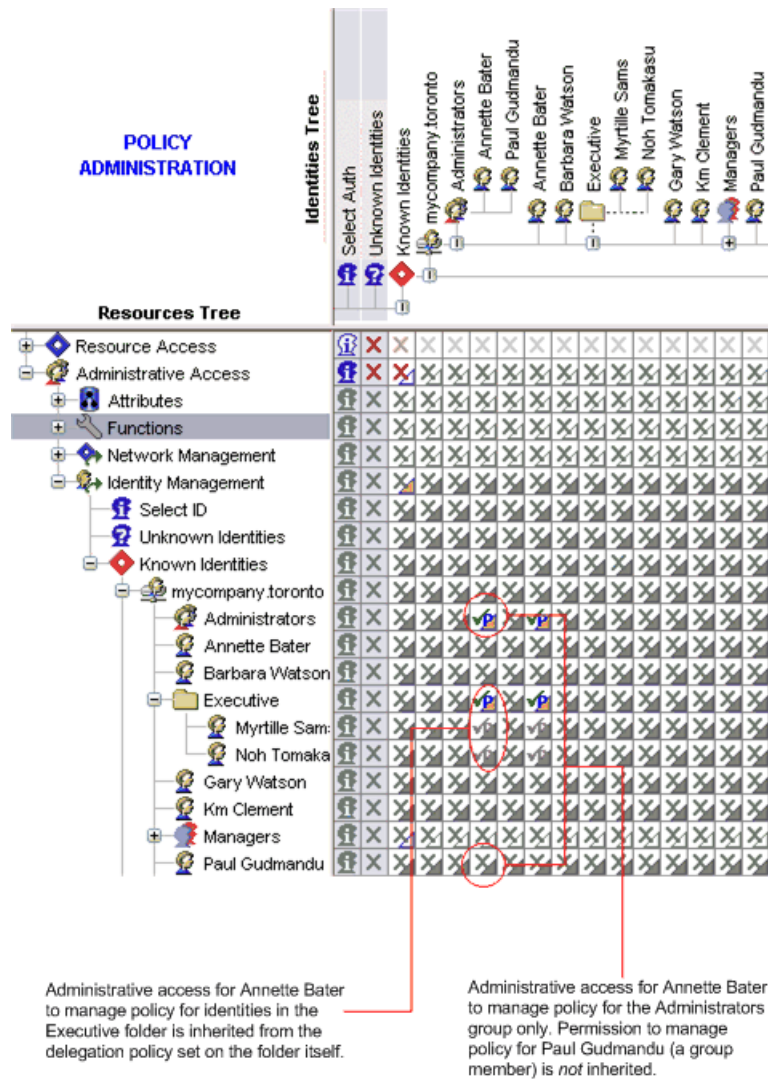


Figure 128 Delegated Inheritance Rule Example

Disinheritance Prevention

Administrators with delegation entitlements cannot remove delegation policies for other identities they have administrative access over, if the entitlement is inherited from a place on the Administration Matrix the administrator cannot see.

For example, Barbara Watson is delegated with Full control over the Accounts folder, as shown in [Figure 129](#) on page 215. This folder holds all the groups that correlate to account divisions to which different account managers may belong. Barbara can manage memberships over the groups as she is director of Sales. Barbara notices that Allistair Simon has the ability to also manage memberships for group, and tries to undelegate this ability from him. However, Allistair inherits this administrative ability because he is also a member of the Administrators group, a group that Barbara does not see in her view and therefore has not authority over. Barbara's attempt to disinherit Allistair therefore fails.

12 Using Administration Workflow

Administration workflow allows you to restrict user or policy changes from taking effect until they have been authorized by selected managers or administrators. This chapter describes how to use workflow to protect corporate data.

Because the administration of Select Access can be delegated and sub-delegated to any number of identities within an organization, the ability to manage the changes that are made and ensure that the integrity of the data is upheld is very important. A well-configured system should have checks and balances in place to ensure that the security of the data being protected is never compromised.

Chapter Overview

This chapter includes the following topics:

- [How Does Administration Workflow Work?](#) on page 217
- [Setting Up Administration Workflow](#) on page 218
- [Creating Workflow Rules](#) on page 221
- [Setting Workflow Conditions](#) on page 222
- [About Administration Workflow Inheritance](#) on page 224

How Does Administration Workflow Work?

When the Administration server receives a change request, it first checks entitlement and determines whether or not the request is subject to administration workflow. If workflow is not enabled for the operation, the change is processed immediately. If workflow is enabled, the following events occur:

- 1 The request is stored in the Policy Store.
- 2 Each administrator designated as an approver in the workflow rule is notified that a change request is pending.
- 3 The Administration server processes each response when it comes in.
- 4 When the required number of approvals or rejections is received, the Administration server:
 - Processes the change request by running it (if approved) or cancelling it (if rejected)
 - Sends a message to the audit log
 - Notifies the submitter of the final state of the request

- Notifies any approvers who have not yet responded to the initial request that the request has been processed
- Removes the change request from the Policy Store

Setting Up Administration Workflow

To set up administration workflow for delegated administrators in the Policy Matrix's Identities Tree, perform the steps outlined in [Table 31](#).

Table 31 Administration Workflow Overview

Setup Task	Details
1 Enable delegation.	Enabling Administration Server Resources on page 199
2 Click Tools → Workflow Configuration to configure the email parameters to enable the Administration server to send email alerts.	Configuring Email Options on page 218
3 Configure workflow rules, which contain the list of administrators who must approve any changes made by the delegated administrator.	Creating Workflow Rules on page 221
4 Set workflow conditions as required for any user/administrative resource in the Administration Matrix. Administrative resources are organized into the following categories: <ul style="list-style-type: none"> • <i>Attributes</i>: Lists the identity profile attributes for which you have either Full Control or Read Only entitlements. • <i>Functions</i>: Lists the Policy Builder functions to which you have access. • <i>Network Management</i>: Replicates the Resource Access tree • <i>User Management</i>: Replicates the Identities Tree. 	Setting Workflow Conditions on page 222

Configuring Email Options

Workflow alerts are message templates that the Administration server emails to each user listed as an approver in a workflow rule. They are automatically generated when a new change request is added to the database or when a request changes its state (rejected, approved, or executed).



If an administrator does not have a valid email address configured as part of their identity profile, workflow alerts cannot be sent.

In order for Select Access to successfully notify both the approvers and submitters of significant workflow events, you must configure the following:

- **Email profile information:** In order to send workflow alerts, you must provide email profile information for the Administration server. This includes:
 - The mail server through which alerts will be sent.
 - A valid email address from which the Administration server will send them.

For more information, see [To configure mail server properties for administration workflow](#) on page 219.

- **Alert template files:** Select Access installs three basic templates for workflow alerts, and is configured to use these by default. However, if you choose, you can change the default templates used. Should you use customized workflow templates, you will need to specify the file names so the Administration server knows which files to send for which events.



If you want to customize these forms for international characters, you need to add HTML entity codes for each character. For example, if you want to replace **Click on the link below to view the very important details of this change request** with a Japanese equivalent, you must take the Japanese characters and convert them to &XXXXX; entity encoding. Do not use a character map to insert Japanese characters in your HTML file templates via a Unicode text file; otherwise, the Japanese characters will not be included in the auto-generated email.

For more information, see [To change which templates will be used for workflow alerts](#) on page 220.

Setting Mail Server Properties

In order for the Administration server to send alerts to administrators, you must properly configure the mail server properties.

To configure mail server properties for administration workflow

- 1 Click **Tools** → **Workflow Configuration**. The **Workflow Configuration** dialog box appears.
- 2 Click the **SMTP** tab to display the SMTP parameters, shown in [Figure 130](#).

Figure 130 Workflow Configuration SMTP Dialog Box

- 3 Configure the fields of this tab as necessary:
 - **Mail server hostname:** The fully qualified name or IP address of the SMTP server that you use as your mail server.
 - **Mail server port number:** The port number used by your mail server. The default SMTP sever port is 25.

- **Email from address:** The email address the Administration server sends the message from when a workflow event is triggered.
- **Email from name:** The sender alias used to identify the Select Access Administration server.

4 Click **OK**.

Specifying Custom Workflow Alert Templates

In order to alert administrators of workflow events, the Administration server must know which template files to send in which situations.

By default, three templates are installed with Select Access, and the Administration server is automatically configured to use these. If you create customized forms, however, you must configure the Administration server to use them.



If you create new workflow alert templates, they must be stored in the `<install_path>\content` directory.

For more information on creating custom workflow alert templates, see the *HP OpenView Select Access 6.2 Developer's Tutorial Guide*.

To change which templates will be used for workflow alerts

- 1 Click **Tools** → **Workflow Configuration**. The **Workflow Configuration** dialog box appears, shown in [Figure 131](#), with the **Templates** tab displayed.

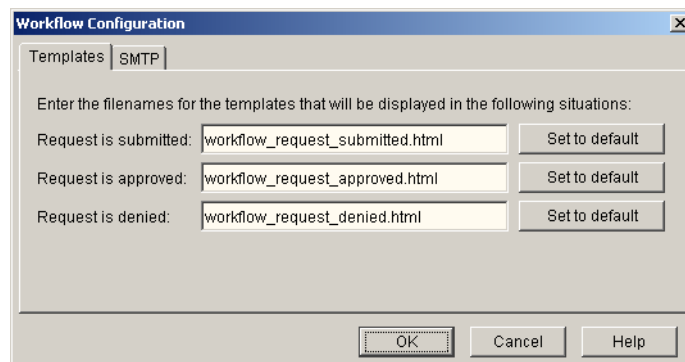


Figure 131 Workflow Configuration Templates Dialog Box

- 2 Configure the fields of this tab as necessary:
 - **Request is submitted:** Identifies the template sent to the list of approvers when the delegated administrator submits a change request.
 - **Request is approved:** When a change is approved, this template is sent to the submitting administrator and any approvers who have not yet responded to the initial change request.
 - **Request is denied:** When a change is denied, this template is sent to the submitting administrator and any approvers who have not yet responded to the initial change request.
- 3 Click **OK**.

Creating Workflow Rules

Workflow conditions are defined by a workflow rule. Like conditional access policy rules, workflow rules are created using the Rule Builder. However, whereas policy rules can be comprised of a number of different decision points which reflect a different condition to be met, workflow rules are comprised exclusively of one or more workflow decision points which define a list of approving administrators.

Workflow rules are created in the Rule Builder and define the approval process required for a change request. A workflow rule is comprised of one or more workflow decision points and ultimately terminates with either an Allow terminal point (for an approval), or a Deny terminal point (for a rejection).

Multiple workflow decision points can be added to a single rule and, as with conditional access rules, they can be comprised of a single branch or multiple branches. For information on how rules are constructed, see [Creating a Rule](#) on page 161. For details on how to configure a Workflow decision point, see [The Workflow Decision Point](#) on page 187.

Each workflow decision point is assessed sequentially. However, if an administrator is defined as an approver in more than one decision point in the rule, he is only notified once; his original response is treated as his response for any subsequent decision points.

Workflow rules are created in the Rule Builder and define the approval process required for a change request. A workflow rule is comprised of one or more workflow decision points and ultimately terminates with either an Allow terminal point (for an approval), or a Deny terminal point (for a rejection).

To create a new workflow rule

- 1 Click **File** → **New Rule**. The **Create New Rule** dialog box appears.
- 2 Select the **Workflow** rule type and enter a name for the rule, then click **OK**.
 - ▶ Only the following alphanumeric characters can be used in a rule name: A–Z, 0–9, _ . All others are invalid characters, and the Rule Builder does not accept them.
- 3 Select a workflow decision point from the Rule Builder toolbar by clicking its icon. The **Workflow Properties** dialog for the selected decision point appears.
- 4 Configure the properties for the decision point. For details, see [To configure a Workflow decision point](#) on page 187.
- 5 Add the decision point to a branch of the rule. To add any decision or terminal point to a branch:
 - Move your cursor to the insertion point of your rule. When you have moved the decision point to a valid insertion location, the branch arrow is highlighted.
 - Click to insert the decision point or terminal point at that location.
- 6 Repeat Steps 3-5 to add any additional decision or terminal points.

Setting Workflow Conditions

You apply workflow conditions to an identity/resource pair in the Administration Matrix. The Administration Matrix comprises the lower portion of the Policy Builder's Policy Matrix.

As with security policy, each workflow condition is set for a specific user/resource combination, and is inherited in the same way.

Applying a Workflow Condition

There are three possible workflow conditions you can apply to any cell in the Administration Matrix: **Enable Workflow**, **Disable Workflow**, or **Inherit Workflow**. The default setting for the Administration Matrix is **Inherit Workflow**.

- To apply a workflow condition for newly-registering users, enable workflow on the folder where new profiles are added. This allows administrators to approve or reject new profiles before Select Access writes them to the directory server.

To apply workflow conditions

- 1 In the Administration Matrix, right-click the cell where you want to apply a workflow condition, as shown in [Figure 132](#).

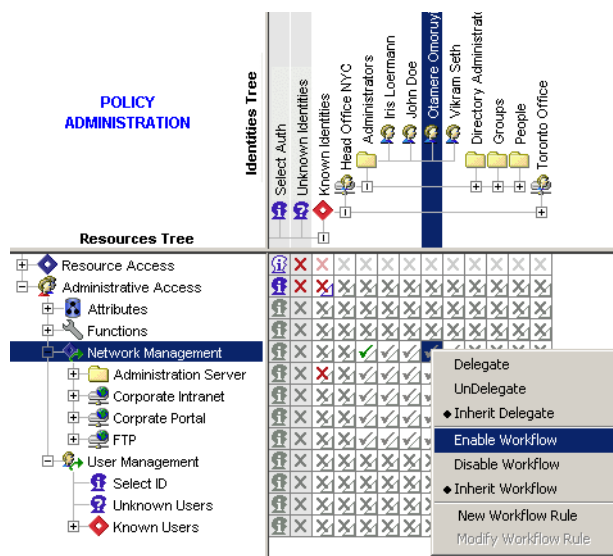






Figure 132Applying Workflow Conditions

- 2 Select an access policy. You can choose from the options described in [Table 32](#).

Table 32List of Workflow Conditions

Icon	Description
Enable Workflow 	Require approval for any changes made by an identity with Delegated Administration entitlements. To set this policy: <ol style="list-style-type: none">1 Right-click the square and select Enable Workflow.2 In the Workflow Rule Selection dialog box, select a rule and click OK. The rule is applied to the cell and a yellow triangle is displayed in the lower right corner.3 If you have not yet created any rules, a message appears asking if you want to create one. Click Yes. For details on how to create a rule, see Creating Workflow Rules on page 221.
Disable Workflow 	Allow an identity with Delegated Administration entitlements to make changes without requiring approval. An empty triangle is displayed in the lower right corner of the cell.
Inherit Workflow  	Inherit the workflow policy used by the parent entry. A gray triangle, either filled (inherit enabled workflow) or empty (inherit disabled workflow) is shown in the lower right corner of the cell.
New Workflow Rule	Display the Rule Builder to create a new rule. <ol style="list-style-type: none">1 Use the Rule Builder to create and save the rule. For details on how to create a rule, see Creating Workflow Rules on page 221.2 Exit the Rule Builder. (Click File → Exit.)3 The rule is applied to the cell and a yellow triangle is shown in the lower right corner.
Modify Workflow Rule	Display the Rule Builder to modify an existing rule. <ol style="list-style-type: none">1 Use Rule Builder to modify and save the rule. For details on how to modify the rule, see To modify a rule on page 163.2 Exit Rule Builder. (Click File → Exit.)3 The rule is applied to the cell and a yellow triangle is shown in the lower right corner.

Applying Workflow to the Creation of New Identity Profiles

The creation of new identity profiles is a special situation in terms of applying a workflow condition. Creating new identity profiles effectively adds a new administrative resource to the Administration Matrix. However, because the cell does not actually exist until after the required number of administrators have approved the change, no workflow condition can be placed on the affected cell.

To ensure that the addition of new identity profiles are subjected to workflow, you must apply the workflow condition to the folder, group, or dynamic group to which the new profile is being added.

About Administration Workflow Inheritance

Administration workflow is inherited the same way access policies are inherited. Therefore, inheritance occurs down the Select Auth column and across both the Resources Tree and Identities Tree. Workflow cannot be assigned to unknown identities, so this column is ignored.

For more details on how inheritance rules affect administration workflow, see [About Access Policy Inheritance](#) on page 133. The same logic described in this section applies to workflow inheritance. The only exception occurs when multiple workflow conditions are inherited.

When a Pairing Inherits Multiple Workflow Conditions

Just as with access policy, there may be occasions when an identity and resource pairing inherits two or more different workflow conditions. Rules for resolving multiple inherited workflow conditions are as follows:

- If a grid inherits multiple workflow rules, any one takes effect, if none of the workflow conditions are disabled. Each condition is evaluated, one by one, until an Approval is found, or until the end of the list of workflow rules is reached. (That is, the result of each workflow rule is Rejected, and the evaluation result is Rejected). The evaluation order of the workflow rules is dependent upon the inherited DN hash value. The order is the same as the order Select Access displays the inheritance in the grid tooltip.
- If one of the inherited workflow conditions is workflow disabled, then any inherited workflow conditions are ignored and workflow is not applied.

Workflow Inheritance and Delegation

A workflow condition is applied to a specific administrator/resource combination. As a result, each administrator has his own workflow configuration. The delegation of a resource from one administrator to another, therefore, does not affect how workflow is inherited by the sub-administrator.

The separation of the workflow condition and the delegation policy means that irrespective of who delegated administrative entitlements, each administrator is always subjected to their own workflow conditions.

For example, suppose Iris Loermann has permission to set access policy for all corporate intranet resources, and has workflow enabled for this function. She subdelegates this entitlement to John Doe, who has inherited a disabled workflow condition for this function.

Although Iris Loermann is subjected to a workflow rule if she were to modify an access policy, she does not pass her workflow condition on to John Doe. So even though John Doe only received access because Iris Loermann delegated it to him, he actually has greater freedom to set access policy than she does.

Using Inheritance to Set Workflow Conditions with Delegation Entitlements

The principle difference between setting access policy and setting administration policy is that, in the Policy Matrix, you can set only one policy for each cell, while in the Administration Matrix, you can set both a delegation entitlement and a workflow condition in a single cell. For details, see [How Administration Policies are Represented](#) on page 203.

While delegation and workflow are set independently of one another, the workflow condition is subordinate to the delegation policy; that is, if an identity does not have delegation entitlements for an administrative resource, then enabling workflow for that user on that resource has no effect, since no change request is possible.

However, despite its dependence on delegation permission, the Policy Builder still allows you to enable workflow on a cell for which delegation has not been set. By doing so, it allows you to make use of inheritance to simplify administration policy management.

For example, if you know that every user in a group should be subject to workflow, even though only a few of those identities will be given delegation entitlements, you can set workflow policy for the entire group, then set the delegation policy on an identity by identity basis.



For specific details behind inheritance logic, see [About Delegation Entitlement Inheritance](#) on page 213.

Administering Change Requests

The administration of change requests is done via JSP pages included as part of Select Access. These pages are served on the same port as form-based administration, but uses a unique URL. Both administrators and submitters can use this port and URL to access workflow pages via:

- Email notifications that summarize the change
- Form-based administration links

Once the administrator/submitter logs in, a list of change requests appear. [Table 33](#) summarizes the actions each can perform.

Table 33 Change Request Actions Available

Action	Submitter	Approver
Select a change request from a list.	•	•
View the properties of each submitted change request: <ul style="list-style-type: none">• What the change is• What the original values were• Who the approvers are• Who has approved the change• The current status	•	•
Cancel/revert the change to its original state, if it has not yet been executed.	•	
Reject the change.		•
Approve the change.		•

Managing Change Requests as a Submitter

If you are an administrator subjected to workflow, you can monitor the progress of your requests. If for any reason the change you have requested approval for is incorrect, inaccurate, or incomplete, you can revert the change to its original state, provided it has not yet been approved and executed.



An issue exists when using the << and >> links to browse through multiple pages of workflow change requests. After approving a change request, these links do not function as expected, bringing you back to the main **Workflow Change Request** page instead of the next page in the list of requests. However, from this page, they again function as intended.

To check the status of a pending change request

- 1 As shown in the image below, the **Change Request Status** page that lists all requests submitted for approval. Click the change request you wish to view information about. You can click on either the change's:

- Description
- Decision



If the request does not appear on the page you are looking at, you can scroll through subsequent pages by clicking the **Next** link or you can simply click the page number link if you know the request's location.

SelectAccess Workflow Change Request Status

ID	Date/Time	Description	Decision
1	Mon Mar 28 15:47:56 EST 2005	Access rule change on the policy matrix for "Joel/New Group23" and "Network".	Revert

[<< Back](#) [Home](#) [Forward >>](#)

Figure 133Workflow Change Request Status Page

- 2 If you clicked the **Description**, the **Workflow Change Description** page appears, as shown in [Figure 134](#).

SelectAccess Workflow Change Description

Change ID:	1
Date/Time:	Mon Mar 28 15:47:56 EST 2005
Submitter:	Workflow User Workflow User
Workflow Name:	workflow2
Approval	Need 1 more approval(s) to approve current decision point. Need 1 more rejection(s) to reject current decision point.
Description:	Access rule change on the policy matrix for "Joel/New Group23" and "Network".
Resource:	Network
Subject:	Joel/New Group23
Changed Values	
Access rule policy	Old: inherit
	New: allow

Figure 134Workflow Change Description Page

The **Workflow Change Description** page lists all the details of the change request, including:

- The request ID, which is used to track the status of the change request.
 - The time the request was submitted.
 - The workflow name, which is used to identify the rule triggering the approval chain.
 - The approval status. Click this link to see the a detailed summary of the approval status. For details, see [To check the approval status](#).
 - A brief text summary that describes the change.
 - A comprehensive summary of the original value as well as what the value is being changed to upon approval.
- 3 To revert the change back to its original value click **Revert**. The **Confirm Revert** page appears.
- Request execution may fail because of conflicts. Irrespective of the success or failure of the approval, the workflow thread updates the state of request and generates alerts to approving administrators.

Managing Change Requests as an Approver

If you are designated as an approving administrator in a workflow rule, you have the ability to approve or reject any change request which uses that rule. Should you reject a change request, you can optionally provide your reason for rejecting it. Once you have responded to a request, the Administration server updates the workflow record and evaluates whether enough approvals or rejections have been received.

- An issue exists when using the << and >> links to browse through multiple pages of workflow change requests. After approving a change request, these links do not function as expected, bringing you back to the main **Workflow Change Request** page instead of the next page in the list of requests. However, from this page, they again function as intended.

Whenever a change request is made for which you are listed as an approver, the Administration server notifies you via an email alert. This email contains links to the following URLs:

- The **Select Access Workflow Change Description** page, which details the change request that has just been submitted, and allows you to approve or reject the rule immediately.
- The **Select Access Workflow Change Request Approval** page, which provides an itemized list of change requests that are awaiting a response from you. You can open and respond to any change request listed at any time.

To view change requests awaiting your response

- 1 In the **Workflow Request Approval** page that lists all requests that require approval, click the change request you wish to view information about. You can click on either the change's:
 - ID
 - Description
 - Action

▶ If the request does not appear on the page you are looking at, you can scroll through subsequent pages by clicking the **Next** link or you can simply click the page number link if you know the request's location.

SelectAccess Workflow Change Request Approval

ID	Date/Time	Submitter	Description	Decision
1	Mon Mar 28 15:47:56 EST 2005	Workflow User Workflow User	Access rule change on the policy matrix for "Joel/New Group23" and "Network".	Approve Reject

[<< Back](#) [Home](#) [Forward >>](#)

Figure 135 Workflow Change Request Approval Page

If you clicked the **Description**, the **Workflow Change Description** page appears, as shown in [Figure 134](#). The **Change Description** page lists all the details of the change request, including:

- The request ID, which is used to track the status of the change request.
 - The time the request was submitted.
 - The workflow name, which is used to identify the rule triggering the approval chain.
 - The approval status. Click this link to see the a detailed summary of the approval status. For details, see [To check the approval status](#) on page 229.
 - A brief text summary that describes the change.
 - A comprehensive summary of the original value as well as what the value is being changed to upon approval.
- 2 To approve the change and allow Select Access to execute the request:
 - Click **Approve**. The **Confirm Approval** page appears.

- Click **Approve** again to execute the change request.
- 3 To reject the change and revert the change to its original state:
 - Click **Reject**. The **Confirm Rejection** page appears.

If you want to explain the reason for rejecting the request, type a brief summary in the optional text box provided. Otherwise, simply click **Reject** to restore the change and cancel the request for approval.

- ▶ Request execution may fail because of conflicts. Irrespective of the success or failure of the approval, the workflow thread updates the state of request and generates alerts to submitting administrators.

To check the approval status

- 1 In either the **Change Description** page (for approvers) or the **Change Status** page (for submitters), click the **Approvals** link. The **Change Approval Status** page appears.
 - To see the number of outstanding approvals required to execute the change, review the details in the **Decision Point Requirements** row.
 - To review which administrators have approved, rejected, or not responded to the request, review the list of administrator names in the corresponding rows.

13 Changing Audit Settings

This chapter introduces you to the term “audit.” It also describes how you use the Policy Builder to change those parameters initially configured when Select Access components were installed.

Chapter Overview

This chapter includes the following topics:

- [Understanding Audits](#) on page 231
- [Configuring Audit Settings from the Policy Builder](#) on page 231

Understanding Audits

Audit settings define a set of rules for detailing how to record events or transactions such as:

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

These recorded events and transactions are useful both to maintaining security of protected resources and ensuring data integrity.



You can set up auditing in two ways, depending on the size of your Select Access deployment. For larger or geographically dispersed deployments, HP recommends that you use a client/server model where the Select Audit Server centralizes logs that were forwarded to it by Select Access clients. In this case, you need configure the Select Audit Server as the output destination for each corresponding component. For smaller, locally based deployments, you can simply configure a local output destination.

Configuring Audit Settings from the Policy Builder

You can change the audit settings used by different Select Access components with the Policy Builder as well as the Setup Tool. You can make changes to the following levels of audit settings:

- Administration server settings, which set the common audit settings shared by all Select Access components.

- Default audit settings, which are shared by a specific component group: Policy Validators and Enforcer plugins.
- Individual override settings, which are used by a single instance of a component only.

How You Can Configure Audit Settings

There are different ways you can change these settings from the Policy Builder, depending on what type of changes you need to make:

- Update Select Access common settings and Administration server settings by clicking **Audit → Default Audit Settings → Administration Server and System Defaults**.
 - The Administration server uses common audit settings that you set for the system. You cannot set unique settings for the Administration server.
 - Since the Policy Builder is an applet running on the Administration server, you cannot configure separate audit settings for it. Any audit data you need to capture must be configured via the Administration server audit settings.
 - Any changes you make via the Policy Builder overwrite what you initially configured with the Setup Tool. The Policy Store subsequently accepts changes from either tool, using the most current changes as Select Access' new defaults.
- Update group defaults by:
 - Clicking **Audit → Default Audit Settings → Validators**.
 - Clicking **Audit → Default Audit Settings → Enforcers**.
 - Clicking **Tools → Component Configuration**, and right-clicking the corresponding component group in the list of available components. For details, see [Changing Configuration for a Group](#) on page 252.
- Override settings by clicking **Tools → Component Configuration**, and right-clicking the corresponding component group in the list of available components. For details, see [Changing Override Parameters](#) on page 253.

To change common and/or group default audit settings

- 1 Do one of the following:
 - To change the Administration server's settings (which also changes the common settings used by the entire Select Access system unless you have created group defaults or individual component overrides), click **Audit → Default Audit Settings → Administration Server and System Defaults**.
 - To change group defaults, click either **Audit → Default Audit Settings → Validators** or **Audit → Default Audit Settings → Enforcers**.
 - To change or create individual component overrides, see [Changing Override Parameters](#) on page 253.

This displays the corresponding **Audit Configuration** dialog box.

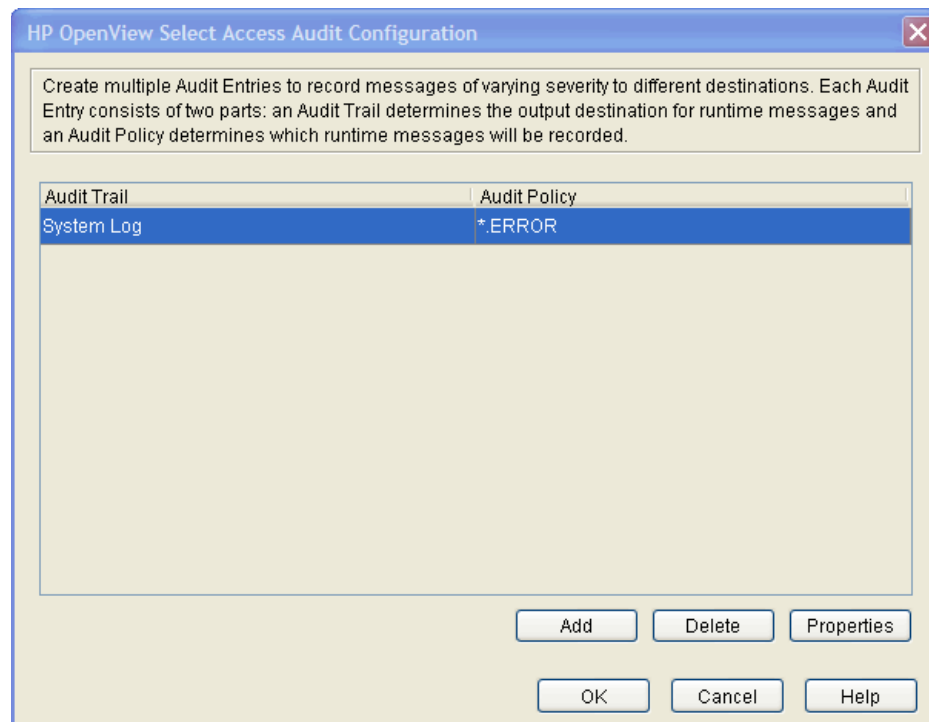


Figure 136 Audit Configuration Dialog Box

- 2 Review the audit settings that appear. To change these settings, do one of the following:

- To create or modify audit settings rows, click **Add** or **Properties** respectively. The **New Audit Entry** dialog box appears displaying two tabs, **Audit Trail** and **Audit Policy**. These tabs correspond to the columns of the **Default Audit Settings** setup screen.

When you configure the tabs of the **New Audit Entry** dialog box and click **OK**, a new row is added below the one you have selected, and the cells get populated automatically. For details, see [Configuring an Audit Trail](#) on page 233 and [Configuring an Audit Policy](#) on page 237.

- To remove an empty or populated row, select the entry in question and click **Delete**.

- 3 Click **OK** to commit these changes to the Policy Store.

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 Display the **Audit Entry** dialog box by following the procedure described in [To change common and/or group default audit settings](#) on page 232.
- 2 Click the **Audit Trail** tab.

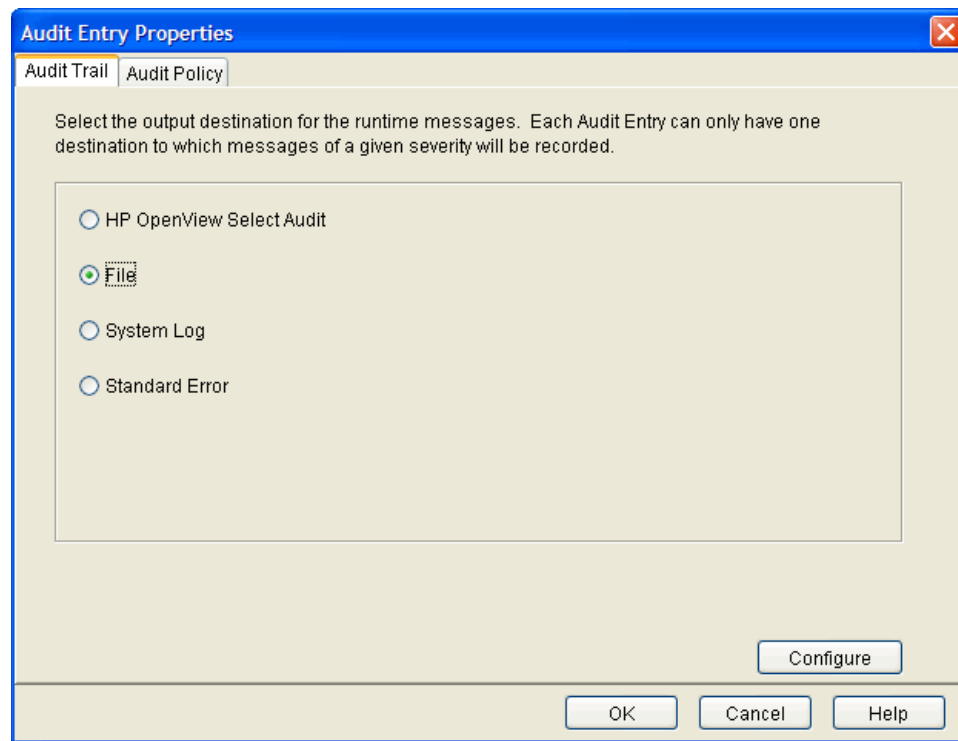


Figure 137Audit Trail Tab

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

► You can configure different audit trails for different events.

Table 34 Configuring the Audit Trail Tab

Output Destination	Description
HP OpenView Select Audit	Outputs to Select Audit.
File	Outputs to a text file. For example, you can send less important messages to a file to reduce network overhead.
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 Select Audit

If you are using Select Access with Select Audit, you must configure Select Audit to receive audit information.

To configure Select Audit:

- 1 From the **Audit Trail** tab on the **New Audit Entry** dialog box:
 - Choose the **HP OpenView Select Audit** option.
 - Click **Configure**.

The **Audit Trail — HP OpenView Select Audit Properties** dialog box appears.

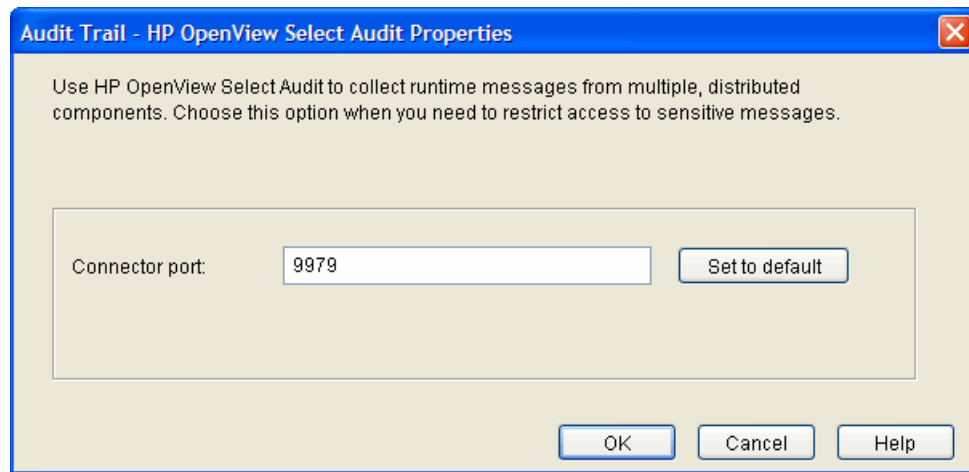


Figure 138 Audit Trail — HP OpenView Select Audit Properties Dialog Box

- 2 In the **Connector Port** field, enter the port on which Select Audit will listen for messages. By default, the port for the Select Audit server is 9979.
- 3 Click **OK**.

Configuring a Log File

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

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

For more details on how to create a report, see the *HP OpenView Select Audit 1.0 Administration Guide*.

To configure a log file

- 1 From the **Audit Trail** tab on the **New Audit Entry** dialog box:

- Choose the **File** option.
- Click **Configure**.

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

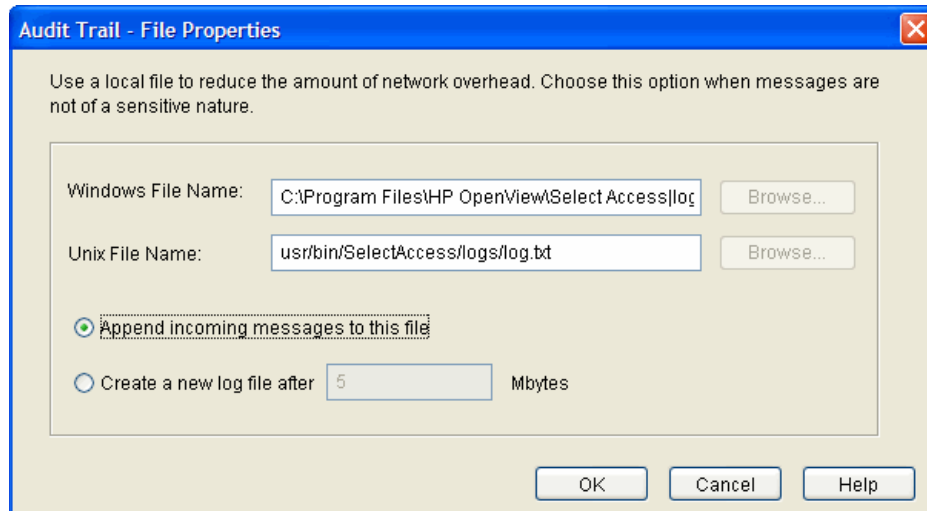


Figure 139 Audit Trail — File Properties Dialog Box

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

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

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

- 4 Click **OK**.

Configuring System Logging

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



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



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

To configure system logging

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

Configuring a Standard Error Stream

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



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

To log to standard error

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

Configuring an Audit Policy

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

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.

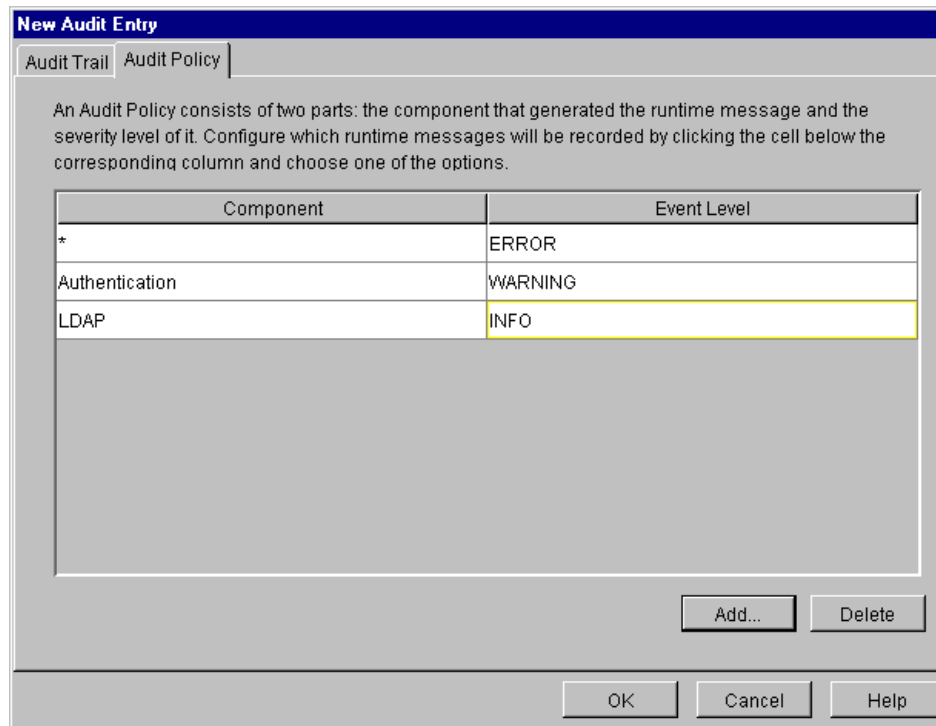


Figure 140New Audit Entry Dialog Box: Audit Policy Tab

To create an Audit Policy

- From the **Audit Configuration** screen 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.
- Click the **Audit Policy** tab to identify the events you want to record.
- To add a new policy to your list of policies, click **Add**.
- To choose the Select Access stream where you want events and messages logged, click the **Component** cell and choose one of the following:
 - ***: Records all events and messages for all streams listed below.
 - Admin Session**: Records events and messages that relate to administration login and logout.
 - Alert**: Records messages generated from an alert decision point that is part of an existing conditional rule.
 - Authentication**: Records events and messages that relate to authentication methods and Enforcer plugins.
 - Cache**: Records events and messages that relate to the caching of identity information and access rules in the Policy Validator.
 - Certificate**: Records events and messages that relate to certificates. For example, processing a certificate query involves multiple processes. Occasionally a certificate query for a transient identity (one that has been synthesized because user data is in a different data source) might take priority over another query. If another query is

interrupted by a certificate query, you see an informational message that says: short-circuiting. This just means that the Policy Validator is not rerunning the complete certificate verification process.

- **Enforcer plugin:** Records events and messages generated by your plugins on your network.
- **LDAP:** Records events and messages that relate to activity between the directory server and Select Access components.
- **Operation:** Records general operation of Select Access components.
- **Password Management:** Captures any password reset events or messages you require.
- **Policy:** Records events and messages that relate to access policies, when someone adds, deletes, and modifies a policy, and by whom.
- **Query:** Records all queries to Policy Validator. If you choose to log query information, Policy Validator logs a message for every access request. On a busy site, this can result in a lot of data being generated as well as a lot of overhead.
- **SOAP Message:** Records log messages between Select Audit and the respective Select Access component acting as the server's client.
- **System:** Records all system messages.

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

- **Workflow:** Records all workflow events.
- **Password Policy Verifier:** Records problems related to the Password Policy
- **Admin API:** Records actions called through the Admin API

➤ Refer to the *HP OpenView Select Access 6.2 Developer's Tutorial Guide* for more information.

- 5 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.

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

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 log 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 35 Common Component and Event Level Combinations

Information Captured	Component Selected	Level Selected
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
Record modification to: <ul style="list-style-type: none">• Group membership• Identities Tree or Resources Tree entries and folder properties• Authentication servers• Access rules	Policy	Info
Select Audit combinations		
Record initialization errors.	Operation	Warning
Track log messages' process errors.	Operation	Error
Record startup and shutdown of the Select Audit server.	Operation	Info
Record changes made to the Select Audit server configuration.	Admin Session	Info
Policy Validator combinations		
Track when the Policy Validator flushes the cache.	Policy	Debug

Table 35 Common Component and Event Level Combinations (cont'd)

Information Captured	Component Selected	Level Selected
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
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 • Identities 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

Table 35 Common Component and Event Level Combinations (cont'd)

Information Captured	Component Selected	Level Selected
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
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 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 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 35 Common Component and Event Level Combinations (cont'd)

Information Captured	Component Selected	Level Selected
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 Resources 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
Track things like: <ul style="list-style-type: none"> • SSO activities (redirects, finding SSO nonces) • Opening new Policy Validator connections 	Enforcer	Debug
SAML combinations		
Record users who have been sent to a SAML server that accepts in-bound transfers.	SAML Out	Info
Record users who have been transferred and accepted by a Select Access SAML server that accepts in-bound transfers.	SAML In	Info

Table 35 Common Component and Event Level Combinations (cont'd)

Information Captured	Component Selected	Level Selected
Record messages that occur as a result of a SAML server sending out-bound transfers. (For example, what the assertion artifact is.)	SAML Responder	Warning
Record 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

14 Managing Your Policy Data

This chapter describes the policy data you create, how it is stored, and how you can better manage that data.

Chapter Overview

This chapter includes the following topics:

- [What is a Policy Store?](#) on page 245
- [What Data Gets Recorded to the Policy Store](#) on page 245
- [Protecting Policy Data Recorded in Your Policy Store](#) on page 247

What is a Policy Store?

When you first configured Select Access' Administration server, you selected a location on a directory server on your network that acts as your Policy Store. This location can be:

- On the same directory server as one of your identity locations
- In a different directory server away from any user data

Your Policy Store records all data specific to Select Access, so that you can manage this policy data separate from any user data that exists on your directory system. It also minimizes the likelihood of one affecting the other, if one system becomes corrupted or is attacked by an intruder.

What Data Gets Recorded to the Policy Store

Policy data recorded in the Policy Store includes information on the following things:

- Access policies
- Conditional access rules and rule components
- Authentication methods and service configuration
- Centralized component configuration parameters
- Services and their resource entries
- Class files
- Serialized objects

These items are recorded in XML entries on the directory server acting as your Policy Store. Entries are created whenever an authorized administrator creates or modifies policy-related data via Policy Builder. Depending on the security requirements of your organization, you can set up the Policy Builder to sign these entries to prevent tampering. For details, see [Protecting Policy Data Recorded in Your Policy Store](#) on page 247.

Updating Policy Data Cached by the Policy Validator

To minimize the amount of network overhead generated by Policy Validator queries to the Policy Store (which is again multiplied by the numbers of Policy Validators you have added for your specific network requirements), the Policy Validator caches policy data it has already retrieved from the Policy Store. In addition to policy data, transient identity profiles are also cached.

To update the Policy Validator cache

- 1 Configure how often you want the cache to be managed. You configure cache preferences when you set up the Policy Validator during installation via its **Tuning Parameters** setup screen. The three fields you need to configure are:

- **Cache refresh interval**
- **Cache cleanup interval**
- **Cache cleanup percent**

For details, see [To configure central Policy Validator parameters](#) on page 267.

- 2 Manually clear the Policy Validator's cache if the Policy Validator needs the new information before the cache is automatically updated. You can do this in two ways:
 - Clear the cache after you have been warned of changes that impact the Policy Validator to allow or deny user access to a restricted resources. For details, see [To enable warnings when policy data affects the Policy Validator](#) on page 246.
 - Clear the cache by clicking **Tools** → **Clear Validator Cache(s)**. Click **Yes** or **Clear caches now** depending on the warning message box that appears.

To enable warnings when policy data affects the Policy Validator

- 1 Click **File** → **Configure Client Settings** and click the **Enable Warnings** tab.
- 2 Select **Display a warning to clear the Policy Validator cache**.
- 3 Click **OK**.
- 4 Click **Yes** or **Clear caches now** depending on the warning message box that appears.

Updating Policy Data Displayed by the Policy Builder

You can update policy data by refreshing data. This is typically done when you have multiple administrators writing data to the Policy Store. Refreshing data causes the Policy Builder to read data from the Policy Store and refresh the display accordingly, which ensures that you are working with the most recent changes on the network.

To refresh policy data

To refresh data, click **View** → **Refresh**. This refreshes information currently shown in the Identities Tree, Resources Tree, and Policy Matrix.

Protecting Policy Data Recorded in Your Policy Store

Because data in your Policy Store is recorded in the directory server as XML entries, you can protect data with data signing. Select Access uses a combination of:

- **Digital signatures:** Select Access allows you to apply digital signatures to policy data so you can readily detect if the Select Access data in the Policy Store had unauthorized changes applied to it. Data is signed with a certificate of your choice.
- **A manifest of valid entries:** Select Access creates a digest of all XML entries that have been cryptographically signed by the certificate you configure. All signed Policy Store entries are listed in a manifest. The Policy Builder checks the manifest when determining whether or not a violation has taken place. Violations occur when changes are made to policy data, but cannot be signed because they are not authorized, and therefore do not get added to the manifest of valid entries.

These two aspects of policy data signing offer you two important security benefits:

- 1 **Data integrity:** Allows you to detect when unauthorized identities have altered data in the directory server. You are notified when entries have been added, deleted or modified.
- 2 **Data authentication:** Allows you to guarantee that the identity making changes with Policy Builder has the right credentials to make the changes.

Setting Up Data Signing

Data signing is not configured or enabled in the Policy Builder. To configure data signing:

- Configure the **Data Signing** setup screen and optionally the **Signer CA Certificate** setup screen (if you want to verify the signer's certificate with a Certificate Authority) in the Administration Server setup wizard.
- Enable data signing via each Policy Validator's corresponding dialog box that appears if you configured data signing in the Administration server. To ensure the right parameters have been configured, see [Chapter 7, Configuring the Policy Validator](#) in the *HP OpenView Select Access 6.2 Installation Guide*.






Policy Builder cannot repair entry violations. Policy Builder can only notify you of where the entry violations exist. You need to assess these violations and determine their impact.

Understanding Signing States

When data signing has been enabled, the signing of entries is automatic. You can determine the status of signing at a glance by monitoring the icon that appears in Policy Builder. There are three states to take note of:

Table 36 Signing status icons

This icon...	Means this...
	Disabled. Signing has not been activated.
	Enabled. Signing has been activated.
	Invalid. Signing has been activated and a violation has been detected.

Losing Your Key

If you permanently lose your certificate, you can still use the Policy Builder. However, all subsequent changes are treated as unsigned entries and Policy Builder is no longer be able to detect entry violations. If you lose your key:

- Delete the digital signature from the directory server.
- Modify the **Data signer CN** field to change the CN. For details, see [To set the Administrator credentials](#) in *HP OpenView Select Access 6.2 Installation Guide*.

Locating and Validating Entry Violations

Any change that does not get recorded in the signed manifest automatically becomes an unsigned change, resulting in an entry violation. Policy Builder cannot tell what the violation is, only that it exists. Examine the violation to determine its cause.

There are three ways to determine when a violation has been detected, as described in [Table 37](#).

Table 37 Violation Detection

Action	Alert
Anything at all.	The enabled icon in Policy Builder changes to the invalid icon.
Click an authorization rule or tree entry.	A message appears directing your attention to the violation.
Click Tools → Policy Data Signature → Verify Signature .	Checks all violations in the directory server.

All directory server entry violation warnings continue displaying until you validate them. Entries can be validated if you:

- **Validate the violation:** Validating entry violations is the process whereby unsigned changes to the directory server become authorized and therefore signed. If you know directory server data has been modified from a trusted source, you can validate any existing violations. For details, see [To validate an entry violation](#) on page 249.
 - Take extreme caution when validating violations. If the wrong unauthorized entry is validated, it can have a severe impact on the security of your organization.
- **Repair and then validate the violation:** You can either discard the violation and recreate the entry, or, if you know what has been modified, you can manually make the corresponding change.

To validate an entry violation

- 1 Click **Tools** → **Policy Data Signature** → **Verify Signature**. If there are any violations, the **LDAP Server Violations** dialog box appears, as shown in [Figure 141](#).

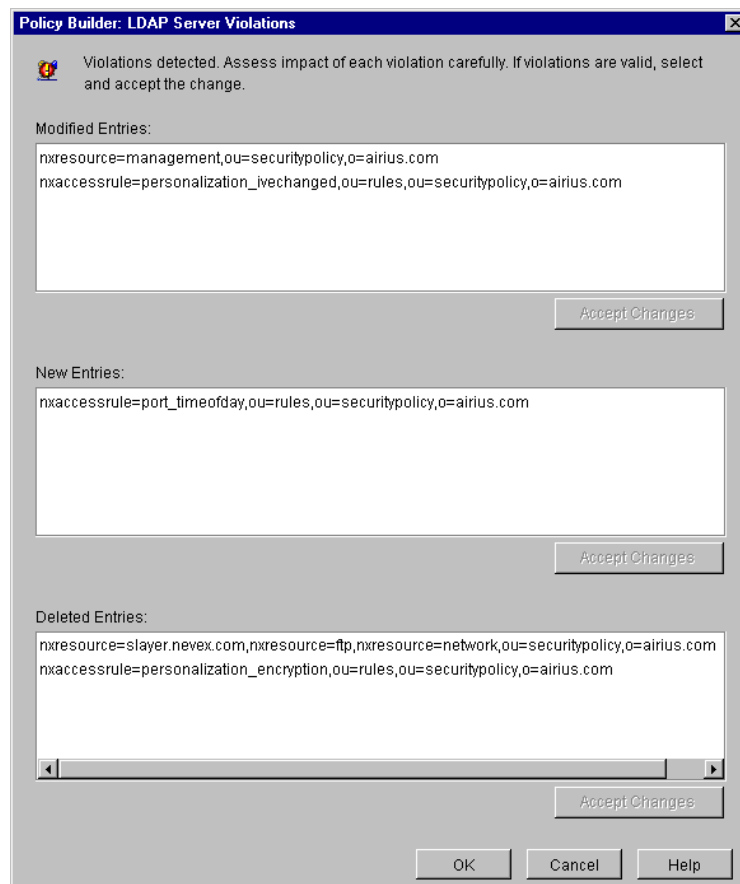


Figure 141 LDAP Server Violations Dialog Box

There are three kinds of violations that can be detected. The detection of violations does not tell you what has caused the violation, but only that one exists. If any violations have been found, the violations are categorized as follows:

- **Modified entries:** An entry has been modified, making the data invalid.
- **New entries:** An entry has been added without the proper authorization.
- **Deleted entries:** An entry is missing and has likely been deleted.

- 2 Select the violation you want to validate and click the corresponding violation by clicking **Accept Change**. Repeat this step as necessary.
- 3 Click **OK** to sign these entries.

To disable warnings

If an unauthorized administrator changed an entry and you click it, an **LDAP Entry violation** dialog box appears, as shown in [Figure 142](#).

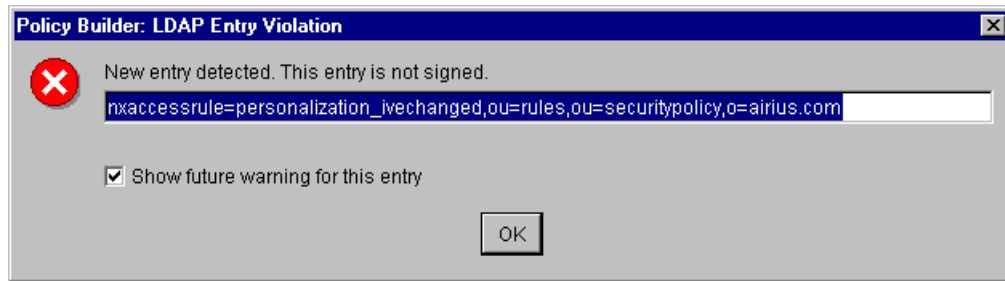


Figure 142Entry Violation Warning Dialog Box

To disable this warning, uncheck the **Show future warning for this entry** box. Warnings are discontinued for this instance of the violation.

15 Modifying Components' Central Configuration Parameters

You can modify the Policy Validators' and Enforcer plugins' configuration from the Policy Builder. This chapter describes how to manage and update the parameters that were originally set after they were installed with the Setup Tool.

Chapter Overview

This chapter includes the following topics:

- [What Parameters You Can Update](#) on page 251
- [Configuring Central Parameters from the Policy Builder](#) on page 251
- [Modifying Group and Override Parameters for the Enforcer Plugin](#) on page 255
- [Modifying Group and Override Parameters for the Policy Validator](#) on page 267
- [Refreshing Configuration Changes](#) on page 271
- [Deleting a Component's Configuration](#) on page 271
- [Displaying Warning Messages](#) on page 271

What Parameters You Can Update

Individual instances of these Policy Validators and Enforcer plugins are identified via the ID currently configured for them. You can modify any of the centrally-located parameters: that is, any parameter stored in the Policy Store can be updated and then uploaded to the component in question without requiring you to stop the component and restart it. Centrally-located parameters are those that are not required by a component at runtime. As a result, they can be downloaded after startup and refreshed at any time.

Configuring Central Parameters from the Policy Builder

The **Component Configuration** window in the Policy Builder configures centrally-located parameters. The **Component Configuration** window is only available to the Select Access super administrator running the Policy Builder Root Administration mode, or by those administrators who have been delegated access to this function. Display this tool by clicking **Tools** → **Component Configuration**. The **HP OpenView Select Access Configuration** window appears, as shown in [Figure 143](#).

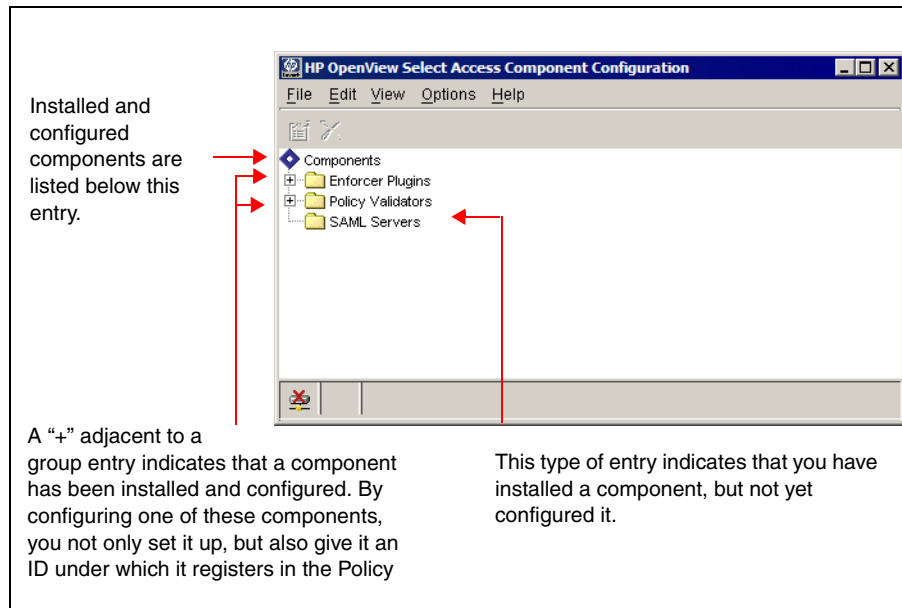


Figure 143 Select Access Configuration Tool

This configuration tool is similar to the Setup Tool: any parameter stored in the Policy Store is made available through this scaled-back version.



Because the configuration tool requires data from the Policy Store, ensure your Administration server is running. The Administration server is required to help manage the configuration information this interface displays and changes.

There are two types of parameters you can configure from the **HP OpenView Select Access Configuration** window:

Table 38 Configurable Parameters

Parameter Type	Details
<i>Group default parameters:</i> For lists of a specific kind of component.	Changing Configuration for a Group on page 252
<i>Override parameters:</i> For individual instances of a component.	Changing Override Parameters on page 253

Changing Configuration for a Group

A group is when you have installed multiple copies of a component on your network. Smaller organizations may only install one Policy Validator and one Enforcer plugin. However, larger companies can install any number of Policy Validator and Enforcer plugins. The number of plugins installed depends on:

- The amount of network traffic they are expecting to service
- How distributed their organization is

Therefore, to maintain a level of consistency in the configuration of these distributed components, you can set up the parameters that must be shared among the group via the Policy Builder.

To change the group defaults shared by multiple components

- 1 Select a group in the configuration tool's window.
- 2 Do one of the following:
 - Right-click the group and choose **Properties** from the shortcut menu as shown below:



OR

- Choose **Edit** → **Properties**. An **Edit Common Settings** dialog box appears. For details, see one of the corresponding sections outlined in [Table 39](#).

Table 39 Editing Components Group and Override Parameters

Components	Details
Enforcer plugin	Modifying Group and Override Parameters for the Enforcer Plugin on page 255
Policy Validator	Modifying Group and Override Parameters for the Policy Validator on page 267

Changing Override Parameters

Depending on the nature of your organization, you can require certain instances of a component to have a specific parameter value other than those configured for the group default. Changing the value for one specific instance of a component only is known as an override. An override value always takes precedence over a group default, even if that group default changes after you configure the override setting.

You can identify an override value by the change of font in the field's name, as shown by [Figure 144](#).



Overrides appear in bold and italics in both the Policy Builder's configuration tool and the Setup Tool.

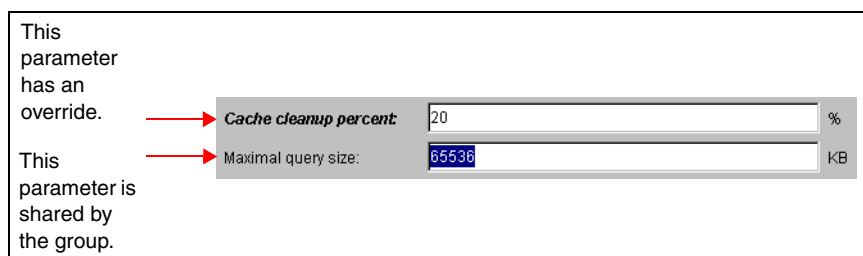
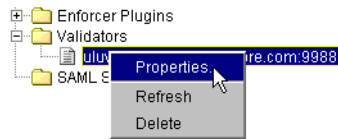


Figure 144Tuning Parameters with an Override Value

To create or change an override value for a single component

- 1 Click a group in the configuration tool's window. A list of available component instances appear.
- 2 Do one of the following:
 - Right-click the corresponding entry and choose **Properties** from the shortcut menu as shown below:



OR

- Choose **Edit** → **Properties**. An **Edit Settings** dialog box appears. For details, see one of the corresponding sections outlined in [Table 39](#).

Table 40 Editing Components Group Parameters

Component	Details
Enforcer plugin	Modifying Group and Override Parameters for the Enforcer Plugin on page 255
Policy Validator	Modifying Group and Override Parameters for the Policy Validator on page 267

Modifying Group and Override Parameters for the Enforcer Plugin

You can modify any of the centrally-located parameters by editing the tabs in the **Edit Enforcer Plugin Settings** dialog box. Centrally-located parameters are those that are stored in your Policy Store and are therefore managed by the Administration server.



If you configure the Policy Builder for Delegated Administration, you notice an Enforcer plugin for this purpose will be added to your list of registered plugins. While the Enforcer plugin for Delegated Administration appears in this window, *do not delete or modify this plugin*.

This Enforcer plugin has been configured specifically for Delegated Administration mode. To ensure this component is never modified or deleted, apply a workflow condition on the Component Configuration administration function to ensure all changes are closely monitored and approved. For details on how to set a workflow condition, see [Applying a Workflow Condition](#) on page 222.

One exception exists: If you are using Registration Authentication via the Administration server to register new users, and the Administration server and web server are on different machines or domains, you need to set certain SSO and/or MD-SSO parameters. For more information, see [Registration Authentication Service](#) on page 107.

Note that every time you reconfigure your Administration server, your Enforcer plugin for Delegated Administration is automatically reconfigured to propagate properties required by the Select Access system. To get this updated configuration information, you should disable and then re-enable Delegated Administration in the Policy Builder. This is particularly important if you have updated the number of Policy Validators deployed on your network. For details, see [To enable delegation](#) on page 206.



To ensure that required Enforcer plugins like the Enforcer plugin for Delegated Administration is never deleted or modified, HP recommends applying a workflow condition on the Component Configuration administrative function.

What You Need to Do to Change Enforcer Plugin Settings

You do not need to modify all tabs in the Edit Enforcer Plugin Settings dialog box; you only need to edit those that require change. For details on how to display this dialog box, see [Configuring Central Parameters from the Policy Builder](#) on page 251.



You can return to Select Access defaults at any time by clicking **Set to Default**.



If you configure the Policy Builder for Delegated Administration, you notice an Enforcer plugin for this purpose has been added to your list of registered plugins. While the Enforcer plugin for Delegated Administration appears in this window, HP suggests that you avoid modifying its configuration. This Enforcer plugin has been configured specifically for Delegated Administration mode. Modifying its configuration parameters can result in unpredictable behaviors.

To configure central Enforcer plugin parameters

- 1 Display an **Edit Enforcer Plugin Settings** dialog box. The **Single DNS Domain SSO** tab appears by default.

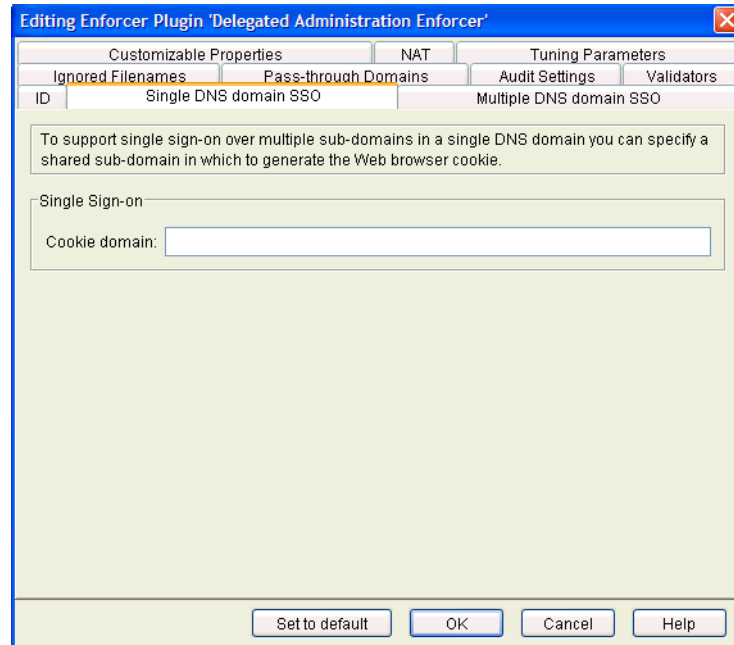


Figure 145Single DNS Domain SSO Tab

- 2 If you need to change the domain name required for SSO, enter the new DNS Domain in the **Cookie Domain** field. The cookie domain must use the following syntax:

.mydomain.com

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

For example, if you enter `mycompany.com`, then whether an identity visits `extranet.mycompany.com`, or `www.mycompany.com`, the same cookie is used and the identity does not need to reauthenticate with each new web server when she tries to access content on an Enforcer-protected subdomain.

For details on how cookies are used with SSO, see [Understanding Nonces and Cookies](#) in the *HP OpenView Select Access 6.2 Concepts Guide*.

- 3 If you need to change or add one or more domain name required for multiple domain SSO, click the **Multiple DNS Domain SSO** tab.

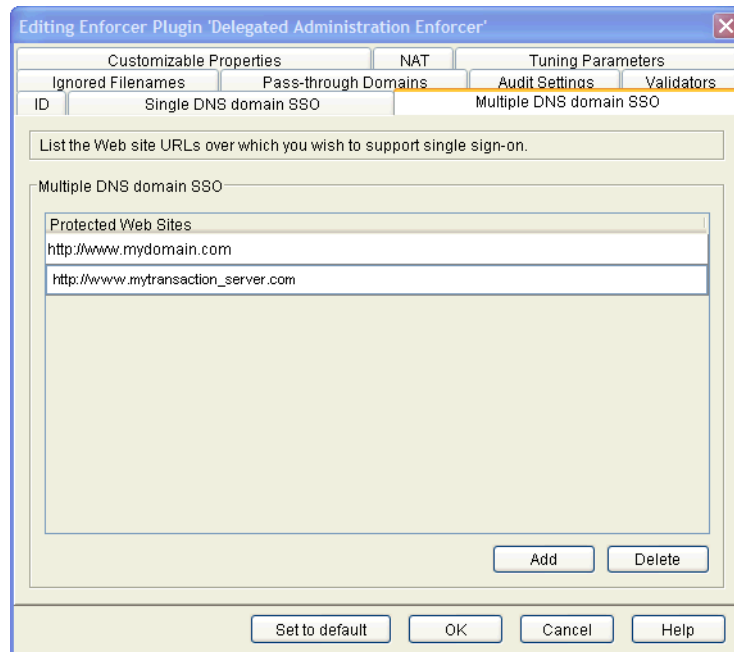


Figure 146 Multiple DNS Domain SSO Tab

4 Do one of the following:

- Click **Add** and enter a domain that needs to be part of your existing **Protected Web Sites** list. Repeat this step as needed to create a complete list.
- Select a row and modify the domain name as needed.

For example, your network might be divided into multiple domains to service different functions of your organization. You may have one for your corporate information, another for your products, and another for your e-commerce transaction server. Therefore, 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, you need to 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-protected web sites must share exactly the same list. otherwise, multidomain SSO fails.
- Multidomain SSO support only works when an identity is accessing content across Enforcer-protected web servers concurrently. If an identity tries accessing an Enforcer-protected site from an intermediate unprotected one, Select Access' multidomain SSO support does not get 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 multidomain SSO, see [Configuring SSO on Multiple Internet Domains](#) in the *HP OpenView Select Access 6.2 Network Integration Guide*.

5 If you need to modify the names of files that do not need protection, click the **Ignored Filenames** tab.

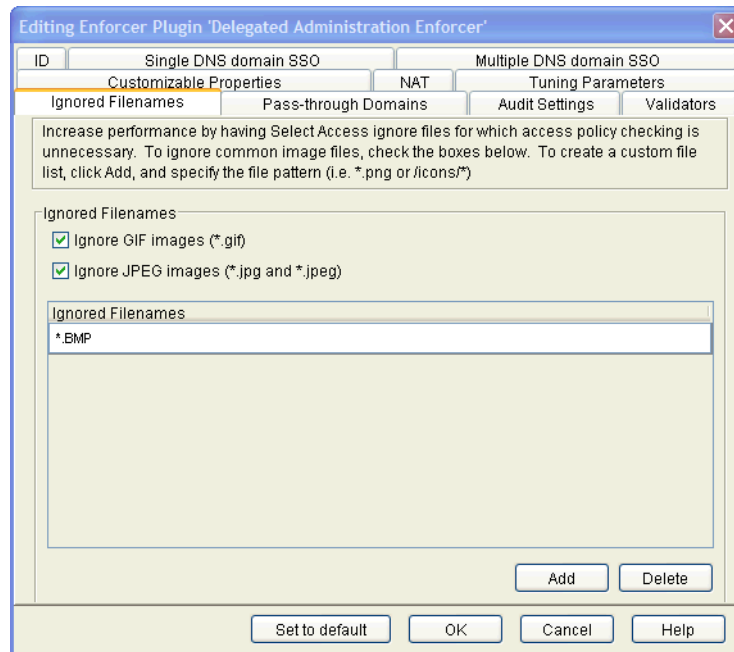


Figure 147 Ignored Filenames Tab

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

- Reduces the number of network-based transactions
 - Frees the Policy Validator to react to queries of a more security-sensitive nature.
- 6 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.

- 7 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.

- 8 To delete a row in the ignored filenames list, select the offending entry and click **Delete**.

- 9 If you need to modify the names of virtual web sites that do not need protection, click the **Pass-through Domains** tab.

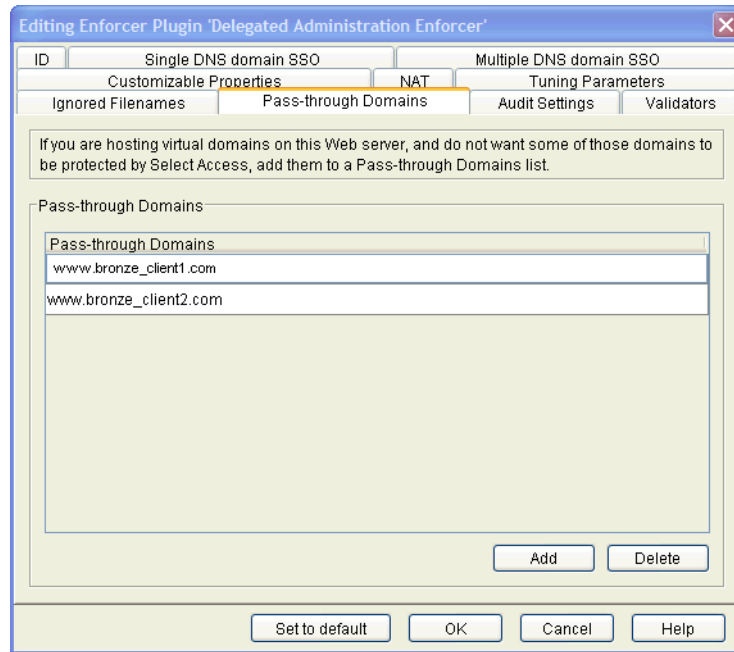


Figure 148Pass-through Domains Tab

- 10 Do one of the following:
- Click **Add** and enter a domain that needs to be part of your existing **Pass-through domains** list. Repeat this step as needed to create a complete list.
 - Select a row and modify the domain name as needed.
- 11 If you need to change where and when messages and or events get logged, click the **Audit Settings** tab.

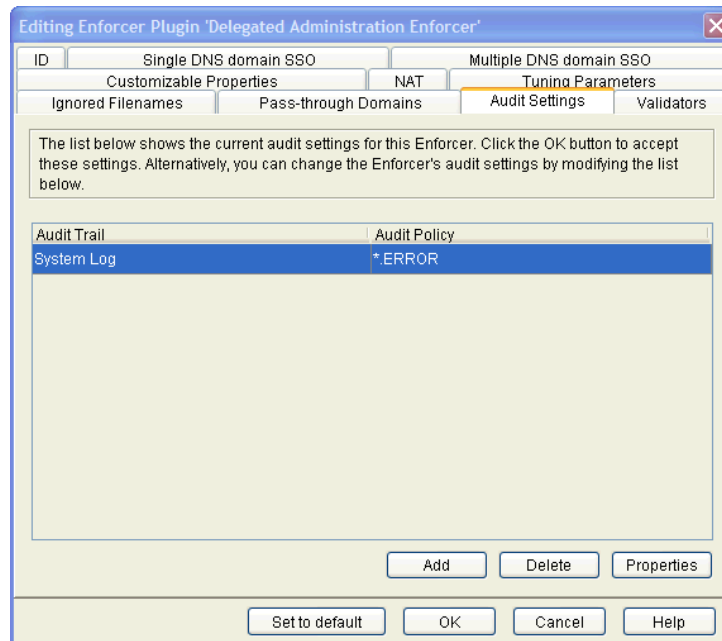


Figure 149Audit Settings Tab

12 Change the settings as required.

- If you log events to Select Audit, this component becomes a client of it. Ensure that you have configured Select Audit before continuing. For details, see the *HP OpenView Select Audit 1.0 Installation Guide*.
- You can create reports from the runtime messages that have been logged to Select Audit, preferably from a nonrefutable administrative log that has been digitally signed and output in XML. For details, see the *HP OpenView Select Audit 1.0 Administration Guide*.
- Do not reconfigure audit setting for the Enforcer plugin for Delegated Administration. It does not output events and messages according to the audit settings you configure.

- To create or modify audit settings rows, click **Add** or **Properties** respectively. The **New Event Log** dialog box appears displaying two tabs, **Audit Trail** and **Audit Policy**. These tabs correspond to the columns of the **Default Audit Settings** setup screen.

When you configure the tabs of the **New Event Log** dialog box, then click **OK**, a new row is added below the one you have selected, and the cells get populated automatically.

- To remove an empty or populated row, select the entry in question and click **Delete**.
- Ensure you have write permissions for the file your Enforcer plugin is configured to log to or logging does not occur. Starting your web server as root on UNIX systems or administrator on Windows systems does not guarantee the web server process has write permissions across the system.

13 If you need to change how Enforcer plugins use Policy Validators to authenticate identities and authorize access, click the **Validators** tab.

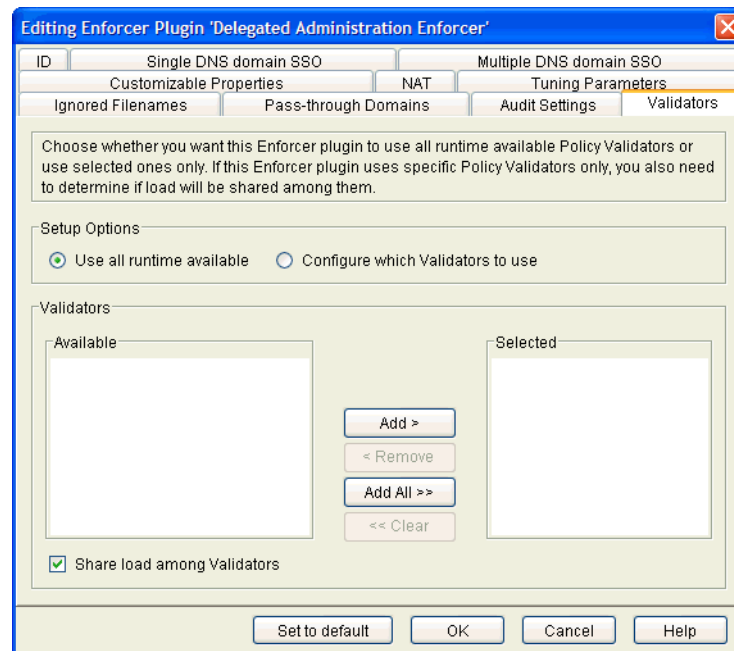


Figure 150Validators Tab

14 Modify fields in the **Setup Options** and **Validators** groups as needed.

- ▶ 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/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), are be able to failover and/or round robin to the new Policy Validators if the test Policy Validator fails. If you must stagger your deployment, re-run the Setup Tool for your existing Enforcer plugin to ensure all new Policy Validators are written to its `enforcer.xml` file.

- ▶ 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.
- **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.
- **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 **Add** or **Add all**. This creates a Validator list to be used 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 **Remove** or **Clear all**.

- **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 is contacted first. If this box is not checked, queries are sent to the first Policy Validator in the selected list unless a connection cannot be established. Queries are then sent to the next Policy Validator in the list, and gradually moves down the list until one can be contacted. 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.

15 If you need to modify the addresses of Policy Validators behind a NAT device, click the **NAT** tab. The Enforcer plugin uses this address to connect to the Policy Validator in question.

- ▶ 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 the **Validators** tab.

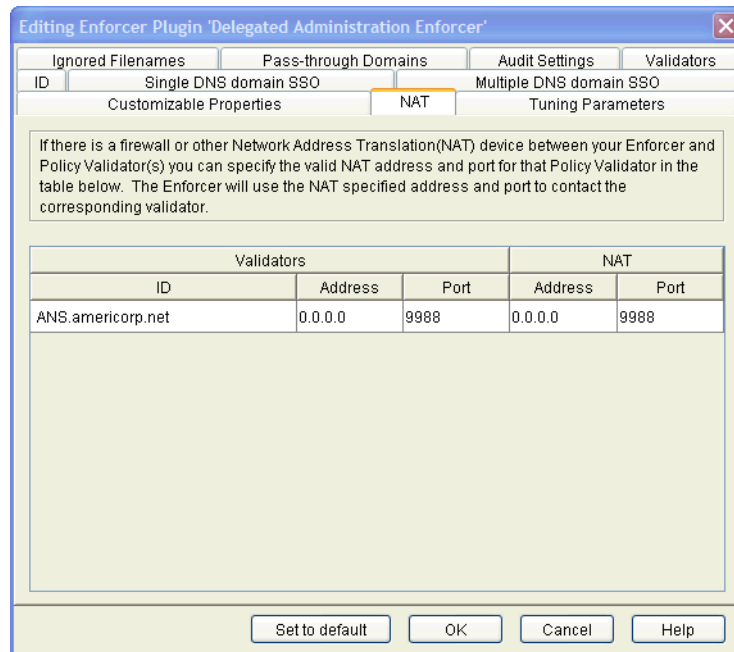


Figure 151 NAT Tab

- 16 Modify the mapping of a Policy Validator as needed.
 - 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.
 - If the NAT port number is different, click the **Port** cell and type the alternate Policy Validator port number.
- 17 If you need to change how Enforcer plugins perform, click the **Tuning Parameters** tab.
 - Overrides appear in bold and italics in both the Policy Builder's configuration tool and the Setup Tool.

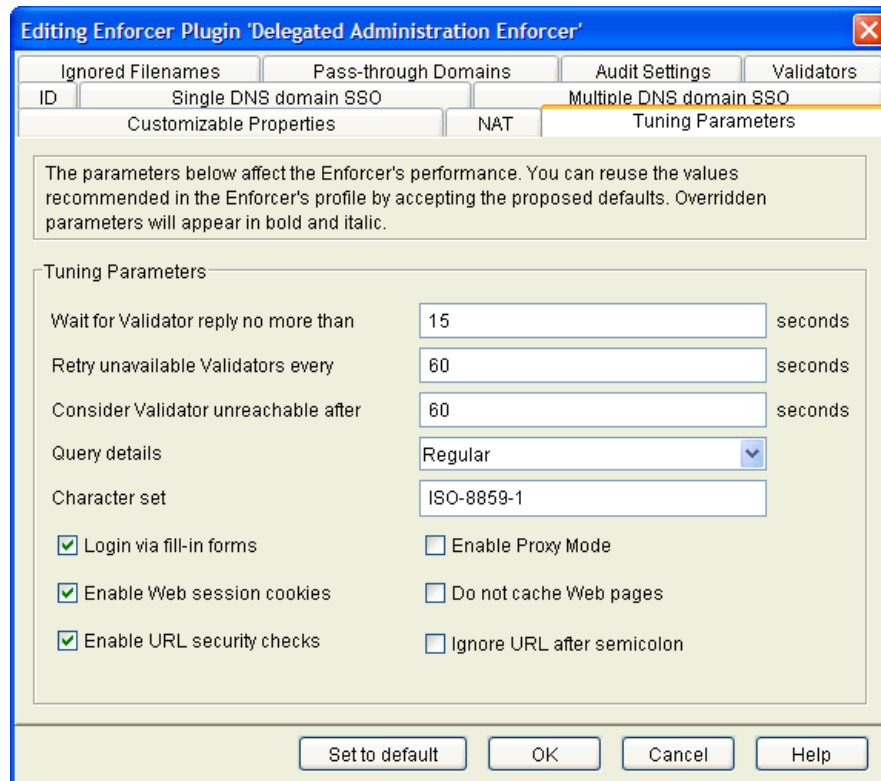


Figure 152 Tuning Parameters Tab

18 Modify fields in the **Tuning Parameters** group as needed.

- **Wait for Validator reply no more than:** Optional. 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 never gives up on the connection.
- **Retry unavailable Validators every:** Optional. Sets the time interval for an Enforcer plugin to retry opening a connection to a broken Policy Validator. If an Enforcer plugin fails, the connection to the Policy Validator is marked 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 Policy Validator is not successful at reopening the connection within the time specified, the Enforcer plugin stops all future connection attempts.


- **Query details:** Optional. Determines the number of fields to be added to the XML query. The more query fields the Enforcer plugin is configured to add (even when they are not used in the decision process) results in a performance trade-off with respect to the Policy Validator. This parameter also allows for a refined decision process due to the levels.

Table 41 Query Level Overview

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

► You can create your own custom plugin to take advantage of the `site_data` query detail. For details, see [Chapter 3, Transparently Supported Web Server Integrations](#), in the *HP OpenView Select Access 6.2 Network Integration Guide*.

- **Character set:** Optional. Enter the name of the character set to be used when data is POSTed from a web browser to a web server, so data that is exchanged can be converted from the set you specify to UTF-8 format. 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 Enforcer plugin is installed.
 - A list of possible character sets you can use is available in the online help for the Setup Tool.
 - **Login via fill-in forms:** Optional. Check this box to enable form-based login.
- If you intend to use SecurID or RADIUS authentication, enable this option.


- **Enable Web session cookies:** Optional. Check this box to use web session cookies.
 HP recommends you check this box: it is required to support form-based login.

- **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 the *HP OpenView Select Access 6.2 Installation Guide*.

- **Do not cache Web pages:** Optional. Check this box to prevent web pages from being cached.
 If you are using multidomain single sign-on with Apache, iPlanet or Sun ONE web servers, check this box.

- 19 If you need to change values for customized Enforcer properties, click the **Customizable Properties** tab.

The **Customizing Properties** setup screen, shown in [Figure 153](#), allows you to define Enforcer-specific properties, so that the Enforcer has more flexibility. [Table 42](#) lists the pre-defined Enforcer-specific properties available.

Table 42 Pre-defined Properties

Property	Description
Login Form URL Tag	You can change the value of the URL tag to display the message of your choice.

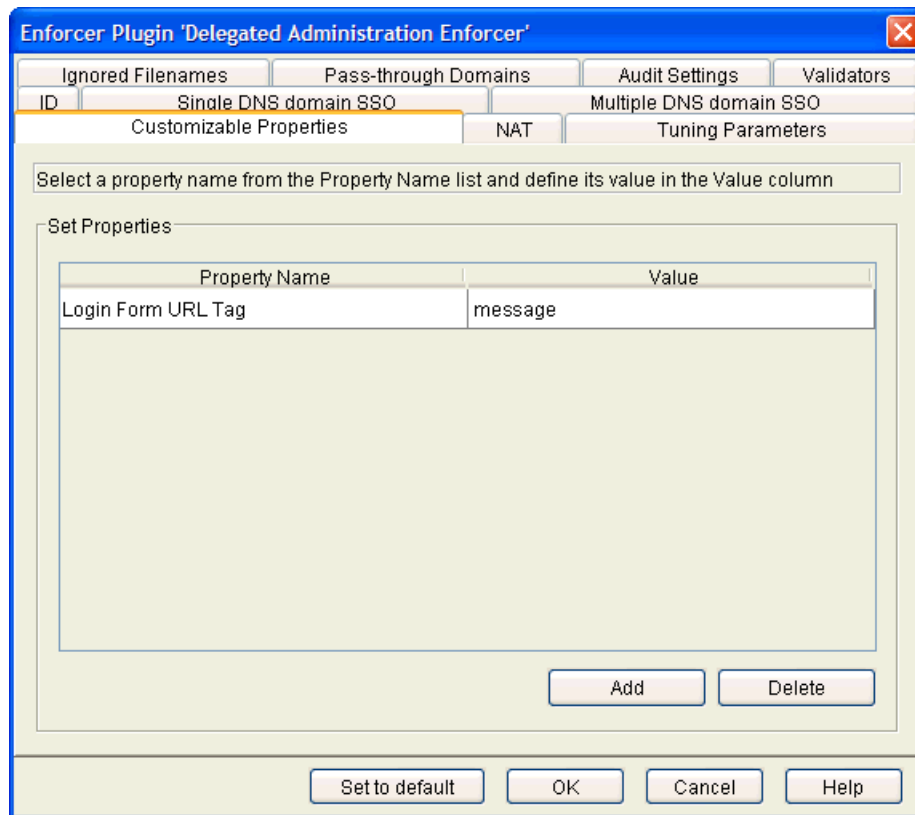


Figure 153 Customizable Properties Setup Screen

20 Do one of the following.

- To customize provided Enforcer plugin properties:
 - a Select a property from the **Property Name** drop-down list.
 - b Enter a value in the **Value** field and click **OK**. The customized property is defined.

➤ Properties must be have unique names.
- To add your own Enforcer plugin properties:
 - Any properties you add will not appear in the **Properties Name** drop-down list.
 - a Click **Add**.
 - b Enter a value in the **Value** field and click **OK**. The customized property is added to the Policy Store.
 - Properties must be have unique names.

Modifying Group and Override Parameters for the Policy Validator

You can modify any of the centrally-located parameters by editing the tabs that exist in the **Edit Validator Settings** dialog box. Centrally-located parameters are those that are stored in your Policy Store and are therefore managed by the Administration server.

What You Need to Do to Change Policy Validator Settings

You do not need to modify all tabs in this dialog box; you only need to edit those that require change. For details on how to display this dialog box, see [Configuring Central Parameters from the Policy Builder](#) on page 251.

- You can return to Select Access defaults at any time by clicking **Set to Default**.

To configure central Policy Validator parameters

- 1 Display an **Edit Validator Settings** dialog box. The **Address, Port, and ID** tab appears by default.

- The address and port fields are only available when you are editing parameters for a specific Policy Validator and not the group of Policy Validators.

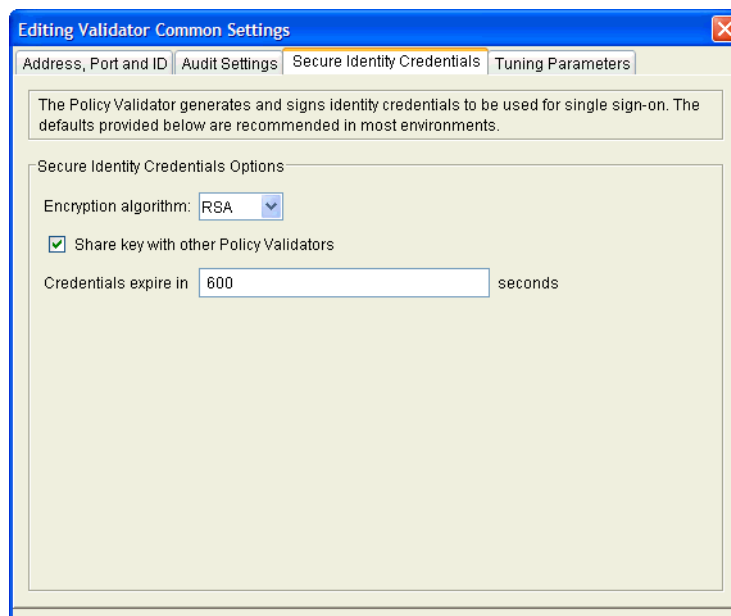


Figure 154Address, Port and ID Tab

- Modify any of the tab's fields as needed. **Host:** Required. Choose which IP address is used 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 then enter the details in the corresponding text box below this option.

- **Port:** Optional. Enter the port Policy Validator is running on. If you leave it blank, the default port of 9988 is used.
 - **ID:** Required. This allows you to create a Policy Validator ID. The ID is used 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 If you need to change when and how messages and events are logged, click the **Audit Settings** tab.

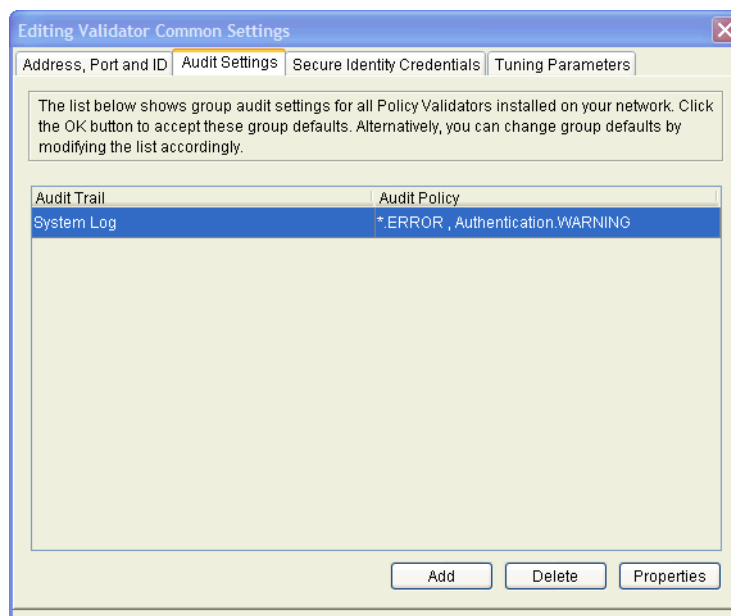


Figure 155Audit Settings Tab

- 3 Review the audit settings that appear. By default, Select Access components use the audit settings you configured with the Administration server. These settings are used as the global common audit settings for all components. To create custom audit settings for this specific Policy Validator only, change the settings as required.

- If you log events to Select Audit, this component becomes a client of it. Ensure that you have configured Select Audit before continuing. For details, see the *HP OpenView Select Audit 1.0 Administration Guide*.
- You can create reports from the runtime messages that have been logged, preferably from a nonrefutable administrative log that has been digitally signed and output in XML. For details, see the *HP OpenView Select Audit 1.0 Administration Guide*.

- To create or modify audit settings rows, click **Add** or **Properties** respectively. The **New Event Log** dialog box appears displaying two tabs, **Audit Trail** and **Audit Policy**. These tabs correspond to the columns of the **Default Audit Settings** setup screen.

When you configure the tabs of the **New Event Log** dialog box, then click **OK**, a new row is added below the one you have selected, and the cells are populated automatically.

- To remove an empty or populated row, select the entry in question and click **Delete**.
- 4 If you need to change how digital signatures are used to create cookies and nonces, click the **Secure Identity Credentials** tab.

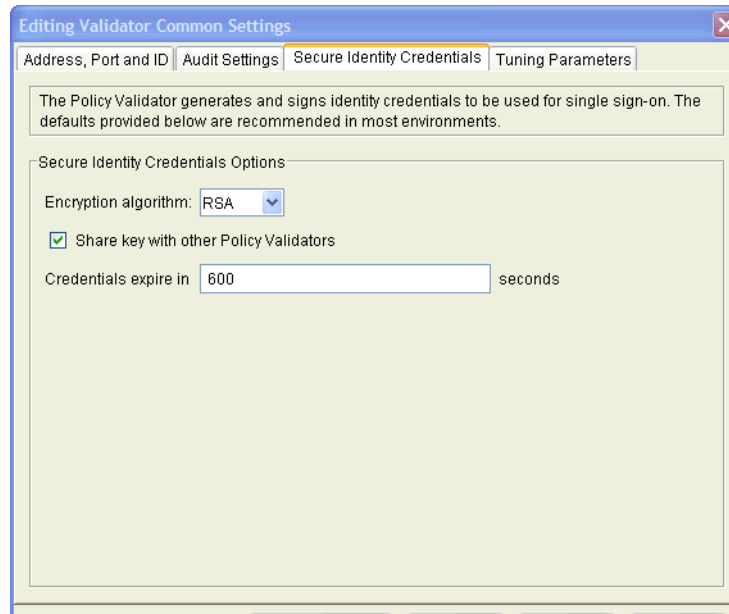


Figure 156Secure Identity Credentials Tab

- 5 Modify fields in the **Secure Identity Credential Options** group as needed.
- **Encryption algorithm:** Required. Choose the algorithm you want to use to encrypt data streams to and from the Policy Validator. By default, RSA is a 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 keys are published. If you check this box, the RSA or Digest key needed to validate Select Access cookies is published to the Policy Store. If you leave this box unchecked, no key is published.
 - You need to publish your keys to do either load-balancing or round-robinning. If you do not share your keys, identities have to reauthenticate themselves. This is because the keys required to validate cookies are not available to a Policy Validator so cookies cannot be checked for their authenticity.
 - **Credentials expire in:** Required. Determines how long, in seconds, an identity 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.
- 6 If you need to change the performance of the Policy Validator, click the **Tuning Parameters** tab.
- Overrides appear in bold and italics in both the Policy Builder's configuration tool and the Setup Tool.

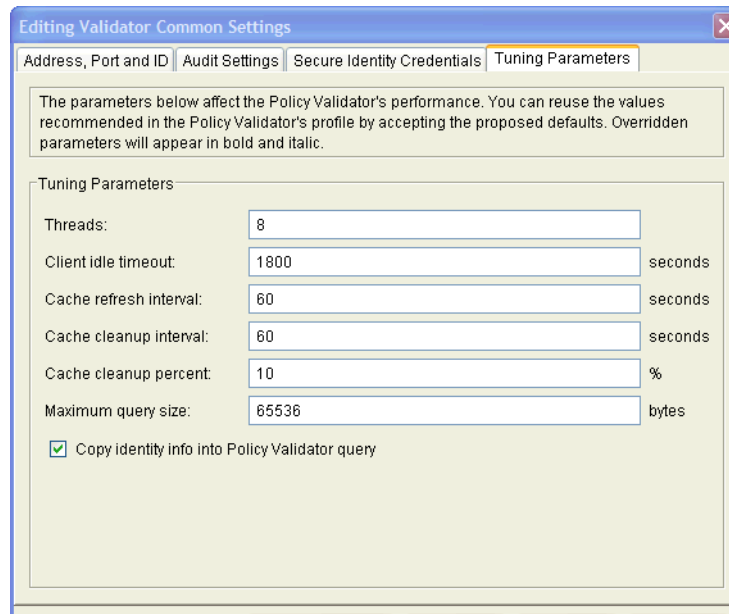


Figure 157 Tuning Parameters Tab

- If you need to change Policy Validator preferences, modify fields in the **Tuning Parameters** group as needed. **Threads**: Optional. Specifies the number of Policy Validator threads that can execute independently.
- **Client idle timeout**: Optional. The length of time, in seconds, before Policy Validator closes an idle client connection.
- **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 had saved to that point. The default is 60 seconds.
 - HP recommends that you also use Policy Builder to clear the cache when you alter policy data or add new identity profiles. This ensures that the Policy Validator updates the identity and policy data. For details, see [Updating Policy Data Cached by the Policy Validator](#) on page 246.
- **Cache cleanup interval**: Optional. The interval, in seconds, that Policy Validator uses to clear unused user profiles from its cache. The default is 60 seconds.
- **Cache cleanup percent**: Optional. The percent of the cache that is checked for unused profiles.
- **Maximum query size**: Optional. The size limit of XML queries allowed.
- **Copy user info into Validator query**: Optional. Makes the attribute/value pairs of an identity entry accessible to other Policy Validators when evaluating any LDAP attribute decision point. If you uncheck this box, only `authenticated_dn` and `uid` attributes are added 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.

- 7 Click **OK** to commit the changes to the Policy Store.

Refreshing Configuration Changes

When you refresh a component's configuration, you are uploading the changes that you committed to the Policy Store to the component itself. By refreshing the configuration, you are allowing the component to use these changes, without requiring you to restart it.

There are three ways to refresh a component's configuration:

- Right-click a group or component entry and choose **Refresh**.
- Click a group or component entry and choose **Refresh** from the **Edit** menu.
- Set an option to update a component's configuration automatically. You can only set automatic refresh for Policy Validator and the Enforcer plugin. To automatically refresh the configuration for these components, choose the corresponding automatic refresh command from the **Option** menu.

Deleting a Component's Configuration

When you delete a component's configuration, you are deleting the centrally-located parameters that have already been committed to the Policy Store only. If you delete the configuration, only the parameters are removed, not the entry for that component.

There are two ways to delete a component's configuration:

- Right-click a group or component entry and choose **Delete**.
- Click a group or component entry and click **Edit** → **Delete**.


Displaying Warning Messages

Clicking the boxes that enable warnings means you do not need to be aware of every condition that requires an update. Instead, a message box appears when data that affects a component changes, prompting you with the corresponding action.

To enable warning messages

- 1 If you want to set warning behaviors while you are working in the Policy Builder, click **File** → **Configure Client Settings**. The **Configure Client Settings** dialog box appears.
- 2 Click the **Enable Warnings** tab.
- 3 Check the events for which you want the Policy Builder to display a warning:
 - **Clearing the Policy Validator's cache.** For details on the Policy Validator cache, see [Updating Policy Data Cached by the Policy Validator](#) on page 246.
 - **Refreshing the Policy Validator's configuration.** For details on configuring the Policy Validator from the Policy Builder, see [Modifying Group and Override Parameters for the Policy Validator](#) on page 267.
 - **Refreshing the Enforcer plugin's configuration.** For details on configuring the Enforcer plugin from the Policy Builder, see [Modifying Group and Override Parameters for the Enforcer Plugin](#) on page 255.

- **Changing authentication properties on administrative resources.** For details on setting authentication properties, see [To enable Select Auth on an Administration server resource](#) on page 199.
- **Changing delegated policy for unknown identities.**

 Unknown identities can never delegated administrative entitlements.

- 4 Click **OK** to save these preferences.

A Invalid Characters

The characters listed in this appendix are characters that are invalid on specific directory servers.

The two directory servers that are the most problematic with certain characters are:

- Novell NDS eDirectory 8.5.1
- Oracle Internet Directory 3.0.1.1

If you use any of the characters that are listed as invalid for your directory server, expect unpredictable behavior. To prevent your directory server from behaving unexpectedly, become familiar with the invalid characters that apply to your directory server and avoid using them in the Policy Builder.

Table 43 Listing of Invalid Characters

Character	Invalid on	
	Novell NDS eDirectory 8.5.1 and 8.6.2	Oracle Internet Directory 3.0.1.1
=	•	•
>	•	
<	•	
#	•	
//	•	
+		•
,		•
\\		•

Table 43 Listing of Invalid Characters

Character	Invalid on	
	Novell NDS eDirectory 8.5.1 and 8.6.2	Oracle Internet Directory 3.0.1.1
;		•
““		•
\	• a	•

- a. You can use this character freely on eDirectory 8.6.2. However, if you intend to use it on version 8.5.1, you must escape this character using the following character sequence: \5c.

B Using Web Administration

The Web Administration application is a customizable, form-based application that allows you to access the Administration server through your corporate portal. Using Web Administration, administrators with the appropriate entitlement can remotely manage your Select Access identities.



You can customize the Web Administration JSP pages using the Web Administration API, shipped with the Select Access SDK, to conform to your corporate look and feel. For more information, see the *HP OpenView Select Access 6.2 Developer's Tutorial Guide* included with the SDK.

Before You Begin

Before using Web Administration to manage identities, you should make sure that you understand how information is stored in the directory server. Select Access supports a number of organizational units (groups, dynamic groups, and folders) that you can use to improve the efficiency and ease of use of both the Policy Builder and the Web Administration application. A clearly architected tree structure goes a long way in minimizing confusion that a large-scale access policy setting operation can encounter.

To learn more about how Select Access stores user information and how you can use organizational units to help with user management, see [Organizing Identities and Resources](#) on page 65.

About Web Administration Security

Because it connects to the Administration server, Web Administration is subject to the same stringent security as the Policy Builder. This means that delegated administrators are subject to the same authentication requirements when logging in and, once authenticated, they can view only those user entries and attributes to which they have been delegated access. In addition, they are still subject to the same workflow configuration as they would be in the Policy Builder.

In order for delegated administrators to use the Web Administration application, the Select Access super administrator must ensure that they have been delegated the necessary entitlements. For more information, see [Setting Up Access to the Web Administration Application](#) on page 276.

Setting Up Access to the Web Administration Application

Before delegated administrators can use the Web Administration application, the Select Access super administrator must perform the steps outlined in [Table 44](#).

Table 44 Delegating Administration Overview

This step...	For details, see...
1 Enable Web Administration.	Enabling Administration Server Resources on page 199
2 Delegate resources in the Administration Matrix to a selected user as necessary to allow the required access. You will need to delegate access to: <ul style="list-style-type: none">• Selected user entries within the Identity Management branch.• Selected attributes within the Attributes branch. You can assign either full or read-only access for each attribute. Delegated administrators may view, but not change, those attributes to which they have been granted read-only access.	Assigning Administration Entitlements on page 207
3 Configure workflow for your delegated administrators as necessary.	Applying a Workflow Condition on page 222

Getting Started with Web Administration

The Web Administration application is a JSP-based application that allows you to remotely manage identities through your browser. You can create, delete and manage:

- Identity profiles
- Group memberships
- Directory server folders

In addition, it allows you to search or browse through your directory server entries to locate specific entries or sets of entries.

Running Web Administration

Like the Policy Builder, Web Administration is accessed through a configurable URL. The URL you use to start Web Administration is defined during the Administration server's configuration. For details, see [Chapter 5, Configuring the Administration Server](#) in the *HP OpenView Select Access 6.2 Installation Guide*.

To run the Web Administration application

- 1 Enter the URL for the Policy Builder in your browser's **Address** box. By default, the URL to access the Policy Builder in full administration mode is:

`https://<host>.<domain>:9991`

where *<host>* is the name of the computer hosting the Administration server and *<domain>* is the domain name of your organization.

► You can also substitute your host's IP address for *<host>.<domain>*.

If you configured the Administration server to allow Select Access to handle SSL certificates and connections, a security alert similar to the one shown below appears.

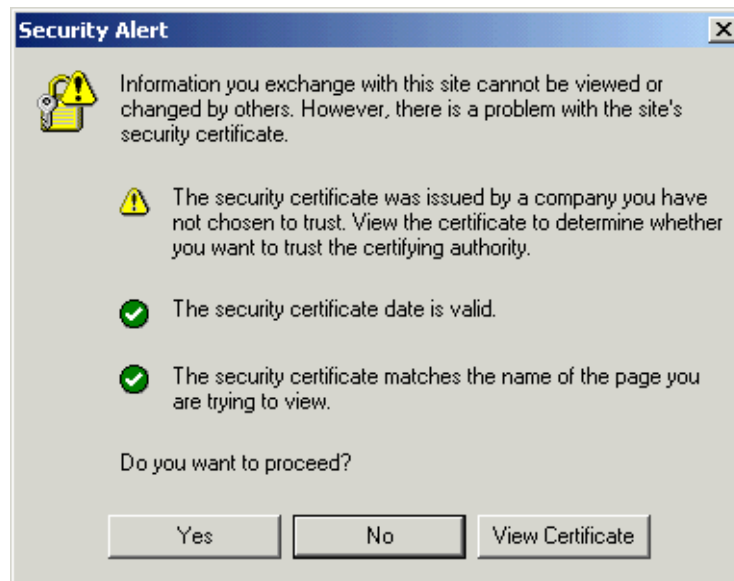


Figure 158 Certificate Security Alert Message Box: Internet Explorer

- 2 Add the certificate to your Root Store. To add the certificate:
 - a Click **View Certificate**. The **Certificate** dialog box appears.
 - b Click the **Certification** tab.
 - c Select the CA root and click **View Certificate**. A second **Certificate** dialog box appears.
 - d On the **General** tab, click **Install Certificate**, and follow the Certificate Manager Import wizard's prompts to add this certificate to your Root Store.
 - e The **Import Successful** message box appears. Click **OK** to close this message box.
 - f Click **OK**.
- 3 Click **Yes** on the **Security Alert** message box. The login page that is used to access the Policy Builder appears.



Please Login for Access to Protected Area

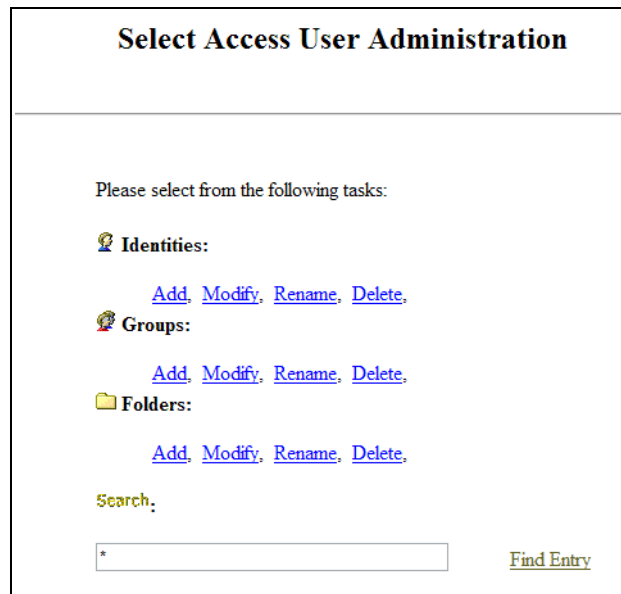
Password Server: Password Server

Login Name

Password


Figure 159Web Administration Login Page

- 4 Enter the login information required to access the Web Administration application (that is, the login information required to log into the specified authentication services), and click **Login now**.
 - Like Delegated Administration mode of the Policy Builder, Web Administration authenticates delegated administrators via the authentication method that has been defined for them (for example, certificate or password).
- 5 Once authenticated, the Web Administration home page is displayed. By default, the home page displayed appears as in [Figure 160](#).
 - If your organization has customized the Web Administration JSP pages, the layout and functionality may differ from the default version.




Select Access User Administration


Please select from the following tasks:

 **Identities:**

[Add](#), [Modify](#), [Rename](#), [Delete](#).

 **Groups:**

[Add](#), [Modify](#), [Rename](#), [Delete](#).

 **Folders:**

[Add](#), [Modify](#), [Rename](#), [Delete](#).

Search:

[Find Entry](#)

Figure 160Web Administration Application Home Page

Locating Identities

In order to add, edit, or delete an identity profile, group, or folder, you need to locate either the parent folder into which new entries will be added, or the specific user, group, or folder you want to edit or remove. You can locate entries in one of three ways:

- By searching on a text string. You can search for either an exact string which returns a single matching profile, or for a partial string with a wildcard character to return a list of matching entries.
- By browsing through the available entries. This allows you to navigate through the visible portion of the Identities Tree to select your profile.
- By displaying all the entries. This simply lists the entries, along with their full path within the Identities Tree.

The Web Administration application automatically returns the profile type that applies to the chosen task. In each case, the link indicates the profile type(s) that is returned.

For example, if you are adding a new identity, you must select the parent folder, and only folders are returned. Likewise, when deleting a group, only groups are returned.

To search for an identity

- 1 In the **Search** field, enter the string you want to search for. There are two types of entries you can make in this field:
 - *To find an exact profile:* Enter the name of the entry you want to find.
 - *To find multiple profiles:* Enter a search pattern by using a wildcard (*). For example, to find all names beginning with s, enter s*. To find all entries, enter *.
- 2 Click **Find Identity** to begin your search. The list of matching results is returned.
- 3 Click the profile to view the properties.

To browse for an identity

- 1 Click **Browse Identities**. The top-most visible folder is displayed.
- 2 Expand and collapse the folders and groups in the tree in order to locate the desired profile.
- 3 Click the profile to view its properties.

To display all the visible identities

- 1 Click **Show All Identities**. A complete list of entries is displayed.



The hostname of the identity location is not displayed when you attempt to locate an entry using the **Show All Entries** option, which may lead to confusing results. This option returns a flat list of entries with the names of the user locations.

A problem could arise if multiple user locations exist with similar hierarchy and entry names. Entries from two different user locations could appear identical. In this case, you should use the **Browse** option to locate your entries.

- 2 Click the desired profile from the list to view its properties.

Managing Identities, Groups, and Folder

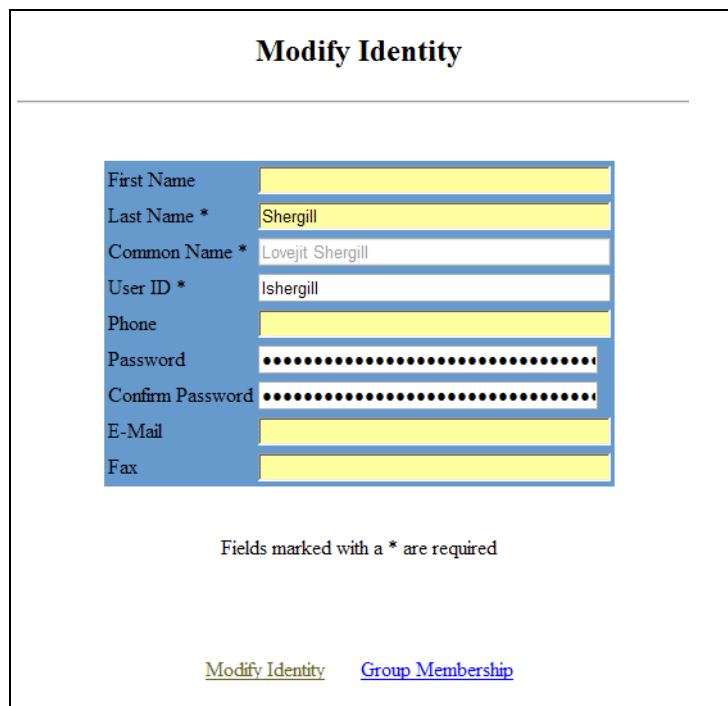
The Web Administration application allows you to add, modify, rename, or delete user entries, groups or folders, as well as modify group memberships. Changes are written to the directory server immediately upon the completion of a task.

Managing Identities

You can add new identities to any existing visible folder, or modify or rename an identity profile you have already added.

To add, modify or rename a new identity profile

- 1 Under **Identities**, click **Add**, **Modify**, or **Rename**.
 - If you are adding a new identity, you will be asked to locate the folder you want to add the new identity to.
 - If you are modifying or renaming an identity, you will be asked to locate the specific user.
- 2 Locate and select the folder or user. An identity properties page appears.



The screenshot shows a web form titled "Modify Identity". It contains several input fields with labels on the left and text boxes on the right. The fields are: First Name (empty), Last Name * (containing "Shergill"), Common Name * (containing "Lovejit Shergill"), User ID * (containing "lshergill"), Phone (empty), Password (masked with dots), Confirm Password (masked with dots), E-Mail (empty), and Fax (empty). Below the fields, a note states "Fields marked with a * are required". At the bottom, there are two links: "Modify Identity" and "Group Membership".

First Name	
Last Name *	Shergill
Common Name *	Lovejit Shergill
User ID *	lshergill
Phone	
Password
Confirm Password
E-Mail	
Fax	

Fields marked with a * are required

[Modify Identity](#) [Group Membership](#)

Figure 161Modify Identity Page

- 3 Enter or review the information outlined in [Table 45](#) as necessary.
 - If you are modifying an existing profile, you cannot change the **Common Name** property.
 - If you are renaming an existing profile, you can *only* edit the **Common Name** property.

Table 45 Profile Properties

Field	Description
First Name	Optional for all directory servers. Enter the identity's first name.
Last Name	Required for all directory servers . Enter the identity's last name.
Common Name	<p>Required for all directory servers. Enter the identity's full name. (For example, John Smith or John T. Smith.) The string you enter is used to display the profile on the Identities Tree.</p> <p>Note: For iPlanet and Sun ONE directory servers, do not create a profile name with two or more backslashes in a row. Otherwise, your directory server experiences difficulties when looking up these entries. This can result in an "object not found" exception when you try to expand the folder containing the item. However, you can create names with a single backslash, as well as with multiple backslashes that are separated by other characters.</p>
Identity ID	Enter the identity's ID.
Account Name	Required for Active Directory . The logon name used to support non-Windows 2000 clients and servers (Windows 95, Windows, and LAN Manager).
Principal Name	Optional for Active Directory . A string property that specifies the principal name of the identity in the form of an Internet-style login name.
Fax	Optional for all directory servers. Enter the identity's fax number.
E-Mail	Optional for all directory servers. Enter the identity's email address.
Phone	Optional for all directory servers. Enter the identity's telephone number.
Password, Confirm Password	Optional for Active Directory if connecting over SSL. For details, see the note at the beginning of To create or modify an identity profile on page 40. Enter the identity's password.

4 Do one of the following:

- If you are adding a new identity, click **Add an identity** to complete the task.
- If you are modifying an identity, click either **Modify Identity** to complete the task, or **Group membership** to add the identity to an existing group. For more information on adding the current user to a group, see [To assign the current identity to a group](#) on page 282.
- If you are renaming an identity, click **Rename User** to complete the task.

The home page appears, informing you whether or not the task was successfully completed.

To assign the current identity to a group

- 1 In the Modify Identity page, click **Group Membership**. The **Group Membership** page appears.

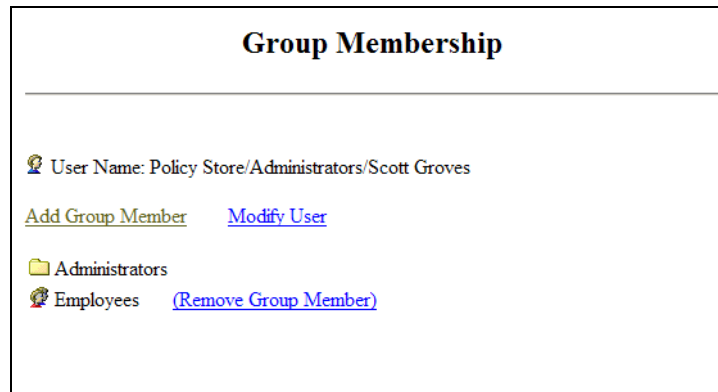


Figure 162Group Membership Page

This page displays a list of the groups the current user is a member of.

- 2 Click **Add Group Member** to assign the current user to another group.
- 3 Locate the group to add the member to, as described in [Locating Identities](#) on page 278.
- 4 Click the group to add the current user as member.
- 5 Repeat Steps 2-4 to assign the identity to additional groups.
- 6 To remove the identity as a member of a group, select the group you want to remove it from and click **Remove Group Member**.

To delete an identity profile

- 1 Under **Identities**, click **Delete**.
- 2 Locate and select the identity you want to delete. A confirmation page appears.
- 3 Click **Delete User** to remove the profile. The home page appears, informing you whether or not the task was successfully completed.

Managing Groups

Groups must be created before identities can be assigned to them as members. Groups can contain identities or even other groups or dynamic groups.

For example, if you create a group called “User Experience” you can assign Technical Writing, Training, and Technical Support groups to it as well as individual user entries like the Director of R&D and the VP of Customer Care.

To add, modify, or rename a group

- 1 Under **Groups**, click **Add**, **Modify**, or **Rename**.
 - If you are adding a new group, you will be asked to locate the folder you want to add the new group to.
 - If you are modifying or renaming a group, you will be asked to locate the specific group.

- 2 Locate and select the folder or group. A group properties page appears.

Modify Group

Group Name *

Description

Fields marked with a * are required

[Modify Group](#) [Group Membership](#)

Figure 163 New Group Dialog Box

- 3 Enter values for the group properties.
 - ▶ If you are modifying an existing group, you cannot change the **Group Name** property.
If you are renaming an existing group, you can *only* edit the **Group Name** property.
 - **Group Name:** Enter the group's name. This is the group's entry name (or RDN) and it appears on the Identities Tree.
 - **Description:** Optionally, enter a description of the group.
- 4 If you choose, you can modify the groups memberships. For more information, see. [To add a new member to the current group](#) on page 283.
- 5 Complete the task by doing one of the following:
 - If you are adding a new group, click **Add a Group**.
 - If you are modifying a group, click **Modify Group**.
 - If you are renaming a group, click **Rename Group**.

The home page appears, informing you whether or not the task was successfully completed.

[To add a new member to the current group](#)

- 1 In the Group properties page, click **Group Membership**. The **Group Membership** page appears.



Figure 164 Group Membership Page

This page displays the present members of the current group.

- 2 Click **Add Group Member** to add a new member to the current group.
- 3 Locate the identity or group you want to add as a member to the current group, as described in [Locating Identities](#) on page 278.
- 4 Click the profile to add it as member of the current the group.
- 5 To remove a member from the group, select it from the list of members and click **Remove Group Member**.

To delete a group

- 1 Under **Groups**, click **Delete**.
- 2 Locate and select the group you want to delete. A confirmation page appears.
- 3 Click **Delete Group** to remove the entry. The home page appears, informing you whether or not the task was successfully completed.

Creating and Modifying a Folder

Folders are often used as an organizational unit for identities and network resources, as well as dynamic groups and groups. Unlike dynamic groups or groups that determine user membership based on attributes, folders organize actual user entries.



If you are using folders to organize your identities, note that Active Directory servers are restricted to certain parts of the Identities Tree. By default, a folder can only be created beneath folders that have an object class of `domainDNS`, `o`, and `ou`. This rule is defined by Microsoft. For example, Active Directory uses a default folder called `Identities` to hold user information. The `objectclass` of this folder is `container`. Therefore, you cannot create a subfolder below it without Active Directory throwing an exception. However, the root entry of Active Directory is an instance of `domainDNS`. In this case, we can create a subfolder without any problem.

To add, modify, or rename a folder

- 1 Under **Folder**, click **Add**, **Modify**, or **Rename**.
 - If you are adding a new folder, you will be asked to locate the parent folder that the new folder will be added to.

- If you are modifying or renaming a folder, you will be asked to locate the specific folder.
- 2 Locate and select the folder. A folder properties page appears.

Modify Folder

Folder Name *	<input type="text" value="Administrators"/>
Description	<input type="text" value="Select Access administrators"/>
Address	<input type="text" value="709 Main Street"/>
Phone	<input type="text" value="416 991 0991"/>
Fax	<input type="text" value="416 991 0992"/>

Fields marked with a * are required

[Modify Folder](#)

Figure 165Folder Properties

- 3 Enter values for the folder properties.

➤ If you are modifying an existing folder, you cannot change the **Folder Name** property.

If you are renaming an existing folder, you can *only* edit the **Folder Name** property.

- **Folder Name:** Enter the folder's name. This is the folder's entry name (or RDN) and is shown on the Identities Tree.
 - **Description:** Optionally, enter a description of the folder.
 - **Address:** If the folder refers to a business unit, enter the business unit's address.
 - **Phone:** If the folder refers to a business unit, enter the business unit's phone number.
 - **Fax:** If the folder refers to a business unit, enter the business unit's fax number.
- 4 Click **OK** to commit these changes to the directory server for that identity location. The folder is added to the Identities Tree.

C Writing LDAP Expressions

LDAP requires you to make requests for information in the form of a stylized search expression that acts as an attribute filter.

This appendix describes how to write this filter using typical comparison operators.

When Search Expressions Are Used

Typically, you use attributes with the following features:

- *Personalization*: For details, see [Enabling Personalization](#) on page 92
- *Profile self-management*: For details, see [Chapter 8, Managing Identity Profiles](#)
- *Dynamic groups*: For details, see [Chapter 4, Organizing Identities and Resources](#)
- *Attribute decision point*: For details, see [Chapter 9, Creating Conditional Access Rules with the Rule Builder](#)

Understanding Comparison Operators

To support the search expression, Select Access uses comparison operators. These operators allow you to evaluate identities' attribute values against a value you provide.

Use the > or < operators and the >= or <= operators, with any kind of alphanumeric string. If you use these operators with alphabetic values, the comparison is performed lexicographically.

For example, words beginning with A are earlier in the alphabet and therefore deemed to be less than words beginning with B. Logically then, the word “abacus” is greater than the word “aardvark” using lexicographic ordering. You can use wildcards (*) with any alphanumeric string in the filter value field.

- Ensure you check the type of the attribute you are creating a filter for. For example, if you assume the attribute is an integer, when in fact it is a string, the results of your search filter expression might behave unexpectedly.
- Each directory server implements comparison operators differently, and operators can therefore act differently than expected. Only the Equal to comparison operator behaves consistently among all directory servers.
- Select Access supports the nesting of multiple search filters with the AND and OR boolean operators. For details, see [Nesting Filters](#) on page 288.

When writing your filters, use one of the comparison operators outlined in [Table 46](#).

Table 46 Comparison Operators

Operator	Description
=	<i>Equal to.</i> For example, if you select <code>street=Dalhousie</code> , all identities with a matching attribute value of Dalhousie street meet this definition.
>=	<i>Greater than or equal to.</i> For example, if you select <code>uidNumber>=939</code> , all identities with an attribute value of <code>uidNumber 939</code> or greater meet this definition.
<=	<i>Less than or equal to.</i> For example, if you select <code>uidNumber<=939</code> , all identities with an attribute value of <code>uidNumber 939</code> or lower meet this definition.
~=	<i>Approximately equal to.</i> For example, if you select <code>businessCategory~=admin</code> , all identities whose attribute value is similar to <code>admin</code> meet this definition.
=*	<i>Has any attribute value at all.</i> For example, if you select <code>businessCategory=*</code> , all identities with any attribute value meet this definition.
!=	<i>Not equal to.</i> For example, if you set <code>newRdn!=Smith</code> , all identities except those with the <code>newRDN</code> attribute value <code>Smith</code> meet this definition.
>	<i>Greater than.</i> For example, if you set <code>postOfficeBox>5</code> , all identities with an attribute value of P.O. Box 6 and higher meet this definition.
<	<i>Less than.</i> For example, if you set <code>postOfficeBox<5</code> , all identities with an attribute value P.O. Box 4 and lower meet this definition.
!~	<i>Not approximately equal to.</i> For example, if you select <code>businessCategory!~admin</code> , all identities except those whose attribute value is similar to <code>admin</code> meet this definition.
!*	<i>Has no value at all, or attribute does not exist in an entry.</i> For example, if you select <code>businessCategory!*</code> only identities without an attribute value meet this definition.

Nesting Filters

Select Access supports the nesting of multiple search filters with the `AND` and `OR` boolean operators. Nesting allows you to embed one expression in another. When multiple expressions are created, they are nested in the order they are added. Nesting allows you to build a single complex comparison expression. For example, if you create the following:

```
filter1
AND filter2
OR filter3
AND filter4
```

They are nested like this:

```
((filter1 AND filter2) OR filter3) AND filter4)
```


D Uploading Custom Plugins

Select Access includes several software modules that add specific features or services to an existing server. However, depending on your environment, you can upload your own plugins to customize Select Access' functionality. This appendix describes how to upload the GUI interfaces for the custom plugins you have created.

What is a Custom Plugin?

A custom plugin is one that is used by a Select Access system to customize it with specific business logic. Custom plugins can be Select Access plugins that you modify, or new plugins that you have made to specifically cater to your needs.

Uploading Different Policy Plugin Types

You can customize the Policy Builder by adding your own plugins:

- **Decision Point plugins** (the GUI equivalent to Policy Validator decider plugins): Rule Builder includes several types of decision criteria (such as authentication and encryption) you can use to create rules. You can also create your own custom plugins for other types of decision criteria. For information on uploading this plugin type, see [To upload a custom Decision Point or Authentication plugin](#) on page 289.
- **Authentication Service plugins**: Along with its supported authentication services, you can also create your own custom plugins for other third-party authentication services not supported by default. For information on uploading this plugin type, see [To upload a custom Decision Point or Authentication plugin](#) on page 289.
- **Subject Editor plugins**: Subject editor plugins allow you to create your own configuration screens that edit user, group, dynamic group, and folder properties. For information on uploading this plugin type, see [To upload a Subject Editor plugin](#) on page 290.

For details on creating custom plugins, see the *HP OpenView Select Access 6.2 Developer's Tutorial Guide*.



You can upload multiple plugins at a time, provided they are stored in the same folder.

To upload a custom Decision Point or Authentication plugin

- 1 Click **Tools** → **Configure Policy Plugins**. The **Configure Policy Plugins** dialog box appears.
- 2 Enter information as outlined in [Table 47](#).

Table 47 Directory Server Configuration

Property	Configuration Details
Decision Point Plugins	<ol style="list-style-type: none">1 Click Browse.2 Select the folder where the Decision Point plugin is located, and click OK. <p>When you next open the Rule Builder, an icon for the new decision criterion is added to the Rule Builder toolbar.</p>
Authentication Service Plugins	<ol style="list-style-type: none">1 Click Browse.2 Select the folder where the Authentication Service plugin is located, then click OK. <p>When you next open the Policy Builder, you can select the new service type when adding an authentication service.</p>

- 3 Click **OK**.

To upload a Subject Editor plugin

- 1 Click **Configure Subject Editor Plugins**. A list of currently installed plugins appears.
- 2 Do one of the following:
 - To add a new Subject Editor plugin, click **Add**.
 - To modify an existing Subject Editor plugin, select it from the plugin list and click **Modify**.
- 3 A dialog box appears which allows you to configure the plugins parameters.
- 4 Enter the **Plugin Name**. This is the name of the plugin as it will appear in the plugin list.
- 5 In the **Jar File** field, enter the path to the plugin `jar` file, or click **Browse** to locate this file.
- 6 In the **Config File** field, enter the path to the file containing the configuration parameters for the plugin, or click **Browse** to locate this file.
- 7 Click **OK** to upload the plugin.
- 8 Click **OK**.

E Troubleshooting

Appendix Overview

This appendix includes topics that troubleshoot the following areas of a Select Access-protected system:

- [Installer Errors](#) on page 291
- [Policy Builder Errors](#) on page 292
- [Policy Validator Errors](#) on page 294
- [Web server/Application Server Errors](#) on page 297
- [Denied Access Errors](#) on page 299
- [Directory Server Errors](#) on page 300
- [Certificate Errors](#) on page 301
- [Browser Errors](#) on page 304
- [Personalization Problems](#) on page 304
- [Password Management Problems](#) on page 304

Installer Errors

HP has documented the following error:

- [Out of Memory Error when Installing on HP-UX](#) on page 291

Out of Memory Error when Installing on HP-UX

Q--->Why am I generating an out of memory error when I try to install Select Access on HP-UX?

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

- 1 Start the System Administration Manager.
- 2 Double-click **Kernel Configuration**.
- 3 Double click **Configurable Parameters**.
- 4 Double click on the `maxdsiz` parameter.

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

Policy Builder Errors

HP has documented the following errors:

- [Policy Builder Does Not Initialize](#) on page 292
- [Network Discovery Not Detecting Redirects](#) on page 292
- [Policy Builder and Critical Path Index Node Values](#) on page 292
- [Running Policy Builder in Delegated Administration Mode](#) on page 293
- [Running Two Sessions on the Same Machine](#) on page 293
- [X11 Display Error with Delegated Mode on Solaris](#) on page 293

Policy Builder Does Not Initialize

Q--->Why do I get an error when I try to start the Policy Builder?

A--->If Policy Builder doesn't startup, there is most likely a proxy set up in the browser. Try to configure the web browser and bypass the proxy to Administration server.

Network Discovery Not Detecting Redirects

Q--->Why is network discovery not detecting redirects?

A--->The HTTP Network Resource plugin only detects a redirect if the HTTP tag contains a relative URL to the resource:

```
<META HTTP-EQUIV="Refresh" CONTENT="0;URL=allow.html">
```

It does not detect a redirect if the HTTP tag contains a fully qualified URL to the resource:

```
<META HTTP-EQUIV="Refresh" CONTENT="0;URL=http://  
www.mycompany.com/allow.html">
```

Policy Builder and Critical Path Index Node Values

Q--->My Policy Builder keeps generating an error. What is causing this?

A--->A misconfigured CP property can cause the Policy Builder to generate an error because the index node value is too low. If you encounter a lot of unusual Policy Builder errors, try to reconfigure this setting.

To set the correct maximum CP index node value:

- 1 Open the following file in a text editor of your choice:

```
<CP_install_path>/ds.properties
```

- 2 Locate the following parameter and ensure that it has the corresponding value:

```
directory.indexNodeMax=524288
```



If this parameter does not exist, you can always include it in your file.

- 3 Restart your directory server to ensure it uses the new parameter value.

Running Policy Builder in Delegated Administration Mode

Q--->I tried to run Policy Builder in Delegated Administration mode and my browser displays a “404 Not Found” message. What is causing this?

A--->This usually occurs if you:

- Enable Delegated Administration.
- Regenerate the Administration server’s and Policy Validator certificates.

This Delegated Administration Enforcer plugin consequently fails to connect to both components because its certificate hasn’t been updated.

To solve this problem:

- 1 Disable Delegated Administration mode.
- 2 Immediately re-enable Delegated Administration mode.

Running Two Sessions on the Same Machine

Q--->I want to run the Policy Builder in two modes: super administrator and delegated. But an error results as a consequence. Can I work around this problem?

A--->An issue exists which prevents administrators from running Policy Builder in both the Full Administration mode and Delegated Administration mode on the same machine. You can work around this issue in one of the following ways:

- By opening each mode in a different browser (that is, one in Firefox, one in Internet Explorer).
- In Internet Explorer, by disabling the **Reuse windows for launching shortcuts** option.

To disable this option:

- 1 In Internet Explorer, select **Tools** → **Internet Options**.
- 2 In the **Internet Options** dialog, select the **Advanced** tab.
- 3 In the **Advanced** tab, under the Browsing category, locate the **Reuse windows for launching shortcuts** option and disable it.

X11 Display Error with Delegated Mode on Solaris

Q--->If I reboot my machine without closing down the Policy Builder in Delegated mode on Solaris, I get the following error the next time I start the Policy Builder:

```
Can't connect to X11 window server using ':0.0' as the value of the
DISPLAY variable.
```

A--->The workaround for this issue involves exporting the display variable via a shell script before restarting the Administration server:

```
DISPLAY=<host_name>:0.0; export DISPLAY
```

Policy Validator Errors

HP has documented the following errors:

- [Policy Validator Registers with Wrong Address on Linux](#) on page 294
- [Policy Validator Generates Error When Installing](#) on page 294
- [Policy Validator Failing at Startup](#) on page 295
- [Policy Validator and Hostnames](#) on page 295
- [iPlanet and Sun ONE 6.0: Cookies Not Refreshed on IE](#) on page 295
- [Policy Validator Looping](#) on page 296
- [Policy Validator Short Circuits](#) on page 296
- [Policy Validator Missing SSL session Information](#) on page 296

Policy Validator Registers with Wrong Address on Linux

Q--->I just installed the Policy Validator on Linux. However, it incorrectly registered itself as local host only, not it's correct IP address. It seems this is causing the "Clear Validator Cache" issue that keeps appearing in the Policy Builder.

A--->On a RedHat Linux installation, the Select Access installer adds the full hostname of the Policy Validator to the localhost line in the `/etc/hosts` file.

For example, if the full hostname is `dev03.can.hp.com`, the line would appear similar to the one shown below:

```
127.0.0.1      localhost.localdomain localhost dev03.can.hp.com
```

Ensure that you remove your full hostname from the `localhost` entry so it looks like this:

```
127.0.0.1      localhost.localdomain localhost
```

Policy Validator Generates Error When Installing

Q--->I just tried installing the Policy Validator, however it keeps displaying an error message and I cannot complete the installation process. Why is this happening and what can I do?

A--->It is likely that your version of the `mscVRT.dll` is very old (that is, older than 6.00.8397.0). Typically, when this file becomes outdated, it may cause Policy Validator to report an error when you install the it as a service. To get around this issue, HP recommends that you follow the steps outlined below:

- 1 When the Policy Validator generates an error, click **OK** on the popup message to continue with the installation.

- 2 Click **OK** until the **Configure HP Select Access** screen appears.
- 3 Check the **No** box to skip the configuration of Policy Validator (as well as other components).
- 4 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.
- 5 Open a Command Prompt and cd to the following directory:

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

```
validator -I
```
- 7 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 and Sun ONE 6.0: Cookies Not Refreshed on IE

Q--->Why is the Policy Validator not refreshing my cookies?

A--->It is. However, session cookies for identities that the Policy Validator allows to access network resources are not refreshing properly. This issue is limited to iPlanet and Sun ONE web servers using Microsoft Internet Explorer. The Internet Explorer only refreshes cookie data from iPlanet and Sun ONE servers when:

- You have recently modified the page.

- A page is not in its cache.

Therefore, the cookie is timing out despite the fact that Policy Validator has refreshed it. To solve this problem, disallow caching of any content:

- 1 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.
- 2 From the drop-down list, select a server and click **Manage**. The **Server on/off** page appears.
- 3 Click the **Content Mgmt** tab. The **Primary Document Directory** page appears.
- 4 Click the **Cache Control Directives** link in the left navigation bar. The **Cache Control Directives** page appears.
- 5 Under **Cache Control Response Directives**, enable **No Cache** and click **OK**. The **Save and Apply Changes** page appears.
- 6 Click **Save and Apply**.

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 6.2 Installation Guide*.

Policy Validator Short Circuits

Q--->The Policy Validator displays a message stating that it is “short circuiting” when it does certificate authentication for transient identities.

A--->Certificate chain verification is a very expensive operation in term of the network traffic it creates, which involves the following operations: LDAP lookups, RSA signature verifications, and possible CRL and OCSP lookups. As a result, it is timing-out before verification is complete. To prevent this from happening, decrease your **Certificate Verify Interval** value by reconfiguring your Administration server.

Policy Validator Missing SSL session Information

Q--->I've noticed that the Policy Validator is dropping session information from queries originating from Apache plugins under SSL mode. How can I correct this?

A--->It is important to get the complete SSL session back into your queries, because without it, any encryption decision points in your existing rules fail. To correct this problem you need to open your `httpd.conf` file on your web server and add the following line to the Enforcer plugin section:

```
SSLOptions +ExportCertData +CompatEnvVars +StdEnvVars
```


Web server/Application Server Errors

HP has documented the following errors:

- [HTTP Basic Authentication Problematic](#) on page 297
- [Restricted IBM HTTP Server Resources](#) on page 297
- [Virtual Web Server Support Problems with IIS](#) on page 298
- [Caching Problems with IIS](#) on page 298
- [Integrated Windows authentication issues on IIS](#) on page 298

HTTP Basic Authentication Problematic

Q--->I have created an HTML form with at least two text boxes named “user” and “password”. I am using HTML basic authentication, and have applied a deny policy to Unknown Identities and an allow policy to Known Identities. However, when an identity enters their credentials with the Password server I configured, they are denied access. The Policy Validator then prompts the end user for credentials again using HTTP basic authentication. Why is this happening?

A--->It appears that the Policy Validator is authenticating with the credential data from the form instead of the credential data from the HTTP basic authentication prompt. If you were to log the Policy Validator’s output, you would notice two user and password XML elements: one from the form and one from the HTTP basic authentication. To get form-based logins to work on a Select Access-protected system, ensure that you both check the **Enable Web Session Cookies** box and uncheck the **Login using Forms** box when setting up the Enforcer plugin’s **Tuning Parameters**.

Restricted IBM HTTP Server Resources

Q--->I have restricted access to confidential resources on the IBM HTTP server that was bundled with WebSphere. However, it appears that irrespective of the policy I set, identities can still access these resources via Telnet. How do I prevent this from happening?

A--->Due to the way in which IBM has implemented security on their IBM HTTP server, identities are able to access restricted resources via Telnet. HP has reported this issue with IBM. In the meantime, HP recommends that you check the **Fast cache response** configuration parameter. If you enable this option, it negatively impacts Select Access’ 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:

- 1 Doing one of the following:
 - Running the Setup Tool
 - Displaying the Component Configuration tool from the Policy Builder
- 2 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 7, Configuring the Enforcer Plugins](#) in the *HP OpenView Select Access 6.2 Installation Guide*. For details on the Component Configuration tool, see [Chapter 15, Modifying Components' Central Configuration Parameters](#).

Integrated Windows authentication issues on IIS

Q--->I am having problems with my Integrated Windows authentication service which runs on an IIS web server over Windows 2000. How can I authenticate using NTLM?

A--->You can authenticate using NTLM by doing the following:

- 1 Open an MS-DOS Command Prompt session.
- 2 Navigate to the `Inetpub\AdminScripts` folder.
- 3 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.
- 4 If you receive an error message, enter the following command from the same location:

```
cscript adsutil.vbs get w3svc/NTAuthenticationProviders
```
- 5 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 299
- [Denied Access on Default Page](#) on page 299
- [Browser Gets Deny yet Policy Validator Returns Allow](#) on page 300

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:

- 1 In the Policy Matrix, right-click the network service and select **Properties**. The **Editing Service Properties** dialog box appears.
- 2 Enter a new **Name** that matches the service name that the Enforcer plugin is sending.

Denied Access on Default Page

Q--->I have allowed access at the service level for my web server, but the Policy Validator denies my identities are access when they go to the default page.

A--->You have manually added the default page as a resource under the web server and created a security policy for the resource. Delete the resource from the Resources Tree; it is not needed because the policies created for the service apply to the web server's default page.

Browser Gets Deny yet Policy Validator Returns Allow

Q--->Why is my web browser displaying a deny error message, even though Policy Validator is returning an allow decision?

A--->Web servers can have their own mechanism for checking access entitlements. So, while you may have configured the Policy Builder with an allow for this resource, you may have set up your server's mechanism with a deny. If you are using server-specific access controls, make sure they are consistent with your Policy Builder policies.

Directory Server Errors

HP has documented the following errors:

- [Active Directory 2003 and Profile Password Setup Problems](#) on page 300
- [iPlanet and iPlanet Unicode Problems](#) on page 301
- [Critical Path Over SSL Problems](#) on page 301

Active Directory 2003 and Profile Password Setup Problems

Q--->I've tried creating a profile with the Policy Builder, but when I try to create a password, an error message tells me that password I set does not meet the password policy for ADS.

A--->You must always try to meet the password policy of your directory server. ADS requires that passwords be equal to or greater than seven characters. However, you can work around this limitation by disabling ADS' policy by modifying the Password properties and Lockout properties for both the Default Domain Security Policy and Default Domain Controller Security Policy on the server as follows:

Password Policy Properties

- reverse encryption: disabled
- complexity rules: disabled
- minimum length: 0
- minimum age: 0
- maximum age: 0
- password history: 0

Lockout Policy Properties

- reset: not defined
- lockout threshold: 0
- lockout duration: not defined

iPlanet and iPlanet Unicode Problems

Q--->How do I fix Unicode character set errors on iPlanet?

A--->Locate the plugin that enforces 7-bit (ASCII) character storage. When you disable this plugin, you will be able to store your Unicode characters correctly.

Critical Path Over SSL Problems

Q--->I am having trouble connecting to Critical Path over SSL. Why is this happening?

A--->The directory server certificate is probably not compliant with Transport Layer Security (TLS) version 1.0. Critical Path does 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 301
- [Generic Problems](#) on page 302
- [Microsoft Certificates and Failed Signing](#) on page 302
- [Problems Specific to IIS](#) on page 303
- [Problems Specific to Apache](#) on page 303

Browsing for OCSP certificates on Critical Path

Q--->Why does the Policy Validator have problems locating the OCSP certificate authentication service's certificate I uploaded?

A--->This problem occurs because you have not configured the `usercertificate` attribute to specify what type of search the Policy Validator can make on its values. You can configure the type of search the Policy Validator can make to find the certificate entry with a Critical Path's feature called "matching rules":

- 1 In Critical Path's InJoin Directory Server Configurer, display the **Attributes Registry** page for the `usercertificate` attribute.
- 2 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 **Help** on this page.

- 3 Click **Change Attributes** to record these changes.
- 4 Restart Critical Path to use these new settings.

Generic Problems

Q--->Why am I having problems using certificates with Select Access?

A--->For the certificate plugin to locate an identity:

- 1 The Subject DN of the certificate must meet one of the following conditions:
 - Exactly match the DN in the identity's profile
 - Contain a `uid` attribute that exactly matches the `uid` attribute in the identity's profile
 - Contain a `cn` attribute that exactly matches the `cn` attribute in the identity's profile
- 2 The identity's profile can have a `userCertificate;binary` attribute that contains the certificate used to authenticate components.
- 3 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:

- 1 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.
- 2 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:
- 1 Choose **Tools** → **Internet Options**.
 - 2 On the **Advanced** tab, in the **Security** section, select the **Use PCT 1.0** check box.



You can also check the Microsoft knowledge base for known issues with IIS certificate authentication.

Problems Specific to Apache

Q--->Why does mod_Enforcer get a malformed certificate when it retrieves SSL session information from the Policy Validator's cache?

A--->This occurs because the Apache 2 Enforcer plugin appears not to correctly save the client certificate. As a result, when it passes this malformed to the certificate, Policy Validator rejects it.

To fix this problem consider either of the following alternatives:

- Turn off SSL session caching on Apache. You can do this by commenting out all `SSLSessionCache` entries.
- Build Apache with the MM shared memory library and use one of the following shared memory caches: `shmmt:` or `shmcb:.`

Browser Errors

HP has documented the following error:

- [SSO Failing on Internet Explorer](#) on page 304

SSO Failing on Internet Explorer

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

A--->SSO always fails on IE when identities link from a protected (HTTPS) to a non-protected (HTTP) site. This failure happens because the HTTP Referer header is not being sent when connecting to or from a non-protected page. Microsoft does this to prevent secure data from being accidentally transferred to unsecured sites. Depending on how you configure the 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.

Personalization Problems

HP has documented the following error:

- [Empty Dynamic Group Attribute Values](#) on page 304

Empty Dynamic Group Attribute Values

Q--->I have set up personalization so that it returns dynamic group and group information and some attributes in the dynamic groups. Why do I get “attribute=”, with nothing appearing after the equals symbol for those attributes?

A--->The attribute is not an attribute of the dynamic group or group. As a result, the value appears empty. For details on which attributes you can use, see [About Directory Attributes](#) of the *HP OpenView Select Access 6.2 Concepts Guide*.

Password Management Problems

HP has documented the following error:

- [Active Directory 2003 and Profile Password Setup Problems](#) on page 300

Glossary

A

Access Control

The authorization policies and conditions that regulate identity access to resources with a goal towards preventing unauthorized use or use in an unauthorized manner.

Administration server

The server that administers Select Access' configuration parameters, policy data, and certificates. This component writes all relevant details to the Policy Store.

Administrator

An identity with delegated entitlements. Only delegated entitlements are available when the individual runs the Policy Builder in Delegated mode or Web Administration. *See also* [Delegation](#) and [System Administrator](#).

Alias

A pointer or shortcut to the actual identity profile (also known as directory entry), which is typically shown under any group to which the identity belongs. *See also* [Identity Profile](#).

Approval Process

The process of approving the grant, modification, or revocation of entitlements for an identity. Often organizations employ manual approval processes. A compelling benefit of Select Access is the automation of these processes through its workflow feature. *See also* [Approver](#) and [Workflow](#).

Approver

An administrator who has been given workflow approval rights via the Workflow function entitlement.

Attribute

One or more characteristics that are part of an identity profile. Attributes are name/value pairs with a type that is assigned a value. For example, an attribute called "Department" may be assigned the values of, "IT", "Sales", or "Support". These attributes are interpreted and assigned appropriately to profiles in different applications (LDAP-compliant directories, databases, SAPs, and so on) based on the mapping rules defined for that application.

Audit Policy

A policy that defines which events are logged for a given Select Access component. Audit policies monitor stability, ensure data integrity, and maintain corporate security. *See also* [Audit Trail](#).

Audit Trail

A log destination to which time-based messages of a given severity are recorded. Select Access allows you to output messages to destinations like Select Audit, databases, files, and so on. *See also* [Audit Policy](#).

Authentication

The act of verifying the credentials of an identity and matching them with an identity profile. The evaluation of credentials ensures that the identity is truly who or what they claim to be. *See also* [Authorization](#).

Authentication Service One of the supported methods used by the Select Access system to verify login credentials claimed by or for an identity. Authentication services can use different mechanisms, which can include tokens, certificates, secrets, or simply IDs/names and password combinations.

Authorization

The process of defining and enforcing the entitlements of an identity. Authentication is a prerequisite for authorization. *See* [Access Control](#) and [Authentication](#).

B

Branch (true/false)

The logical connections among two or more nodes in a conditional access rule:

- **If the request does match the criteria:** It is considered *true* and follows the true branch to the next node in the rule.
- **If the request does *not* match the criteria:** It is considered *false* and follows the false branch to the next node in the rule.

See also [Node](#) and [Rule](#).

C

Caching

The ability to retrieve recently accessed data in order to speed up repeated access to the same data.

Challenge-Response

A common authentication technique that prompts an identity (the challenge) to provide some data only known by the identity (the response). An example of challenge-response authentication is a smart card.

Conditional Access

See [Access Control](#), [Policy](#) and [Rule](#).

D

Data Signing

See [Signature](#).

Data Location

A directory server that acts as a repository for identity profiles. *See also* [Identity Profile](#) and [Policy Store](#).

Delegation

The act of assigning administration or even registration entitlements to another identity. For example, by delegating registration, you are entitled to perform registration on behalf of another identity.

Dynamic Group

Sometimes referred to as a Role in LDAP directories. A named collection of identities and possibly other groups whose membership is based on attribute values in the identity profile. Unlike Groups which are static, Dynamic Groups do not allow you to directly add additional members. Assignment to a dynamic group is automatic and shifts over time. For example, you can create a Dynamic Group called “Big Spenders”. To become and remain a member of this dynamic group, an attribute called “Monthly Purchases” must be higher than \$500.00. *See also* [Group](#).

E

Entitlement

Administrative functions of Select Access that are used by the system to:

- Control access
- Manage identities and resources
- Manage internal components

For example, in Select Access, a typical administrative entitlement is the delegation of component configuration responsibilities to other/additional administrators on your team.

Entity

An individual, a corporate body, a federation, an application, or a service that can be described conceptually by a set of attributes. For example, you can have an Employee entity with attributes values such as Last Name, First Name, Address, and so on. You can also have a Server entity with attribute values such as Domain, Type, Organization, and so on. *See also* [Identity Profile](#).

F

Failover

The transfer of operation from a failed component (for example, directory, server, system) to a similar, redundant component. In Select Access specifically, redundant Policy Validators and directory servers ensure that data flow remains uninterrupted and your access control system operable.

Federation

The combination of business and technology practices to enable identities to span systems, networks and domains in a secure and trustworthy fashion. This is analogous to how passports are used to assert our identity as we travel between countries.

G

Group

A named collection of identities and possibly other groups. You can directly make an identity a member of a group or indirectly through membership in a sub-group. A group is often composed to apply similar access control rights. For example, you can create a group for all your customers, another group for your suppliers, and another group for your employees.

When you create an access rule for a group, all group members inherit the access policy, unless you override it. *See also* [Dynamic Group](#).

H

There are no terms that begin with this letter.

I

Identity location

See [Data Location](#).

Identity Management (IdM)

The process of identifying entities in a system and controlling their access to resources within that system. In Select Access, access is typically controlled by associating rights and restrictions with the established identity profile. You can use additional software (for example, Select Identity) to automate many administrative tasks associated with the management of identity profiles (for example, creating, deleting, modifying, and so on). *See also* [Entity](#) and [Identity Profile](#).

Identity Profile

A database record or directory entry that includes a set of authentication credentials, profile attributes, and entitlements for a single entity. Identity is often used as a synonym for “user”, although identity is not restricted to an individual. *See also* [Entity](#).

Inheritance

Occurs when the authorization policies of a defined group or folder are applied to each constituent (identities or resources) within that group.

J

There are no terms that begin with this letter.

K

There are no terms that begin with this letter.

L

LDAP (Lightweight Directory Access Protocol)

A set of open protocols for accessing information directories. LDAP can make the physical network topology and protocols transparent so that a network identity can access any resource without knowing where or how it is physically connected.

M

There are no terms that begin with this letter.

N

Network Resource

See [Resource](#).

Network Service

See [Resource Service](#).

Node

In a rule decision tree, a point where two or more true/false branches meet. A node can be a decision point (where outcomes are evaluated based on criteria configured by an administrator) or a terminal point (where final outcomes are triggered).

Nonce

An opaque piece of data created by the Policy Validator and placed in a cookie. In Select Access, a nonce is an important component of an authentication and authorization protocol.

O

There are no terms that begin with this letter.

P

Password Management

The process of securely setting, maintaining, and synchronizing passwords in an identity profile. *See also* [Identity Profile](#), [Password Synchronization: Forward/Reverse](#), [Password Reconciliation](#) and [Password Reset](#).

Password Synchronization: Forward/Reverse

The business policies/processes, software, and network infrastructure that enable identities to maintain a single Password value that is accepted across multiple Login Accounts, domains, applications, and so on. Password synchronization can be forward sync mechanisms (where the password in the identity profile is shared with multiple systems) or reverse sync mechanisms (where one of the multiple systems writes the password to the identity profile). *See also* [Identity Profile](#), [Password Management](#), [Password Reconciliation](#) and [Password Reset](#).

Password Reconciliation

The process of adopting passwords in the identity profile when:

- The identity has a recognized profile
- An aliasing technology is used

See also [Identity Profile](#), [Password Management](#), [Password Synchronization: Forward/Reverse](#) and [Password Reset](#).

Password Reset

The business policies, software, and network infrastructure that determines when and how an Password values in an identity profile can be securely changed if they are forgotten. *See also* [Identity Profile](#), [Password Management](#), [Password Reconciliation](#) and [Password Synchronization: Forward/Reverse](#).

Policy

A set of defined practices or a formal statement of operational rules, set by an organization to assist in managing some aspect of its business. For example, in Select Access, an access control policy determines identity-based level of access (allow/deny/conditional) for specific internal and external resources.

Policy Query

A request for a resource made by an Enforcer plugin to the Policy Validator. The Policy Validator evaluates the identity's authorization policy to determine whether an identity is allowed access to the network resource. The access decision is sent to the Enforcer plugin. *See also* [Policy Reply](#).

Policy Reply

A decision to a resource request made by the Policy Validator via an Enforcer plugin. Based on the identity's authorization policy, the Policy Validator replies with an allow, deny or conditional decision. *See also* [Policy Query](#).

Policy Signing

See [Data Signing](#).

Policy Store

A directory server that acts as a repository for policy data and configuration information. *See also* [Data Location](#).

Profile

See [Identity Profile](#).

Profile Self-Management

Also known as Self-Service. The business policies, software, and network infrastructure that determines when and how identities can securely update attribute values in their profile. Select Access supports self-management with conditional rules that include a Profile Self-Management terminal point. *See also* [Password Management](#).

Provisioning

The automation of all business processes and tools to centrally manage the life cycle of an identity. For example, the creation and modification of profile attributes, the propagation of data to affiliated systems, the delegation of identity authentication and authorization, the decommissioning the profile, and so on.

Q

Query

See [Policy Query](#).

R

Referral

A response that redirects the Select Access component to the directory server that holds the data it requires.

Registration

The business policies, software, and network infrastructure that allows an unknown identity to become a known and authenticatable identity by formally recording attributes and values in a central repository for future identity verification. Registration is typically performed by an end user that is requesting resource access. However, registration can also be delegated. *See also* [Delegation](#).

Resource

A discrete piece of information, such as a file or URL, that you can access on a network. A resource can contain other resources. On the Resources Tree, a resource must be stored below a service. The Resource plug-in is used to gather resource URLs and add them to the Resources Tree. *See also* [Resource Service](#).

Resource Service

A computer or device on a network that manages network resources. A service provides access to a resource via one or more protocols, for example, HTTP or FTP. Examples of services include file servers, web servers, NT domains, Certificate servers. A service can also provide access to other services, and can be represented in the Resources Tree by a host name. For example, a web server may be shown in the tree according to the server's host name, for example, www.acme.com. *See also* [Resource](#).

Rule

A programmatic control over system behavior. Rules are typically used for intelligent assignment of entitlements or for the capture of granular access criteria and/or conditions.

S

Self-Registration

See [Registration](#).

Self-Service

See [Profile Self-Management](#).

Signature

An encrypted digital text block that authenticates the identity of the sender of a message, or of the signer of a document. By signing data with a digital signature, you can also ensure that the original data is untampered with.

System Administrator

Also known as the super administrator. A system administrator is the Root Administrator of the Policy Builder, and has all features and functions activated. The system administrator can also use Web Administration if she chooses. *See also* [Administrator](#).

T

There are no terms that begin with this letter.

U

There are no terms that begin with this letter.

V

There are no terms that begin with this letter.

W

Workflow

A business process that helps to ensure data integrity by tracking administrative events and automatically routing the outcome of these events to an approver. Only after approval does the change become implemented. Workflow is considered a multi-administrator, multi-stage

process, because two or more administrators collectively share, manage, and operate on a shared repository of information.

X

There are no terms that begin with this letter.

Z

There are no terms that begin with this letter.

Index

A

Access policies

- administering, 130
- allow, overview, 131
- creating and applying, 15
- deny, overview, 131
- for multiple identities, 135
- for unknown identities, 130
- how used, 129
- icons used, 132
- inheritance of. *See* Inheritance
- managing, 205
- overriding, 137
- rules. *See* Rules
- scalability of, 133
- setting, 131, 132
- tips, 129, 139
- types of, 129, 131, 132
- using the Policy Matrix, 130, 132

Access rules. *See* Rules

Accounts

- activating, 142, 143, 146
- definition of, 142
- disabling, 144, 146
- idle time allowed, 144
- name, defining, 281
- re-enabling after deactivation, 151
- self-managing, 142
- setting preferences, 141
- status of, 144

Accounts. *See* Profiles

Addresses

- business, 285
- email, 42, 281
- entity, attribute for, 307
- for Policy Builder, 277
- network, 21, 35, 37, 49, 51, 116, 160, 165, 277
- Policy Validator, 267

Administration Matrix

- categories of, 202
- delegation policy options, 210
- entitlements, delegation. *See* Delegated Administration
- entitlements, workflow. *See* Workflow
- icons, 203, 204
- overview, 202
- policies, 202
- See also* Policy Matrix

Administration modes

- configuring Select Access for, 199
- Delegated Administration. *See* Delegated Administration
- overview, 197
- Root Administration. *See* Root Administration
- Self Administration. *See* Self Administration
- Web Administration. *See* Web Administration

Administration server

- administration modes. *See* Administration modes
- certificates for, 199
- comparing login credentials, 23
- configuring audit settings, 232
- configuring components, 252
- configuring data signing, 247
- configuring Policy Builder URLs, 20
- configuring the Web Administration URL, 276
- logging in, 278
- logging into, 22
- security alerts, 21, 277

Alerts

- configuring notification with, 160, 183
- Java security, 23
- policy data violations, 248
- SSL security, 21, 277

Algorithm, encryption types used, 269

Aliases, 68

Applet, Policy Builder. *See* Policy Builder

Attributes

- activating, 94, 142
- available for self-management, 193
- available with directory servers, 187
- decision point for, 170
- delegation policies for, 210
- directory servers, implementation of, 172
- directory servers, limitations of, 94
- directory servers, reading from, 37
- directory, using in rules, 160
- exporting, 94
- features using, 287
- knowing which to use, 95
- list of available, 37
- names of, 95
- ordering, 195
- query, copying into, 179, 270
- query, using in rules, 160, 176
- searching for. *See* Search expressions
- selecting with Citrix NFuse, 186
- self-managing. *See* Self Administration
- troubleshooting, 304
- types, 172
- used in dynamic groups, 74
- values, 172

Audit

- benefits, 231
- client, 231
- common settings, 231, 232
- component, 237
- default settings, 232
- entry, 233
- event level, 237
- group settings, 232
- log file destination, 235
- override settings, 232
- policy, configuring, 233, 237, 238, 240, 268
- settings, definition, 231
- standard error destination, 237
- system logging destination, 237
- trail, configuring, 233, 260, 268

Authentication

- Certificate. *See* Certificate authentication
- decision point plugin, using, 86
- failed, 87
- HTTP basic, 191
- identities, segmenting, 127
- Integrated Windows. *See* Integrated Windows authentication
- of delegated administrators, 86
- Password. *See* Password authentication
- RADIUS. *See* RADIUS authentication
- Registration. *See* Registration authentication
- SAML. *See* SAML
- SecurID. *See* SecurID authentication
- Select Auth. *See* Select Auth
- services, delegating, 208
- services, list of, 100
- services, list of, creating, 98
- services, list of, refreshing, 100
- services, methods employed, 86
- services, plugins for, 289
- setting up, overview of, 97
- storing transient identities, 98
- Trusted server. *See* Trusted Servers authentication
- using in rules, 93, 160, 173

Authorization. *See* Access policies

B

Backslashes, using, 46

Boolean operators, nesting filters with, 170, 176, 178, 287

Browsers

- configuring preferences, 24
- errors, 304
- importing certificates into, 22, 199, 277
- opening Policy Builder in own window, 24
- recommended, 21

Business logic, capturing, 162

C

Cache

- cleanup interval, 246, 270
- cleanup percent, 246, 270
- displaying prompts for, 271
- fast cache response, 297
- manually clearing, 246
- of policy data, 246, 270
- of user data, 36, 99, 105, 106, 108, 113, 115, 118, 121, 125, 126, 246
- preferences of, 246
- refresh interval, 73, 147, 246, 270
- transient identities, 99, 100
- warnings for, 246
- warnings, configuring, 246
- web pages, 265

Case sensitivity, 172

CDP, 122

Certificate authentication

- advanced configuration, 122
- CDP support for, 122
- certificate requirements for, 120
- configuring lookups for, 123
- creation of transient profiles with, 99
- CRL checks, 123
- database used by, 99
- introduction, 86
- OCSP checks, 123
- properties of, 120, 122
- troubleshooting, 120
- uploading, 120
- verification process, 99

Certificates

- DN mapping, 123
- encoding for, 199
- for signing log data, 248
- for signing policy data, 247
- for SSL encryption, 21, 22, 35, 277
- identity data location, 39
- importing, 35, 39, 199
- installing, 22, 277
- key file, losing, 248
- key file, sharing, 269
- query property for, 179
- SSL security alert, 21, 277
- troubleshooting, 296, 301, 302, 303
- unknown CAs, 122
- viewing Policy Builder's, 22, 277
- X.509, 117

CGI, troubleshooting, 304

Challenge/response authentication. *See* Radius authentication or SecurID authentication

Characters

- invalid, 273
- naming limitations, 103, 163, 221
- set used, 264
- special, for passwords, 148

Citrix NFuse

- personalizing content for, 186
- uploading plugin for, 186

Client settings

- configuring tree thresholds, 83
- threshold values, 83
- warnings, enabling, 246

Code signing, 23

Comparison operators

- behavior of, 287
- using in search expression, 178, 287, 288

Components, configuring

- Administration server requirement, 252
- audit settings, 232
- centrally located parameters, 251
- client settings, 271
- configurable parameters, 252
- deleting parameters, 271
- Enforcer plugins, 255
- group default parameters, 252
- IDs for, 251
- multiple components, 253
- override parameters, 252, 253
- Policy Validator, 267
- refreshing parameters, 271
- restoring defaults, 255, 267
- tool, displaying, 251
- tool, interface elements of, 252
- warning message, 271

Conditional expressions. *See* Search expressions

Conditional rules. *See* Rules

Content

- forms. *See* Forms
- network resources. *See* Resources
- personalization of. *See* Personalization

Cookies

- configuring with Policy Validator, 269
- domain for, 256
- effect on Rule Builder, 157
- session, enabling, 265
- troubleshooting, 295, 304

Credentials
 administrator login, 23
 authentication with, 85
 collecting, 106, 107, 116, 118, 125, 127, 128
 expiry of, 23, 269
 lookup, order of, 32
 renewing, 23
 securing, 269

Criteria, decision. *See* Rules

CRLs, 122

Custom properties, Enforcer plugin, 266

Custom responses, 161, 189

D

Data
 audit, capturing. *See* Audit
 authentication of, 247
 collecting from identities, 86, 106, 107, 116, 118, 125, 127, 128, 141
 configuring signing of, 247
 creating hierarchy of, 66, 67
 directory. *See* Directory servers
 entitlements, types of, 203
 for personalization. *See* Personalization
 managing, 15, 141
 refreshing in Policy Builder, 42, 100, 162, 207, 246
 representation of in Policy Matrix, 25, 27, 28, 29, 31, 35, 42, 43, 44, 45

Data integrity, ensuring. *See* Audit

Data signing
 delegating, 208
 detecting violations, 248, 249
 enabling and disabling, 247
 key for, 248
 overview, 247
 setting up, 247

Databases
 used by certificate servers, 99
 used by RADIUS, 99
 used by SecurID, 99

Debugging, event level filter, 239

Decider plugin, Policy Validator, 159

Decision points
 alert decision point, 183
 attribute logic decision point, 287
 authentication decision point, 93, 160, 173
 Citrix NFuse decision point, 186
 copying and pasting, 165
 custom plugins for, uploading, 159, 289
 definition of, 159
 deleting, 165
 directory attributes decision point, 160
 encryption decision point, 169, 170, 172
 list of available, 165
 network and domains decision point, 165
 overview, 164
 part of rules, 165
 ports decision point, 174
 query attributes decision point, 176
 See also Rules
 time of day decision point, 167
 workflow, configuring
 XPath decision point, 180, 181, 182

Delegated Administration
 administrators, authenticating, 98
 attributes, list of, 207
 authentication services for, 201
 certificates, 199
 changes, refreshing concurrent, 207
 enabling, 207
 Enforcer plugin for, 206, 255
 functions, list of resources, 207, 208
 grid for, 205
 identity management, list of resources, 208
 impact of, 206
 inheritance of entitlements, 213
 logins, 205
 matrix for. *See* Administration matrix
 network management, list of resources, 208
 overview, 19, 203
 policies, types of, 209
 port for, 198
 running Policy Builder in, 21
 sub-delegation, 208
 troubleshooting, 293

DER encoding, 199

Desktop
 authentication. *See* Integrated Windows authentication
 shortcuts to run Policy Builder, 23

Dictionary, used for passwords, 145

Digital certificate *See* Certificates

- Digital signatures
 - benefits of, 247
 - overview of, 247
 - setting up, 247
 - signing audit trails, 268
 - signing states, 248
 - troubleshooting, 302
 - used to sign data, 247
 - Directory servers
 - differences in operator behaviors, 287
 - encrypting sessions with SSL, 35
 - entries, deleting, 62
 - entries, permanently deleting, 77
 - identity lookups, 99
 - invalid characters, 273
 - limitations of attributes, 187
 - logging into, 35
 - organizing, 68
 - password limitations with, 193
 - plugins, uploading, 159, 289
 - policy data violations, 248, 250
 - policy store. *See* Policy store
 - profiles. *See* Profiles
 - publishing keys to, 269
 - refreshing Policy Builder data, 42
 - replicating, 36
 - schemas, reading, 37
 - transient entries, 99
 - troubleshooting, 300, 301
 - uploading certificate for authentication server, 120
 - using attributes in rules, 160
 - Discovery, network
 - delegating, 208
 - plugins, built-in, 56
 - plugins, configuring, 54, 56
 - plugins, list of, 55
 - plugins, requirements of, 54
 - preconditions, 58
 - running, 58
 - scan order of multiple plugins, 55
 - scanning HTTP or HTTPs services, 54
 - terminating, 63
 - URLs, invalid, 54
 - URLs, relative, 54
 - Disinheritance, preventing, 214
 - Domains
 - cookie, 256
 - multiple, 256
 - pass-through, 259
 - scanning, 43
 - single, 256
 - using in rules, 160, 165
 - Dynamic groups
 - assigning membership to, 74
 - attributes needed for, 287
 - authenticating, 127
 - comparison expressions, creating, 75
 - configuring, 73
 - creating, 73
 - definition, 29, 66, 307
 - deleting, 77
 - impact on performance, 73
 - inheritance logic with, 73
 - limitations, 73
 - members, finding, 75
 - members, hiding, 73, 75
 - members, viewing, 75
 - membership, viewing, 75
 - multiple locations, spanning, 73
 - overview, 68, 73
 - personalization for, 94
 - tips, 73
 - troubleshooting, 304
 - when to use, 69
- E**
- Email
 - alerting administrators with, 183
 - as user entry property, 42, 281
 - server for, configuring, 219
 - Encoding
 - DER, 199
 - PEM, 199
 - Encryption
 - algorithm types, 269
 - using in rules, 160, 169, 170, 172

- Enforcer plugins
 - audit settings for, 232, 260
 - available Policy Validators, 261
 - caching pages, 265
 - character set, 264
 - configuring, 251, 255
 - custom properties, 266
 - enabling cookie session, 265
 - enabling form-based login, 264
 - exporting environment variables, 95
 - for Delegated Administration, 255
 - HTTP headers, 95
 - load balancing support in, 269
 - local configuration file, 261
 - Policy Validators, communicating with, 260, 261, 263
 - protected sites, sharing list of, 257
 - queries, details in, 264
 - settings for password management, 145
 - troubleshooting, 298, 299
 - tuning performance of, 263
 - used for Delegated Administration, 206

Envelope, SOAP, 181

Environment variables

- exporting attributes to, 94
- names of, 95
- personalizing with, 93

Errors

- browser, 304
- codes for SecurID, configuring, 119
- configuring to a standard stream, 237
- denied access, to service, 299
- denied access, web page, 299, 300
- logging, 239
- Policy Builder, 292
- standard, logging to, 237

Evaluation criteria in Rules. *See* Rules

Events, recording. *See* Audit

F

Failover, 261, 263

Fatal exceptions, 239

Filenames, ignored, 257

Filtering

- events, 237
- searches. *See* Searching

Filtering events, 239

Finding

- dynamic group membership, 75
- entries, 80, 82, 278
- expanding, 78, 79
- post-search results, 81
- profiles, 77
- quick search, 78
- resources, 77

Folders

- configuring properties for, 76
- creating, 75, 98, 284
- definition of, 29, 67
- deleting, 77
- organizing identities with, 67
- using with identities, 29
- using with resources, 43, 67
- when to use, 68

Forms

- customizing for use, 128
- login, 264, 297
- password, 125
- RADIUS challenge response, 116
- registration, 106, 107, 110, 127
- SecurID authentication, 118
- self-management, 142, 145, 146, 151
- where saved to, 128

Frame sizes, reconfiguring, 157

Functions

- delegation policies for, 208, 211
- list of, 207

G

Grids

- Administration. *See* Administration
- Matrix
- Policy. *See* Policy Matrix

Groups

- authenticating, 127
- configuring, 71
- creating, 69, 282
- definition of, 29, 66
- deleting, 77
- dynamic. *See* Dynamic groups
- membership, assigning, 70, 71, 73, 77
- membership, changing, 71
- membership, viewing, 72
- modifying, 284
- overview, 66
- personalization, configuring, 94
- policies, assigning access, 135
- properties, configuring, 69, 282, 284
- renaming, 282
- when to use, 69

H

Hiding

- dynamic group membership, 75
- entries, 82
- profiles, 82
- unhiding, 83

Hostnames

- directory server, 35
- directory server, replicated, 37
- limitation of, 165
- mailserver, 219
- output by plugin, 55
- RADIUS, 116
- resources, 47, 48, 59
- rules, including in, 165
- substituting IP with, 21
- web service, 46
- web services, 80

HTML form templates, 106, 110, 116, 118, 125, 127, 142, 145, 149, 193, 194, 195

HTTP

- basic authentication, 191, 297
- collecting credentials over, 104
- GET request, 304
- headers, 95, 304
- importing list of resources, 61
- relative paths to, 54
- running resource discovery for, 44, 54, 56
- tags, troubleshooting, 292

HTTPS

- encryptions. *See* SSL
- SSO failing over, 304

I

Icons

- for rules, 160
- inheritance effect on, 133, 204
- inherited policies, 131, 223
- of Identities Tree, 29
- Policy Matrix, 132
- Select Auth, 87
- signing status, 248

Identities

- aliases
- assigning access policies for. *See* Access policies
- attributes, self-managing. *See* Self Administration
- authenticating, 160
- configuring personalization for, 94
- credentials for, 269
- credentials, troubleshooting, 297
- dynamic groups. *See* Dynamic groups
- failed logins, 151
- groups. *See* Groups
- ID for, 281
- ignoring, 224
- logging out, 161, 190
- management, delegation of, 208, 212
- passwords. *See* Passwords
- profile. *See* Profile
- providing custom response to, 161, 189
- redirecting to new page, 161, 191
- registering, 107
- segmentation of, 127
- self-managing. *See* Self Administration
- threshold value, setting, 83

Identities Tree

- affect of directory structure on, 28
- aliases, 68
- considerations, 27, 65
- definition of, 26
- directory server location, selecting, 39
- dynamic groups. *See* Dynamic groups
- folders. *See* Folders
- groups. *See* Groups
- icons of, 29
- Identity data location, adding. *See* Identity data location
- importing a certificate, 39
- Known Identities, 26, 28, 30
- levels of branches, 27
- object class structure of, 73
- organizing, 65
- overlapping DNs, 36
- overview of, 28
- profiles, adding, 40
- profiles. *See* Profiles
- refreshing, 42
- replicated directories, configuring, 36
- unknown identities, 26

- Identity data locations
 - adding, 29, 33
 - certificate for, importing, 39
 - configuring replicated directories, 36
 - configuring search order of, 33
 - directory server location, selecting, 39
 - global list of, 31, 33
 - Identities Tree. *See* Identities Tree
 - matching to resource data, 26
- Idle timeout, 23, 205, 270
- IDs
 - configuring components', 251, 267, 268
 - profile element, 41, 42, 148, 281
- Ignored
 - filenames, 257
 - identities, 224
 - URLs, 61
 - workflow condition, 224
- Importing
 - browser certificate, 22, 199, 277
 - directory certificate, 35
 - identity location certificate, 39
 - resource lists, 44, 61
- Inheritance
 - by dynamic groups, 73
 - determining parent entry of, 136
 - difference between policy and delegation, 213
 - disinheritance, preventing, 214
 - effect on scalability, 133
 - icons of, 131, 133, 204, 223
 - laws of, 133, 135, 137
 - of delegation privileges, 213
 - of multiple policies, 137
 - of Select Auth policy, 90
 - of workflow conditions, 224
 - overriding, 137
 - overview of, 133
 - priority of, 136
 - taking advantage of, 27
- Integrated Windows authentication
 - configuring, 99, 103, 104
 - introducing, 86
 - properties of, 104
 - sequence of events, 104
 - troubleshooting, 298
 - user authentication process, 99
- Invalid characters, 103, 163, 221, 273
- IP address. *See* Addresses
- ISAPI, 304
- ISO characters, 264

J

- Java security alert, 23
- JSP pages
 - for password reset, 154, 155
 - for registration, 107, 110
 - for Self Administration, 198, 199
 - for Web Administration, 276
 - for workflow change requests, 225

K

- Kerberos
 - configuring, 125
 - logins, 106, 127
 - passwords, changing, 105, 125, 149, 194
 - properties of, 126
 - user authentication process, 99
- Key file
 - locating, 247
 - losing, 248
 - sharing, 269
- Known Identities
 - definition, 26, 30
 - introduction, 28
 - overview, 30

L

- LDAP. *See* Directory servers
- Level, logging hierarchy, 237, 239
- Lexicographic searches. *See* Searching
- Lists
 - available attributes, 37
 - available decision points, 165
 - available Policy Validators, 261
 - available rules, 163
 - certificate revocation, 122
 - global identity locations, 33
 - global network plugins, 55
 - imported network resources, 61
 - of authentication services, 100
 - protected web sites, 257
 - revocation, 122
- Load balancing, 261, 269
- Lockout, profile, 151
- Log file, configuring, 235

Logins

- changing passwords during, 143
- Delegated Administration, 205
- enabling form-based, 264
- failed attempts, 151
- incorrect authentication setup of, 127
- Kerberos/NTLM, 106, 127
- password, 125
- RADIUS, 114, 116, 264
- Root Administration, 205
- SecurID, 118, 264
- to Administration server, 22, 278
- to directory server, 35

Logout identity, terminal points, 190

Looping queries, 296

M

Mail. *See* Email

Manifest

- detecting violations, 247
- valid entries in, 247

Matrix

- administration. *See* Administration Matrix
- Policy. *See* Policy Matrix

Membership

- to dynamic groups, 75
- to groups, 70, 71, 75

Messages, recording. *See* Audit

Modes

- Delegated Administration. *See* Delegated Administration
- overview of, 19
- Root. *See* Root Administration
- Web Administration. *See* Web Administration

N

Namespaces, 181

Netmask, 165

Network

- addresses, using in rules, 160, 165
- discovery, 208
- discovery, troubleshooting, 292
- management, delegating, 208, 211
- See also* Discovery, network

Node. *See* Decision points

Nonces, 269

Notification. *See* Alerts

NTLM

- authentication, 298
- logins, 106, 127
- overview of, 105
- passwords, changing, 105, 125, 149, 194
- properties of, 105, 106
- user authentication process, 99

O

Object classes, 73

- certificationAuthority, 120
- structure of, 73

OCSP

- checking, 123
- configuring, 122
- timeouts, 124, 296
- troubleshooting, 296, 301

Online Certificate Status Protocol. *See* OCSP

Operational attributes. *See* Attributes

Operators

- boolean, nesting filters with, 170, 176, 178, 287
- comparison, 80, 287, 288

Overrides

- changing, 253
- identifying, 253
- parameters for, 252

P

Passcodes, 99

Password authentication

- configuring, 124
- form used, 125
- logins, 125
- properties of, 124

Passwords

- answers that authenticate, 152
- case-insensitivity, 149
- changing, 142, 143, 144
- defining, 42, 281
- dictionary for, 145, 149
- disabling, 144, 152
- disallowing changes, 143
- enabling, 144
- Enforcer settings for, 145
- enforcing, 145
- expiry of, 34, 143, 144, 146
- failure of, 150
- forms for, 146, 151
- JSP pages for, 154
- managing, 143
- policies, configuring, 141, 142, 143, 144, 145, 146
- policies, delegating, 208
- resetting, 154
- self-managing, 142
- strength, configuring, 146, 147
- triggering workflow with, 153
- usage guidelines, 144

PDFs, troubleshooting, 298

PEM encoding, 179, 199

Personalization

- attributes, activating, 287
- configuring with Select Auth, 91
- definition of, 92
- enabling, 92, 93
- environment variables, 93, 94
- identity information in query, 270
- troubleshooting, 304
- with authentication decision point, 93
- with Citrix NFuse, 186
- with Select Auth, 93

Plugins

- authentication, 289, 290
- Citrix NFuse decision point, 186
- configuring, 289
- custom, 289
- decider, for Policy Validator, 289
- decision points for Rule Builder, 159, 289, 290
- discovery output formats, 55
- Enforcer. *See* Enforcer Plugins
- identity editors, delegation of, 208
- network discovery, 54, 56
- site data, 264
- uploading, 289

Policies

- access. *See* Access Policies
- authentication. *See* Authentication services
- authorization. *See* Access policies
- delegation. *See* Delegated Administration
- workflow. *See* Workflow

Policy

- data location of. *See* Policy Store
- setting, delegated mode, 19
- setting, full mode, 19

Policy Builder

- administration Delegated, 197
- administration, Root, 197
- cache warnings, configuring, 246
- configuring audit settings from, 231
- configuring browser preferences, 24
- configuring Select Access components with. *See* Components, configuring
- delegating administration resources, 208
- displaying in browser window, 20
- errors, 292
- how to use, 25
- icons, signing, 248
- interface elements, 15, 25
- logging in, 23, 278
- opening in own browser window, 24
- overview, 15
- plugins, built-in, 56
- plugins, uploading, 289
- refreshing data of, 42, 246
- running in Delegated Administration mode, 293
- running in Root Administration mode, 21
- setting up, 27
- shortcuts, 19, 23
- SSL security alert, 21, 277
- troubleshooting, 299
- URLs for, 20, 277
- viewing certificate, 22, 277

Policy Matrix

- administration functions. *See* Administration Matrix
- administration modes. *See* Modes
- axes of, 25
- data, representation of, 25, 27, 28, 29, 31, 35, 42, 43, 44, 45
- grid function, 26
- icons used, 132
- policies, setting, 130
- profiles. *See* Profiles
- refreshing, 42, 205, 207, 247
- Select Auth, using. *See* Select Auth
- setting up, 27

Policy store

- cache. *See* Cache
- configuring parameters in, 251
- data in, types of, 245
- publishing keys to, 269
- signing data, 246
- signing states, 248
- violations of, definition, 248
- violations. *See* Violations
- why important, 245

Policy Validator

- address, defining, 267
- audit settings for, 232, 268
- cache. *See* Cache
- communicating with Enforcer plugins, 263
- configuring, 251, 267
- cookies, 256, 269
- creating transient entries, 99
- credentials, 269
- decider plugins, 289
- deploying multiple Validators, 261
- idle timeout, 270
- impact of dynamic groups on, 73
- inability to authenticate identities, 87
- list of available, 261
- load balancing, 261
- logging, 239, 297
- maximum query size, 270
- nonces, 269
- password dictionary, 145
- query details, 264, 270
- registration, 294
- segmenting identities, 127
- sharing key, 269
- SOAP envelope, 181
- threads, configuring, 270
- troubleshooting, 294, 295, 296, 299, 301, 302
- tuning performance, 246, 269

Ports

- configuring, 48, 59, 116, 219
- Delegated Administration, 198
- output by plugin, 55
- ranges for, large, 47
- Root Administration, 197
- Self Administration, 198
- using in rules, 160, 174
- Web Administration, 198

Prefixes, 181

Profiles

- adding, 27, 29, 31, 40
- aliases, how used, 68
- attributes needed for, 287
- defining a password, 42, 281
- deleting, 42, 77
- disabling, 144
- fields available, 41
- finding, 71, 77, 78, 79, 80, 81
- hiding, 71, 75, 77, 82, 83
- ID property, 41, 42, 148, 281
- lockouts of, 151
- lookups, order of, 32
- modifying, 40
- moving, 28
- password reset data in, 153
- re-enabling, 151
- representation of on Policy Matrix, 28, 29, 31, 35, 42
- searching for, 71, 75
- self-managing. *See* Self Administration
- transient, creating, 99
- types of, 28, 29

Q

Queries

- copying user information into, 270
- details of, 264
- evaluating, 178
- looping, 296
- maximum size of, 270
- property tags used, 179
- SOAP envelope, 181
- troubleshooting, 296
- using attributes of in rules, 160, 176

Questions, secret, 155

Quick search, 78

R

RADIUS authentication, 86
 configuring, 114
 creation of transient profiles, 99
 database used by, 99
 enabling form-based login, 264
 forms used, 116
 logins, 114, 116
 properties of, 114
 sharing secrets with, 99
 user authentication process, 99

Redirecting, identities, 161, 191

Registering, Policy Validator, 294

Registration authentication
 configuring, 107
 form used, 106, 110, 127
 JSP pages for, 107
 overview, 107
 properties of, 107
 using, 86

Relative URL paths, 54

Replication
 adding a directory server, 36
 deleting a directory server, 36
 how to define identity locations with, 31

Resetting, passwords, 154

Resources Tree

 about, 43
 adding resources, 27, 43, 44, 52, 54
 adding services, 43, 44, 45, 48, 52
 administration of, 218
 building, 43, 44
 considerations, 27, 65
 definition of, 25
 discovery of resources. *See* Discovery, network
 elements of, 43
 entries, deleting, 62
 entries, finding, 71, 77, 78, 79, 80, 81
 entries, hiding, 71, 75, 77, 82, 83
 entries, organizing, 68
 entries, searching, 71, 75
 folders. *See* Folders
 guidelines for, 43
 hiding entries, 83
 imported list syntax, 61
 importing a resource list, 44, 52, 61, 62
 organizing, 65
 plugins, configuring, 59, 60
 refreshing, 42, 45, 207
 representation of resources, 43, 44, 45
 scanning. *See* Discovery, network
 threshold value, setting, 83
 URL limitations, 52
 what you can add, 43

Resources. *See* Resources Tree

Response, to identities, 161, 189

Revocation lists. *See* CRLs

Roles. *See* Dynamic groups

Root Administration
 logins, 23, 205
 overview, 19, 197
 port for, 197
 running in, 21

Root certificates, 121

Root context, 182

Rule Builder
 creating a new rule with, 161
 description pane, 157
 displaying, 157
 effect of cookies on, 157
 features of, 162
 interface elements of, 157
 overview of, 157
 rules, types of. *See* Rules

Rules

- administering, 130
- conditions defined with, 159
- considerations for, 161
- copying and pasting, 163
- creating, 132, 223
- decision points. *See* Decision points
- definition of, 157, 158
- deleting, 164
- how they work, 158
- icons of, 160
- inserting rules within rules, 160, 184
- lists of, 163
- modifying, 132, 163, 223
- naming, 103, 162, 163, 221
- printing, 164
- refreshing, 162
- saving, 164
- single-branch, definition, 161
- subrule decision point, using, 184
- terminal points. *See* Terminal points
- text version of, 157
- time of day decision point, using, 167

S

Scalability, increasing, 133

Scanning. *See* Discovery, network

sdconf.rec, locating, 117

Searching

- advanced searches, 80
- expressions, creating, 75, 182, 287, 288
- expressions, nesting of, 287
- expressions, rules of, 287
- for profiles, 71, 78, 80
- modifying searches, 81
- quick search, 78
- results, displaying, 82
- results, post-search, 81
- threshold values, 77
- wildcards available, 78, 79, 279

Secrets

- for RADIUS, 86
- questions, for password resets, 155

Secure Sockets Layer. *See* SSL

SecurID authentication, 86

- configuring, 117
- creation of transient profiles, 99
- database used by, 99
- enabling form-based login, 264
- error codes, configuring, 119
- form used, 118
- logins, 118
- multiple identity locations limitations, 117
- passcodes, 99
- properties of, 117
- properties of, advanced, 119
- Select Access compatibility with, 117
- user authentication process, 99
- X.509 certificates, using, 117

Select Access

- Administration server. *See*
 - Administration server
- authentication services. *See*
 - Authentication services
- data, identity. *See* Identity data location
- data, policy. *See* Policy Store
- different administration modes,
 - enabling, 199
- Enforcer plugins. *See* Enforcer plugins
- features requiring attributes, 287
- HTTP headers supported, 95
- overview, 15
- plugins. *See* Plugins
- Policy Builder. *See* Policy Builder
- Policy Validator. *See* Policy Validator
- Rule Builder. *See* Rule Builder
- SDK, elements of, 198
- Select Auth. *See* Select Auth
- test deployments, tips, 261
- using digital signatures with, 247

Select Audit, configuring, 235

Select Auth

- authenticating identities, 87
- authentication services for, 86, 90
- authentication services for. *See* Authentication services
- column in Policy Matrix, 87
- configuring personalization, 91
- definition of, 30
- disabling, 89
- enabling, 89
- enabling personalization. *See* Personalization
- how used, 30
- icons used with, 87
- inheriting, 88, 90
- limitations of, 87
- overview, 87
- properties of, 91
- using SecurID authentication with, 117

Self Administration

- accounts, 142
- configuring details of
- JSP pages for, 198
- overview
- password resets, 153
- passwords, 142
- port for, 198
- profile attributes available for, 142
- self management resource, 198
- self registration resource, 198

Services, discovery of. *See* Resources Tree

Setup Tool, configuring audit settings from, 231

Signatures, digital

- benefits of, 247
- definition, 311
- overview of, 247
- setting up, 247
- signing audit trails, 268
- signing data with, 247
- signing states, 248
- troubleshooting, 302

Signs. *See* Comparison operators

Single sign-on. *See* SSO

SMTP server, 219

SOAP, envelope for, 181

SSL

- certificates for, 21, 277
- encrypting directory and Policy Builder sessions, 35
- running Administration server over, 19
- running directory server over, 35
- running network discovery over, 54
- security alert for, 21, 22, 277
- troubleshooting, 296, 301
- verifying certificate for, 35

SSO

- limitations by web servers, 265
- multi-domain support for, 256, 257
- single domain support for, 256
- troubleshooting cookies, 295, 304

Standard error, configuring, 237

Sub-delegation. *See* Delegated Administration

Subnet mask, 49

Super administrators. *See* Root Administration

Synthetic identities. *See* Transient identities

System logging, configuring, 237

T

Telnet, accessing resources, 297

Templates, HTML forms, 106, 110, 116, 118, 125, 127, 128, 142, 145, 149, 152, 193, 194, 195, 297

Terminal points

- allow terminal point, 161, 195
- custom response terminal point, 161, 189
- definition, 160
- deny terminal point, 161, 195
- logout identity terminal point, 190
- logout user terminal point, 161
- profile self-management terminal point, 193
- redirect terminal point, 161, 191
- See also* Self Administration

Threads, configuring, 270

Threshold values

- searching entries, 77
- setting, 79, 83

Time

- expiry of passwords, 149
- idle, disabling accounts after, 144
- interval, retry Validators, 263
- limit, client idle, 270
- limit, Validator reply, 263
- of day, rule decision point, 160, 166, 167, 168
- RADIUS timeout, 116
- re-enabling accounts after, 151
- using in rules, 160, 167

Timeouts

- OCSP, 124, 296
- Policy Validator, 205

Tokens, 86, 99, 117

Transactions, recording. *See* Audit

Transient identities

- authenticating, 99
- creating, 98, 99
- folders for, 114, 117, 120

Transient identities, certificates for, 238

Troubleshooting

- attributes, 304
- browser errors, 304
- certificates, 296, 301, 302, 303
- CGI, 304
- denied access, to service, 299
- denied access, to web page, 299, 300
- digital signatures, 302
- directory servers, 300, 301
- Enforcer plugin, 298
- forms, 297
- HTTP basic authentication, 297
- HTTP headers, 304
- integrated Windows authentication, 298
- ISAPI, 304
- network discovery, 292
- network services, 299
- OCSP, 301
- PDFs, 298
- personalization, 304
- Policy Builder, 292, 293, 299
- Policy Validator, 294, 295, 296, 301, 302
- referrer headers, 304
- registration, 294
- roles, 304
- SSL, 296, 301
- SSO cookies, 295, 304
- URLs, 292
- virtual servers, 298
- web servers, 297

Trusted Servers authentication

- configuring, 113
- overview, 112

U

UID, adding to query attributes, 270

Unknown Identities

- access policies for, 130
- authenticating, 26, 87
- ignoring, 224
- using Select Auth. *See* Select Auth

URI, XPath namespace, 181

URLs

- creating resource list, 43
- ensuring correct format of, 61
- for Web Administration, 276
- invalid syntax used, 54
- output by plugin, 55
- relative, 54
- restrictions, 52
- syntax for resources, 61
- troubleshooting, 292
- used to display Policy Builder, 20, 277
- workflow change requests, 225

UTF-8, 264

V

Variables, environment. *See* Environment variables

Violations

- caused by lost key, 248
- definition, 248, 249
- detecting, 247
- disabling warnings of, 250
- policy data, 247
- validating, 248, 249

Virtual domains, 259

W

Warnings

- client settings, 271
- enabling, 246
- for cache, enabling, 246
- policy data violations, disabling, 250

- Web Administration
 - folders, managing, 285
 - group membership, 282, 283
 - groups, managing, 282
 - interface for, 198
 - interface used, 278
 - JSP pages for, 276
 - loading, 276
 - logging in, 278
 - management categories, 276
 - organizational units supported, 275
 - overview, 20
 - port for, 198
 - prerequisites, 275
 - profile, properties, 281
 - profiles, finding, 278
 - profiles, managing, 280
 - running in, 21
 - security of, 275
 - setting up, 276
- Web content. *See* Resources
- Web pages, avoiding caching of, 265
- Web servers, scanning. *See* Network discovery
- Web sites
 - caching pages, 265
 - character set used, 264
 - denied access to, 299, 300
 - plugin for site data, 264
 - protected, 257
 - troubleshooting, 297
 - virtual, 259, 298
- Wildcards, 165, 287
- Workflow
 - alert templates, configuring, 220
 - change requests, administering, 225
 - conditions, ignoring, 224
 - conditions, setting, 222
 - conditions, types of, 223
 - delegation of, 208, 224
 - email options, configuring, 218, 219
 - icons, 223
 - inheritance, 224
 - JSP pages for, 225
 - overview, 203, 217
 - password resets, 153
 - policies, multiple, 224
 - policy, inheriting, 224
 - rules, applying, 223
 - SMTP server, configuring, 219
 - unknown identities, ignoring, 224
 - workflow rules, 221

X

- X.509 certificates, 117, 179, 199
- XML
 - bootstrap configuration files, 261
 - namespaces, 181
 - policy data entries, 246
 - prefixes, 181
 - queries, details in, 270
 - query details in, 264
 - root context, 182
 - signing, troubleshooting, 302
- XPath
 - decision point, configuring, 180
 - expressions, writing, 182
 - searching SOAP envelope, 181