

# HP OpenView Select Access

For the Windows<sup>®</sup>, Linux<sup>®</sup>, Solaris<sup>®</sup>, and HP-UX<sup>®</sup> Operating Systems

Software Versions Tested Against: 6.0 Patch 1 and 6.1

---

Integration Paper for BEA WebLogic™ 8.1 Servers

## Legal Notices

### Warranty

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

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

### Restricted Rights Legend

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

Hewlett-Packard Company  
United States of America

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

### Copyright Notices

© Copyright 2004-2005 Hewlett-Packard Development Company, L.P.

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

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

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

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

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

### Trademark Notices

WebLogic Server is a US trademark of BEA Systems, Inc.

Java™ is a US trademark of Sun Microsystems, Inc.

HP-UX Release 10.20 and later and HP-UX Release 11.00 and later (in both 32 and 64-bit configurations) on all HP 9000 computers are Open Group UNIX 95 branded products.

Intel®, Pentium®, and Itanium® are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux® is a U.S. registered trademark of Linus Torvalds.

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

Unix® is a registered trademark of The Open Group.

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

## Support

Please visit the HP OpenView web site at:

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

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

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

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

HP OpenView online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valuable support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter discussions with other software customers
- Research and register for software training

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

To find more information about access levels, go to the following URL:

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

To register for an HP Passport ID, go to:

**<https://passport.hp.com/hpp2/newuser.do>**

## Support

Please visit the HP OpenView web site at:

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

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

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

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

HP OpenView online software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valuable support customer, you can benefit by using the support site to:

- Search for knowledge documents of interest
- Submit and track progress on support cases
- Manage a support contract
- Look up HP support contacts
- Review information about available services
- Enter discussions with other software customers
- Research and register for software training

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

To find more information about access levels, go to:

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

To register for an HP Passport ID, go to:

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



# Contents

<b>1</b>	<b>Understanding Your Select Access Integration</b>	<b>9</b>
	Understanding the Key Components of this Integration	9
	The Select Access WebLogic Enforcer Plugin's Architecture	10
	Supported Security Configuration Scenarios	12
<b>2</b>	<b>Integration Tasks</b>	<b>17</b>
	Getting the Required Files	18
	To install an Enforcer plugin	19
	To configure the plugin and create the XML bootstrap file	19
	Files You Need to Append	20
	To append Enforcer API JAR files to the classpath	20
	About the bea_enforcer.properties File	22
	To create the bea_enforcer.properties file	22
	Setting Select Access as WebLogic's Security Provider	24
	To set up Select Access as WebLogic's Security Providers	24
	Enabling SelectID Authentication	26
	Modifying WebLogic Server Startup Scripts	26
	To configure the WebLogic server to protect all resources	26
	Modifying Deployment Descriptors	27
	How Protocol Hierarchies Affect Resource Organization	30
	Constructing WebLogic Resource Hierarchies	32
	When to Use Default Security Providers	34
	Using Graphics on Login Pages	35
	To set up SSO	36
	To set up Perimeter authentication	38
	To modify your HTTP 401 error page	39
	To set up authentication via a proxy	39
	How it Works in Select Access' WebLogic Enforcer plugin	41
	To extract personalization data	41
	Configure Resources Required During Server Startup	47
	To determine resource denials	48
	Configure Security Policy and User Profiles in the WebLogic Administration Portal	48





---

# 1 Understanding Your Select Access Integration

Select Access is an integral part HP's comprehensive Identity Management suite. It delivers a full solution for complex access management across the enterprise. Select Access:

- Automates access control and user life-cycle management.
- Extends the enterprise through federation.
- Delegates management to business owners and the end users themselves.

Along with robust workflow, user self-service, reporting, and delegated administration capabilities, Select Access is the most comprehensive access control system available. Select Access simplifies your ability to secure user access to BEA WebLogic 8.1 Server™ resources.

## Assumptions in this Document

This document assumes the following:

- That you have BEA WebLogic 8.1 installed and running on your network.
- That you understand the features and functions of Select Access.
- That you have updated Select Access 6.0 with Engineering Patch 1B.
- That you have a working knowledge of Select Access and LDAP 3.0-compliant directory servers.

## Integrating the Select Access and WebLogic

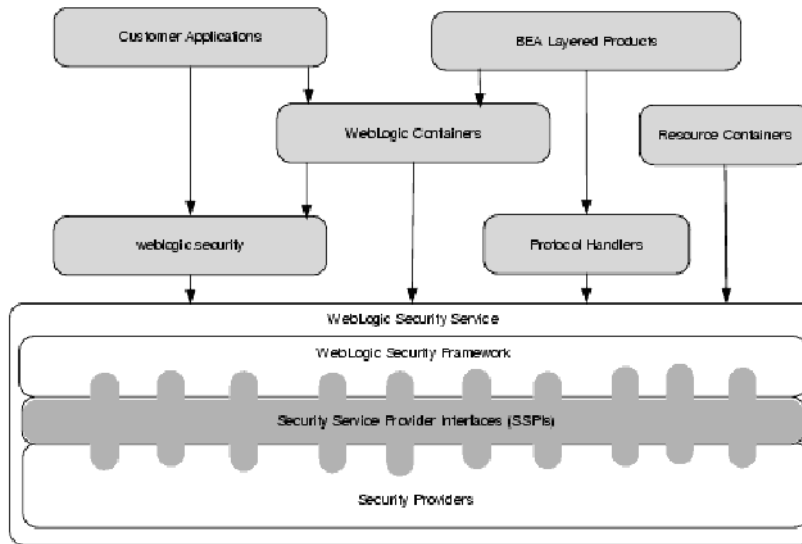
To understand the integration between Select Access and the WebLogic Server, you need to understand where critical integration points lie.

### Understanding the Key Components of this Integration

WebLogic's Security Service architecture consists of three major components:

- the WebLogic Security Framework
- the Security Service Provider Interfaces (SSPIs)
- the WebLogic Security Providers.

Select Access' WebLogic Enforcer plugin protects WebLogic Server resources by adding three Select Access Security Providers to WebLogic Server. In so doing, Select Access' WebLogic Enforcer plugin assigns all authentication and authorization responsibilities to the Policy Validator. [Figure 1](#) shows a high-level view of WebLogic Security Service Architecture.



**Figure 1 The WebLogic Security Service Architecture**

The WebLogic Enforcer plugin differs in structure from other Enforcer plugins available with Select Access: it is implemented via independent JAR files (`SASecurityProviders.jar` and `SAPrincipal.jar`), but it is also written using two APIs:

- WebLogic’s Security Service API: To create a pluggable security provider on the WebLogic server for the realm you designate.
- Select Access’ Enforcer API: To create security providers that delegate authentication and authorization to Select Access Policy Validator.

Because the implementation and deployment of Select Access’ WebLogic Enforcer plugin is unique to this integration, the method for configuring password authentication, Single Sign-On (SSO), and personalization differs from other Enforcer plugins. For details, see [Chapter 2, Integration Tasks](#).

## The Select Access WebLogic Enforcer Plugin’s Architecture

Select Access’ WebLogic Enforcer plugin includes three types of security providers. These three security providers act as the agent for Select Access on the WebLogic Server. The actual authentication and authorization is still done by a Policy Validator. Security providers use the Enforcer API to communicate with a Policy Validator and use WebLogic SSPIs to communicate with the WebLogic Security Framework. These providers are described below:

- Authentication Provider—Checks user’s credentials and populates the principal object to the WebLogic Server. For details, see [The Authentication Provider](#) on page 11.
- Identity Assertion Provider—Performs perimeter authentication based on Select Access tokens (known as nonces). For details, see [The Identity Assertion Provider](#) on page 12.
- Authorization Provider—Makes access decisions based on policy.

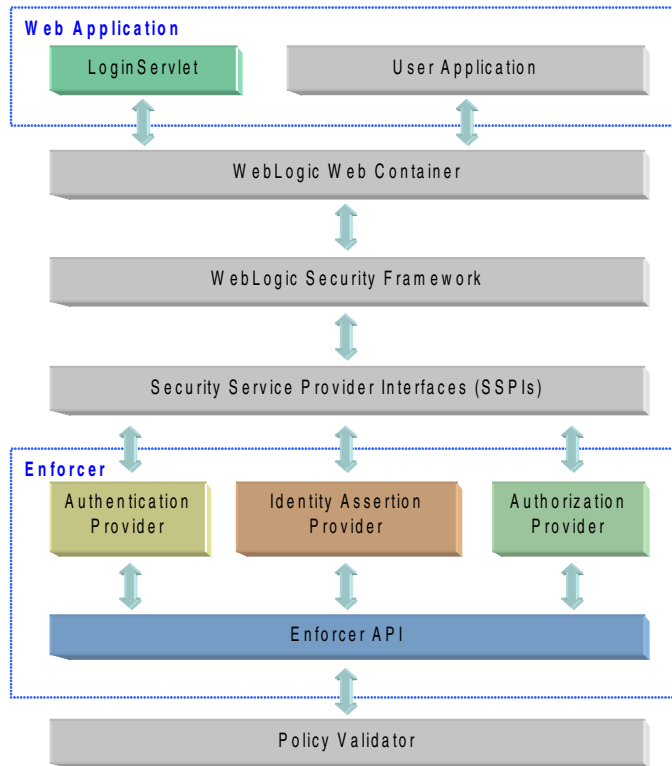
The plugin also includes a servlet:

- Login Servlet—Gathers user login information from either a:
  - login form
  - cookie

— URL

It then provides that information to Authentication Providers and Identity Assertion Providers. The Login Servlet is also used to do redirects for MD-SSO.

Figure 2 illustrates the high-level architecture of Select Access' WebLogic Enforcer plugin.



**Figure 2 Select Access' WebLogic Enforcer Plugin Architecture**

### The Authentication Provider

The Enforcer plugin's Authentication Provider component delegates the authentication to Policy Validator. It supports six types of authentication: Password, SecurID, RADIUS, certificate, NTLM and Kerberos. Depending on the type of client, the authentication implementation can vary:

- Fat-clients (standalone java clients)—Can use Password, SecurID, NTLM, and Kerberos authentication.
- Thin-clients (browser clients)—BEA WebLogic server supports HTTP Basic Authentication or Form-based Authentication to authenticate to the Select Access Authentication Provider. Only Form-based Authentication supports all of the Select Access Authentication methods (password, certificate, SecurID, Radius, NTLM, and Kerberos authentication). You can configure the authentication method to be used through the Web application's deployment descriptor configuration.

For details, see [Setting up Form-based Authentication with Multiple DNS Domain SSO](#) on page 36.

## The Identity Assertion Provider

The Identity Assertion Provider is the component that performs Perimeter Authentication by using a nonce—a unique token required by the Select Access system. Perimeter Authentication is the authentication method that allows users or system processes to assert their identity using tokens, and therefore, supports single sign-on (SSO). The Identity Assertion Provider can authenticate users by reading the token set by a different system protected by Select Access, and stored in the cookie.

## The Authorization Provider

The Authorization Provider is the component that delegates the authorization to the Policy Validator. The Policy Validator can control access to the following WebLogic Server resources:

- URL Resources (HTML, JSP, Servlet)
- EJB Resources
- JNDI Resources
- JDBC Resources
- JMS Resources
- Application Resources
- Server Resources
- Administration Resources
- Web Services Resources

## Supported Security Configuration Scenarios

Table 1 lists the security scenarios you can configure with Select Access' WebLogic Enforcer plugin. These options vary in the degree of difficulty required to set it up.

**Table 1 Supported Authentication Scenarios**

Type	Difficulty	Use this When	What is Required
HTTP Basic	Simple	<ul style="list-style-type: none"><li>• You do not need Select Access to control session timeouts. Choose another method if this is required.</li><li>• You want users signing in from a WebLogic Server to also log into other systems protected by Select Access in the same DNS domain.</li></ul> <p><i>Note:</i> The reverse is not possible</p>	<ul style="list-style-type: none"><li>• Configure Select Access's Authentication and Authorization Providers.</li><li>• No configuration for Web application required.</li></ul>

**Table 1 Supported Authentication Scenarios**

<b>Type</b>	<b>Difficulty</b>	<b>Use this When</b>	<b>What is Required</b>
Form	Moderate	<ul style="list-style-type: none"><li>• You want a custom login page for your applications.</li><li>• You want users signing in from a WebLogic Server to also log into other systems protected by Select Access in the same DNS domain.</li></ul> <p><b>Note:</b> The reverse is not possible</p>	<ul style="list-style-type: none"><li>• Configure Select Access's Authentication and Authorization Providers.</li><li>• Configure the Web application to use Form Authentication.<ul style="list-style-type: none"><li>— Create two pages: login and login error.</li><li>— Modify the application's deployment descriptor to indicate the FORM authentication method.</li></ul></li></ul> <p><b>Note:</b> You cannot globally configure all applications on the WebLogic Server.</p> <p>For details, see <a href="#">Setting up Form-based Authentication</a> on page 35.</p>

**Table 1 Supported Authentication Scenarios**

Type	Difficulty	Use this When	What is Required
Form with multiple DNS domain SSO <sup>a</sup>	Moderate	<ul style="list-style-type: none"><li>• You want a custom login page for your applications.</li><li>• You want users signing in from a WebLogic Server to also log into other systems protected by Select Access. The other systems can be in different DNS domains.</li><li>• You want users signing in from other systems protected by Select Access to also log into the WebLogic server. The other systems can be in different DNS domains.</li></ul>	<ul style="list-style-type: none"><li>• Configure all three Select Access Security Providers.</li><li>• Configure the Web application to use Form Authentication. This requires that you:<ul style="list-style-type: none"><li>— Modify the application's deployment descriptor to indicate the FORM authentication method.</li><li>— Configure Select Access's Login Servlet as the login page for the application.</li><li>— Configure authentication server and login form by using Select Access Policy Builder.</li></ul></li></ul> <p><b>Note:</b> You cannot globally configure all applications on the WebLogic Server.</p> <p>For details, see <a href="#">Setting up Form-based Authentication with Multiple DNS Domain SSO</a> on page 36.</p>

**Table 1 Supported Authentication Scenarios**

Type	Difficulty	Use this When	What is Required
Perimeter	Moderate	<ul style="list-style-type: none"> <li>You do not plan to let users log in from the WebLogic Server. For example, you have a dedicated login server and all users must log in from that server.</li> <li>You want users signing in from other systems protected by Select Access to also log into the WebLogic server. However, users cannot use Forms or HTTP Basic Authentication to log into the WebLogic server directly, due to a limitation of WebLogic Server's Web container.</li> <li>Do not require automatic redirects. When the session timeout token expires, the browser instead displays an unauthorized message to user. However, you can configure the WebLogic Server's unauthorized error page (401) to redirect user to your login server.</li> </ul>	<ul style="list-style-type: none"> <li>Configure all three Select Access Security Providers.</li> <li>Modify the application's deployment descriptor to indicate the CLIENT-CERT authentication method.</li> </ul> <p><b>Warning:</b> If you setup FORM or BASIC authentication in your Web application, WebLogic Server does not perform perimeter authentication—even if you configured Select Access's Identity Assertion Provider.</p> <p>For details, see <a href="#">Setting up Perimeter Authentication</a> on page 38.</p>
Proxy servers		<ul style="list-style-type: none"> <li>Want the proxy server to authenticate users.</li> <li>Want full protection of all the resources supported by Select Access' WebLogic Server Enforcer plugin-not only the URL resources protected by the proxy server.</li> </ul>	<ul style="list-style-type: none"> <li>Install and configure an appropriate Enforcer plugin on the proxy server.</li> <li>Configure all three Select Access Security Providers.</li> <li>Modify the application's deployment descriptor to indicate the CLIENT-CERT authentication method.</li> </ul> <p><b>Warning:</b> If you setup FORM or BASIC authentication in your Web application, WebLogic Server does not perform perimeter authentication—even if you configured Select Access's Identity Assertion Provider.</p> <p>For details, see <a href="#">Setting up Authentication Via a Proxy Server</a> on page 39.</p>

a. HP recommends this scenario.





## 2 Integration Tasks

To ensure Select Access and the WebLogic server function properly as a unit, you must follow a specific series of steps to integrate them correctly. [Table 2](#) summarizes the steps you need to perform, to configure and delegate all authentication and authorization responsibilities to Select Access.

- Due to requirements with Select Access' WebLogic Enforcer plugin, you must update your deployment of Select Access 6.0 with Engineer Patch 1B. Please make sure you have installed the patch before starting any integration tasks.
- You can still use WebLogic's native security mechanisms, however HP recommends that you do so to support WebLogic's internal functions only. See [When to Use Default Security Providers](#) on page 34 for details.

**Table 2 Integration Overview**

Integration Tasks	Details
1 Install Select Access' WebLogic Enforcer plugin files on the same host as the WebLogic server.	<a href="#">Deploying Select Access on a BEA WebLogic Host</a> on page 18
2 Define the classpath for Enforcer JAR files. The classes in these JAR files are used by the BEA WebLogic Server.	<a href="#">Defining Select Access Classpaths</a> on page 19
3 Create a properties file for the Enforcer plugin.	<a href="#">Storing WebLogic Connection Information</a> on page 21
4 Configure the BEA WebLogic Server to use Select Access as its Security Provider.	<a href="#">Making Select Access the WebLogic Security Provider</a> on page 24
5 Set default security constraints for WebLogic resources so that they are protected as they are added to the Policy Builder.	<a href="#">Setting Default Security Constraints for WebLogic Resources</a> on page 25

**Table 2 Integration Overview (cont'd)**

Integration Tasks	Details
6 Configure the Policy Matrix in the Policy Builder so it displays the correct combination of users, resources, and services.	<a href="#">Configuring Select Access to Protect WebLogic Resources</a> on page 28
7 Choose and configure your preferred authentication method.	<a href="#">Setting up Form-based Authentication</a> on page 35 OR <a href="#">Setting up Form-based Authentication with Multiple DNS Domain SSO</a> on page 36 OR <a href="#">Setting up Perimeter Authentication</a> on page 38 OR <a href="#">Setting up Authentication Via a Proxy Server</a> on page 39 OR <a href="#">Setting up Certificate Authentication</a> on page 40 OR <a href="#">Setting up Multiple Authentication Methods</a> on page 40
8 Set up personalization, if required.	<a href="#">Setting up Personalization</a> on page 40

## Deploying Select Access on a BEA WebLogic Host

You can install Select Access components across any combination of host computers. However, to ensure that your WebLogic server has the right components and files required to make Select Access its Security Provider, you need to install one Select Access Enforcer plugin on WebLogic's host machine.



This can be any of Select Access' Enforcer plugin. It is not, however, the Select Access WebLogic Enforcer plugin. You will be installing this plugin manually, later in this document. These WebLogic-specific files are not installed as part of Select Access 6.0.


### Getting the Required Files

At minimum, HP recommends you install and configure one of the Enforcer plugins available with the Select Access 6.0 installer on the WebLogic host. This ensures that the required Enforcer API files are installed locally. Upon completion, you need to create the

enforcer\_bea.xml bootstrap file. This file contains the configuration parameters that are required by the Enforcer API classes that are part of Select Access' WebLogic Enforcer plugin JAR files.

## To install an Enforcer plugin

- 1 Run the Select Access 6.0 installer.
- 2 Follow the instructions described in [Chapter 3, Installing Select Access](#), in the *HP OpenView Select Access 6.0 Installation Guide*.
- 3 When you have reached the **Choose HP OpenView Select Access Components** screen, click one of the following boxes to install all of the correct Enforcer API files:
  - Sun ONE (iPlanet) Enforcer plugin
  - IIS Enforcer plugin
  - Apache Enforcer plugin

 You do not need to have Web server software installed on WebLogic's host machine to install and configure an Enforcer plugin.
- 4 Click **Next** and finish the installation as required.

## To configure the plugin and create the XML bootstrap file

- 1 Run the Setup Tool as described in [Chapter 4, Configuring Select Access](#), in the *HP OpenView Select Access 6.0 Installation Guide*.
- 2 Click **Next** until you reach the **Generic Enforcer plugin** setup screen. This wizard creates the XML bootstrap file Select Access' WebLogic Enforcer plugin requires.
- 3 Click the **Browse** button and select the folder to where the XML file will be created.
- 4 Name and specify the path for the file you are about to generate. HP recommends that you save the file to the same folder as the Web Logic Domain. For example, <WL\_Domain\_path>/enforcer\_bea.xml. This file name must match the path file name you configure in your properties file. For details, see [About the bea\\_enforcer.properties File](#) on page 22.
- 5 Click the **Configure** button and configure the Enforcer plugin as required. For Select Access' WebLogic Enforcer plugin, a **Typical** configuration is suitable for most deployments. For details, see [Configuring the Enforcer Plugin](#) on page 129, in the *HP OpenView Select Access 6.0 Installation Guide*.
- 6 Click the **Finish** button to exit the setup wizard and commit the configuration to the XML file.

## Defining Select Access Classpaths

Because the WebLogic server uses the Enforcer API classes in Select Access' WebLogic Enforcer plugin JAR files, you need to append the required Select Access files to the CLASSPATH of WebLogic Server.

Typically, you define CLASSPATHs in the WebLogic server's startup script. By default the name of startup script is `startWebLogic.cmd`, which is stored in the WebLogic Server Domain directory.

## Files You Need to Append

You need to append the following JAR files to the CLASSPATH section of the WebLogic server's startup script:

- `SAPrincipal.jar`: Contains the `SAPrincipalImpl` class that extends the `WLSUser` interface. It allows WebLogic to use its default security providers with Select Access' Enforcer plugin in the same security realm. The `SAPrincipalImpl` class accomplishes this by representing Select Access users as native users in the WebLogic system.
- `EnforcerAPI.jar`: Contains all the classes used to create an Enforcer plugin.

### To append Enforcer API JAR files to the classpath

- 1 Create a new folder for holding all the JAR files Select Access' WebLogic Enforcer plugin requires:

`<WebLogic_install_path>/server/lib/sa`

- 2 Copy the JAR files listed in [Table 3](#) into the folder you just created.

**Table 3 Files You Need**

Filename	Where to Get it
<code>EnforcerAPI.jar</code> <code>jakarta-oro-2_0.jar</code> <code>mail.jar</code> <code>SAPrincipal.jar</code>	<code>&lt;SA_install_path&gt;/shared</code>
<code>shared.jar</code> <code>xml.jar</code> <code>castor-0.9.3.19-xml.jar</code> <code>msgsresources.jar</code> <code>bcprov-jdk14-125.jar</code> <code>protomatter.jar</code> <code>jdom.jar</code> <code>ldapjdk.jar</code> <code>xercesImpl.jar</code> <code>xml-apis.jar</code>	<code>&lt;SA_install_path&gt;/shared/jetty/policy_builder/protected</code>
<code>jce1_2_2.jar<sup>a</sup></code> <code>local_policy.jar<sup>a</sup></code> <code>US_export_policy.jar<sup>a</sup></code>	<ol style="list-style-type: none"> <li>1 Download and extract the Java Cryptography Extension (JCE) 1.2.2 file (<code>jce-1_2_2.zip</code>) from <a href="http://java.sun.com">java.sun.com</a>.</li> <li>2 Browse to the <code>jce1.2.2\lib</code> folder.</li> </ol>

- a. Only required for JRE 1.3. HP recommends you use JRE 1.4.

- 3 Open your startup script for the WebLogic server. By default the name of startup script is `startWebLogic.cmd`, which is stored in the domain directory you configured with the WebLogic Configuration Wizard.
- 4 Create an `SA_LIB` that points to the Select Access folder you created in [step 1](#). Using the example provided in that step, the variable added to the startup script is:

```
set SA_LIB=C:\bea\weblogic81\server\lib\sa
```

- 5 Create an `SA_CLASSPATH` variable that includes all the JAR files listed in [Table 3](#). This defines the correct classpaths to the required Select Access JAR files described in [Table 3](#). Without these paths, the WebLogic server would not know where to find the files for the Enforcer plugin. [Sample of the SA\\_CLASSPATH Variable](#) shows the contents of this new variable.

➤ If you want to condense the path, use the `SA_LIB` variable you created in [step 4](#).

➤ Depending on your platform, the separators you should use will vary: on Unix, use a colon (:), on Windows, use a semicolon (;).

- 6 Locate the `CLASSPATH` variable and append `SA_CLASSPATH` variable as another value for the `CLASSPATH` variable. For example:

```
set CLASSPATH=%CLASSPATH%;%SA_CLASSPATH%
```

- 7 Save the changes to this file.

#### Sample of the SA\_CLASSPATH Variable

The following is a sample of the `SA_CLASSPATH` variable:

```
set SA_LIB=/opt/bea/weblogic81/server/lib/sa
SA_CLASSPATH=${SA_LIB}:${SA_LIB}/bcprov-jdk14-125.jar:
${SA_LIB}/SAPrincipal.jar:${SA_LIB}/castor-0.9.3.19-xml.jar:
${SA_LIB}/EnforcerAPI.jar:${SA_LIB}/jdom.jar:
${SA_LIB}/ldapjdk.jar:${SA_LIB}/protomatter.jar :
${SA_LIB}/msgsresources.jar:${SA_LIB}/shared.jar:${SA_LIB}/xercesImpl.jar:
${SA_LIB}/xml.jar:${SA_LIB}/jakarta-oro-2_0.jar:${SA_LIB}/mail.jar:
${SA_LIB}/xml-apis.jar:${SA_LIB}/US_export_policy.jar:
${SA_LIB}/jce1_2_2.jar:${SA_LIB}/local_policy.jar
CLASSPATH=${CLASSPATH}${SA_CLASSPATH}
```

## Storing WebLogic Connection Information

In order for the Enforcer plugin to send valid queries to the Policy Validator for WebLogic resources, it must know the service name and root resource path defined for the protected WebLogic server. The Enforcer plugin reads this information from a configuration file called `bea_enforcer.properties`.

## About the `bea_enforcer.properties` File

This file is not native to Select Access nor to the WebLogic server. In order to use Select Access with WebLogic, you must create this configuration file and save it to the domain directory you configured with the WebLogic Configuration Wizard.



The service name you define as a parameter in this file must exactly match the host name and port that you configured for your WebLogic services. You will eventually add these services to the Policy Matrix. See [Configuring Select Access to Protect WebLogic Resources](#) on page 28 for information about adding WebLogic services with the Policy Builder.

### To create the `bea_enforcer.properties` file

- 1 In a text editor create a new file.
- 2 Add the parameters listed in [Table 4](#) to the file.
- 3 Save the file. When you are finished, your properties file should look similar to the one shown in [Sample `bea\_enforcer.properties` file](#).

**Table 4 Properties You Need to Add**

Property Name	Description
<code>EnforcerAPIConfigFile</code>	This file name must match the file name you defined for your XML configuration file. For details, see <a href="#">To configure the plugin and create the XML bootstrap file</a> on page 19.
<code>Service</code>	Identifies where the WebLogic server is located using the host name for the computer on which the WebLogic server is located and the a port number. This parameter uses the following syntax: <code>Service=&lt;hostname&gt;:&lt;port&gt;</code>

**Table 4 Properties You Need to Add (cont'd)**

Property Name	Description
Resource	<p>Identifies the root directory that all queries to the Policy Validator start with. This parameter uses the following syntax:</p> <p>Resource="&lt;root_path&gt;"</p> <p><b>Note:</b> Typical deployments often use a value of "/" as the root path.</p>
LogLevel	<p>Because audit configuration has not been enabled for this implementation of Select Access' WebLogic Enforcer plugin, you may want to include this parameter if you want to collect log messages generated by the Enforcer plugin. HP recommends you include this property to minimize output to platform-specific locations. You can choose any of the following values, listed in order of severity:</p> <ul style="list-style-type: none"> <li>• fatal</li> <li>• error</li> <li>• warning (the default setting)</li> <li>• info</li> <li>• debug</li> </ul> <p>These values correspond to Enforcer plugin options you can configure with Select Access's Setup Tool. All log messages are forwarded to the location you defined in the Enforcer plugin's configuration file. For details on these values see <a href="#">Configuring Enforcer-Specific Audit Settings</a> on page 146 in the <i>HP OpenView Select Access 6.0 Installation Guide</i>.</p>
SecurityRealm	<p>The security realm used by Perimeter Authentication. Set it to the Select Access's Security Realm.</p>

[Sample bea\\_enforcer.properties file](#)

The following is a sample of the `enforcer.properties` file:

```

EnforcerAPIConfigFile=enforcer_bea.xml
Service=myBEAas:7001
Resource=/
LogLevel=info
SecurityRealm=SARealm

```

## Making Select Access the WebLogic Security Provider

A critical integration step is to make Select Access the Security Provider for the WebLogic server. This step ensures that Select Access components—not WebLogic’s native mechanisms—protect the application server and its available resources. Setting up Select Access as the Security Provider requires that you follow the steps described in [Table 5](#).

**Table 5 Making Select Access the Security Provider**

Setup Task	Configuration Details
<p><b>Step 1:</b> Copy the Java archive file that contains the Security Providers to the required location on the WebLogic server host computer.</p>	<ol style="list-style-type: none"> <li>1 Stop the WebLogic server.</li> <li>2 Copy <code>SASecurityProviders.jar</code> that you downloaded from the HP OpenView Select Access support site.</li> <li>3 Move it to the following folder: <code>&lt;WebLogic_install_path&gt;/server/lib/mbeatypes</code></li> <li>4 Restart the server.</li> </ol>
<p><b>Step 2:</b> Set up the WebLogic server to use Select Access as its Security Provider.</p> <p><b>Note:</b> For specific procedural details for any of the tasks listed for this step, refer to the WebLogic server’s documentation.</p>	<ol style="list-style-type: none"> <li>1 Open the WebLogic Server Console in a Web browser of your choice.</li> <li>2 Create and configure a new security realm for Select Access by using default settings provided in the <b>Create a new Realm</b> page. The only unique property you want to manually configure is the realm name: for example <code>SArealm</code>.</li> <li>3 Click the realm you created in step <a href="#">step 2</a>, and create and configure its Security Providers. You must set up these according to HP’s recommendations. For details, see <a href="#">Setting Select Access as WebLogic’s Security Provider</a> on page 24.</li> <li>4 Because you can have multiple security realms in a WebLogic Server domain, but only one set as the default (active) realm, ensure the Select Access realm you created in step <a href="#">step 2</a> is the default security realm of your domain.</li> </ol>
<p><b>Step 3:</b> Restart the WebLogic server.</p>	<p>WebLogic server’s documentation</p>

### Setting Select Access as WebLogic’s Security Provider

You must define Select Access as the WebLogic server’s Security Provider. You can still use other security providers, but they should only support WebLogic’s internal functions.

#### To set up Select Access as WebLogic’s Security Providers

- 1 In the `<realm_name>` page for the realm you created in step 2 of [Table 5](#), click the **Providers** tab.



- 2 In the **Adjudicators** tab, create and configure a `Default Adjudicator`. Use defaults provided by WebLogic, except in the **Details** tab: ensure that you uncheck the **Require Unanimous Permit** box.
- 3 In the **Auditors** tab, optionally create and configure a `Default Auditor`. Choose the desired severity, according to your security requirements.
- 4 In the **Authentication** tab, create and configure the following `Authentication Providers` in the order outlined in [Table 6](#).

**Table 6 Required order of Authentication Providers**

Provider Name	Required?	Configuration Details
1 <code>SAAuthenticator</code>	yes	In the <b>General</b> tab, set the <b>Control Flag</b> set to <code>OPTIONAL</code> .
2 <code>Default Authenticator</code>	yes	In the <b>General</b> tab, set the <b>Control Flag</b> set to <code>OPTIONAL</code> .
3 <code>SAIdentity Asserter<sup>a</sup></code>	for Perimeter Authentication only	In the <b>General</b> tab, make <code>PolicyUser</code> an active token by moving it from the <b>Available</b> column to the <b>Chosen</b> column.  In the <b>Details</b> tab, uncheck the <b>Base64Decoding Required</b> option.
4 <code>DefaultIdentity Asserter<sup>a</sup></code>	for Perimeter Authentication only	In the <b>General</b> tab, make <code>AuthenticatedUser</code> an active token by moving it from the <b>Available</b> column to the <b>Chosen</b> column.

a. Required for form-based authentication with SSO, perimeter authentication, and authentication via proxy only.

- 5 In the **Authorizers** tab, create and configure `SAAuthorizer` and `Default Authorizer`, by using WebLogic's default values.
- 6 In the **Credential Mappers** tab, create and configure a `Default Credential Mapper`, by using WebLogic's default values.
- 7 In the **Role Mappers** tab, create and configure a `Default Role Mapper`, by using WebLogic's default values.

## Setting Default Security Constraints for WebLogic Resources

Due to the design of the J2EE architecture, WebLogic resources cannot use `SelectID` for authentication by default. While you can still enable `SelectID` in the Policy Builder for each resource, the authentication mechanisms will have no effect. This restriction exists because security for each J2EE resource is controlled by a deployment descriptor XML file that is resource-specific. However, this descriptor file does not initially include default security constraints.

## Enabling SelectID Authentication

To enable SelectID authentication, you must manually set these security constraints for each resource, before adding the resource in question to the Policy Builder's Resource Tree. Set security constraints for WebLogic resources such that they are protected by default as you add them to the Policy Builder. There are two methods you can use:

- WebLogic server startup scripts. HP recommends you use this method. For details, see [Modifying WebLogic Server Startup Scripts](#) on page 26.
- Deployment descriptors for each resource. For details, see [Modifying Deployment Descriptors](#) on page 27.

## Modifying WebLogic Server Startup Scripts

This method allows you to configure the WebLogic server to protect all WebLogic resources by default. Of the two methods available to you, this method is more secure than the modification of deployment descriptors. In this case, Select Access passes a flag to the WebLogic server upon the application server's startup. This flag forces it to protect all resources—irrespective of any security constraint information specified in the deployment descriptors.



Users can be transferred from the WebLogic internal user store to an LDAP directory using the Migrate functionality in the WebLogic Admin console.

### To configure the WebLogic server to protect all resources

- 1 Open the `<WLDomain_path>/startWebLogic.cmd` file.
- 2 Do one of the following:
  - If you have a `JAVA_OPTIONS` variable—append the following parameter to the end of it:  

```
-Dweblogic.security.fullyDelegateAuthorization=true
```
  - If you do not have a `JAVA_OPTIONS` variable—create this variable and set the required parameter for it:  

```
set JAVA_OPTIONS=  
-Dweblogic.security.fullyDelegateAuthorization=true
```
- 3 Ensure the `JAVA_OPTIONS` variable appears in the line that starts WebLogic Server. This line is automatically included if you used the Configuration Wizard to setup WebLogic. Otherwise, if you have manually created your file, you may need to append this line.  
[Sample Startup Line](#) shows this variable in bold. All other variables vary depending on your deployment of WebLogic.
- 4 Save the file and restart your server. By default, all WebLogic resources are protected by Select Access with these changes.



You must set the corresponding access policy for each user in the Policy Builder. See [Configuring Select Access to Protect WebLogic Resources](#) on page 28 for details.

## Sample Startup Line

The example below shows how to use the `JAVA_OPTIONS` variable in the startup line:

```
%JAVA_HOME%\bin\java %JAVA_VM% %MEM_ARGS% %JAVA_OPTIONS%  
-Dweblogic.Name=%SERVER_NAME% -Dweblogic.management.username=%WLS_USER%  
-Dweblogic.management.password=%WLS_PW%  
-Dweblogic.ProductionModeEnabled=%PRODUCTION_MODE%  
-Djava.security.policy="%WL_HOME%\server\lib\weblogic.policy" weblogic.Server
```

## Modifying Deployment Descriptors

Deployment descriptors are XML documents which define how a resource is used. By adding a security constraint to the deployment descriptor of a resource, you can control how the resource is accessed.



The deployment descriptors must be modified with security information as defined in the J2EE specification. HP does not recommend this option as it is less secure than the method described in the previous section. Therefore, modifying deployment descriptors is beyond the scope of this document.

# Configuring Select Access to Protect WebLogic Resources

This integration currently cannot support network discoveries on a WebLogic server. Until this feature is fully implemented, you need to manually build the Resources Tree in the Policy Builder. [Table 7](#) describes the steps required to protect WebLogic resources.

**Table 7 Configuring Select Access**

Step	Configuration Details
<p><b>Step 1:</b> Manually add the service you want to protect using Select Access.</p>	<ol style="list-style-type: none"> <li>1 Right-click a folder or the root of the Resources Tree.</li> <li>2 Click <b>New</b>→<b>Service</b>. The <b>New Service</b> dialog box appears.</li> <li>3 Name the resources and configure the service depending on whether or not the service is specific to a single server. For details see either: <ul style="list-style-type: none"> <li>• <a href="#">Entering Information for a Non-Server-Specific Resource Service</a> on page 43 in the <i>HP OpenView Select Access 6.1 Policy Builder Guide</i>.</li> <li>• <a href="#">Entering Information for a Server-Specific Network Resource Service</a> on page 43 in the <i>HP OpenView Select Access 6.1 Policy Builder Guide</i>.</li> </ul> <p><b>Note:</b> The host name and port number you specify must exactly match the host name and port number configured in the <code>bea_enforcer.properties</code> file. For more information on this file, see <a href="#">To create the bea_enforcer.properties file</a> on page 22.</p> <p><b>Note:</b> Setup the proper protocol for the service according to the resource type you want to protect. You may need to setup mutiple service nodes as each has a different protocol. A service node with protocol “WebLogic” is mandatory, because that service node will be used for authentication. For a complete protocol list please refer to <a href="#">Table 8 Resource Hierarchies</a> on page 32.</p> </li> <li>4 Click <b>OK</b>.</li> </ol>
<p><b>Step 2:</b> Add the WebLogic resources you would like protected below the service entry you created in step 1.</p> <p><b>Caution:</b> Before adding resources, first consider the resource structure of the WebLogic system—the resource architecture varies depending on the protocol deployed. Each resource type has a hierarchy. For more details, see <a href="#">How Protocol Hierarchies Affect Resource Organization</a> on page 30.</p>	<ol style="list-style-type: none"> <li>1 Right-click the WebLogic service you just created</li> <li>2 Click <b>New</b>→<b>Resource</b>. The <b>New Resource</b> dialog box appears.</li> <li>3 Name the resource.</li> <li>4 Click <b>OK</b>.</li> </ol> <p>For details, see <a href="#">To create a new network resource or edit an existing one</a> on page 49 in the <i>HP OpenView Select Access 6.1 Policy Builder Guide</i>.</p>

**Table 7 Configuring Select Access (cont'd)**

Step	Configuration Details
<p><b>Step 3:</b> Enable SelectID and choose an Authentication Server for the service you created in Step 1. Select Access' WebLogic Enforcer plugin supports six types of authentication servers:</p> <ul style="list-style-type: none"> <li>• password</li> <li>• SecurID</li> <li>• RADIUS</li> <li>• NTLM</li> <li>• Kerberos</li> <li>• Certificate</li> </ul> <p><b>Note:</b> You must enable Select Auth for ALL the service you created and make sure they are all configured to use the same authentication servers.</p>	<ol style="list-style-type: none"> <li>1 On the SelectID column, enable SelectID in the corresponding cell for the service. The <b>Authentication Properties</b> dialog box appears. For details on SelectID, see <a href="#">Setting a Select Auth Policy</a> on page 82 in the <i>HP OpenView Select Access 6.1 Policy Builder Guide</i>.</li> <li>2 Click the <b>Authentication</b> tab and do the following:               <ol style="list-style-type: none"> <li>a If you have not already configured an authentication server, click <b>Add</b>. The <b>Available Authentication Servers</b> dialog box appears allowing you to configure the server as required. For details on authentication servers, see Chapter 7, <i>Setting up authentication servers</i>, in the <i>HP OpenView Select Access 6.1 Policy Builder Guide</i>.</li> <li>b If you have already configured an authentication server, select one or more server names from the list of <b>Available Servers</b> and click <b>Add</b>. The server names appear in the <b>Selected Servers</b> window. To reorder the servers, select a server in the <b>Selected Servers</b> list and click the up arrow or down arrow buttons.</li> <li>c Click <b>OK</b>.</li> </ol> </li> </ol>
	<ol style="list-style-type: none"> <li>3 <b>Optional.</b> To supply a meaningful user name to the WebLogic Server and your applications, you need to configure an LDAP attribute from a user's entry that Select Access sets as the user name. Select Access also uses this attribute to set the result of <code>HttpServletRequest.getRemoteUser()</code> method. To define an attribute that will act as a meaningful user name:               <ol style="list-style-type: none"> <li>a Click the <b>Personalization</b> tab</li> <li>b Create a new environment variable, <code>UID</code></li> <li>c Choose an LDAP attribute from the dropdown list. For example, <code>uid</code> or <code>userid</code>.</li> </ol> <p>This procedure should be performed on the service node which has 'weblogic' protocol.</p> <p>If you choose not to define a custom user name, Select Access will use the user's DN as user name by default.</p> </li> <li>4 Configure the rest of personalization data as your specific deployment requires. Make sure you configure the personalization data on the proper resource tree, according to your resource type. For details on enabling personalization, see <a href="#">Chapter 5, Authentication Basics: Select Auth &amp; Personalization</a>, in the <i>HP OpenView Select Access 6.1 Policy Builder Guide</i>. For details on specific issues with the Select Access   WebLogic integration, see <a href="#">Setting up Personalization</a> on page 40.</li> </ol>

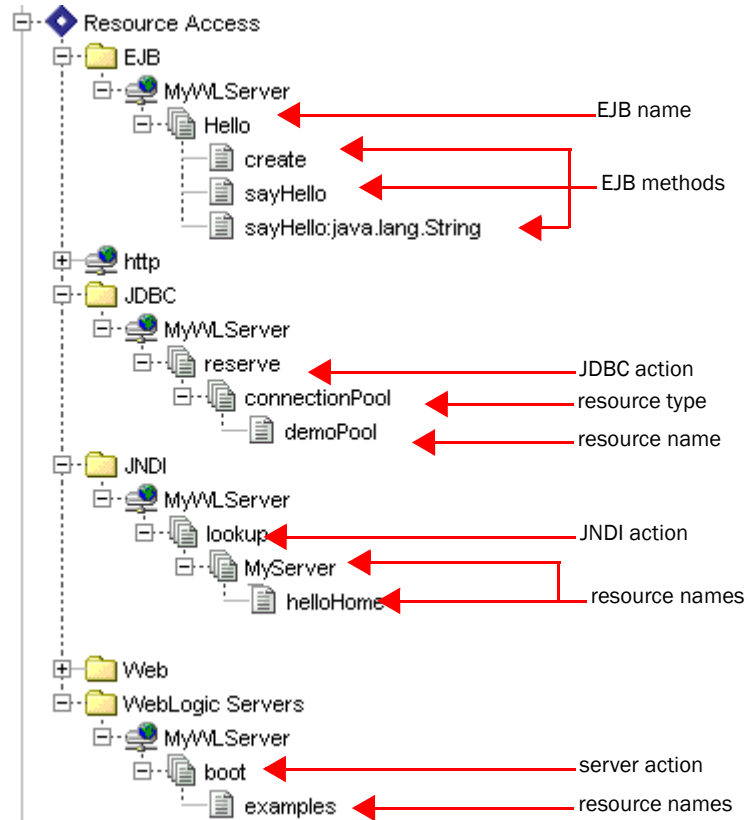
**Table 7 Configuring Select Access (cont'd)**

<b>Step</b>	<b>Configuration Details</b>
<p><b>Step 4:</b> Assign access policies to your users and WebLogic resource combinations. Select Access can handle all authorization requirements you have, when you use any combination of allow/deny/conditional policies.</p> <p><b>Note:</b> There is one exception. For details, see <a href="#">When to Use Default Security Providers</a> on page 34.</p>	<p>For details, see <a href="#">Chapter 7, Controlling Network Access</a>, and <a href="#">Chapter 8, Creating Conditional Access Rules with the Rule Builder</a>, in the <i>HP OpenView Select Access 6.1 Policy Builder Guide</i>.</p>

## How Protocol Hierarchies Affect Resource Organization

In order to add a sub-resource to an existing resource, you must understand how the resource hierarchy is constructed for each protocol. Without knowing the protocol, you cannot add a valid sub-resource. Therefore, unless you give some forethought to how you intend to organize your resources in the Resources Tree, your ability to see what protocol a resource uses limited to displaying its properties.

To easily identify which protocol a resource uses, HP recommends that you group resources of a similar protocol into well-organized folders. Figure 3 illustrates how WebLogic resources might be organized in the Resources Tree.



**Figure 3 WebLogic resources in the Policy Matrix**

For a description of each available protocol in the WebLogic server, see [Constructing WebLogic Resource Hierarchies](#) on page 32 for a detailed description of each protocol.

## Constructing WebLogic Resource Hierarchies

Because of the variety of protocols used, resource hierarchies for WebLogic resources are constructed in a variety of different ways. [Table 8](#) outlines how WebLogic resource hierarchies for each different protocol must be constructed.

**Table 8 Resource Hierarchies**

Resource type	Protocol	Resource Hierarchy	Description
URL	HTTP	context path	Web Application's context path. <i>Note:</i> For HTTPS resources use HTTP as the protocol, the WebLogic enforcer plugin does not distinguish HTTP and HTTPS resources.
		resource_name1 resource_name2 ... resource_nameX	Each sub-resource is a step deeper into the directory hierarchy of the host machine, which may terminate at a specific file.
EJB	EJB	ejb_name	The name of the EJB resource, as defined in the <ejb-name> tag in the resource's deployment descriptor.
		method_name:param1: param2	The name of the EJB method. You can append optional parameters by separating them with a colon.
JNDI	JNDI	jndi_action	An action (lookup, modify, or list) performed on an external directory.
		resource_name1 resource_name2 ... resource_nameX	Each sub-resource is a step deeper into the directory hierarchy of the host machine, which may terminate at a specific resource.
JDBC	JDBC	jdbc_action	An action (reserve, admin, shrink, restore) performed on a database.
		resource_type	The type of persistent connection.
		resource_name	The name of the connection.



**Table 8 Resource Hierarchies (cont'd)**

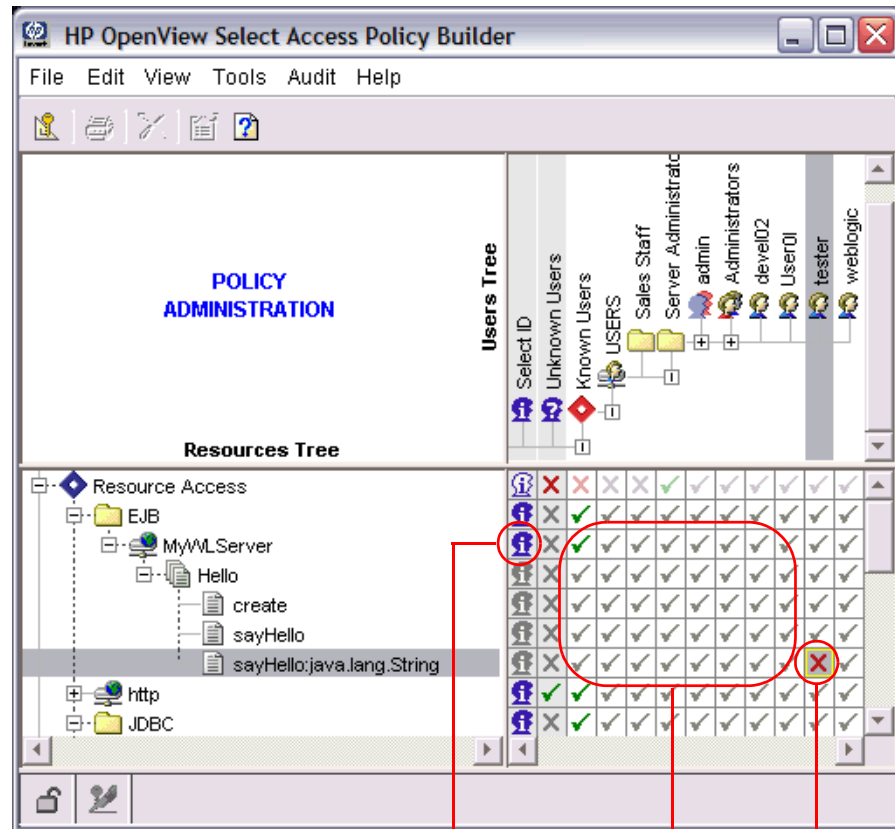
Resource type	Protocol	Resource Hierarchy	Description
JMS	JMS	.jms_action	An action performed on a message. You can protect the send and receive functions.
		destination_type	The destination type (queue or topic) the message is being sent to or from.
		resource_name	The name of the queue or topic.
Web Service	webservice	context_path	The Web application's context path.
		web_service_name	The Web Service name.
		method_name{param1 :param2...}	The name of the Web Service method. You can append optional parameters in a brace, separated by a colon.
Application	WebLogic	application_name	The name of the application.
Server	WebLogic	server_action	An action (boot, shutdown, lock, unlock) performed on the WebLogic server.
		server_name	The name of the WebLogic server. <b>Note:</b> You must define a boot action for a WebLogic server and set the policy at the server_name level to define who can perform this action.
Administration	WebLogic	resource_name	The name of the administration resource.

### An Example EJB Hierarchy

In the example shown in Figure 4, an administrator adds an EJB resource named Hello, as well as three sub-resources (methods):

- create
- sayHello
- sayHello:java.lang.String

All users, once authenticated, can access the EJB Hello, as well as the methods create and sayHello. Note that the user named “Tester” does not have permission to use the EJB method sayHello with the parameter java.lang.String.



SelectID enabled and password authentication used. Unknown users are denied access until correct login credentials supplied.

Known users inherit access down the branch for the Hello resource.

“Tester” is allowed access to all EJB resources—except the EJB method & parameter.

**Figure 4 Example Policy Shown with EJB Entries**

## When to Use Default Security Providers

The WebLogic server uses an internal LDAP user source to authenticate users who try to:

- Access critical system tools.
- Invoke operations on critical system administration Management Beans (MBeans).

Consequently, the WebLogic server attempts to authenticate these users against its own data source—even after you integrate Select Access with it. To protect those resources, use the WebLogic server’s default security providers instead. This includes managing who can boot the server.

# Setting up Form-based Authentication

If you want to have your own custom login page instead of browser's login dialog box, you can setup form-base authentication.

To setup form-base authentication you define `auth-method` tag in you web application deployment descriptor (`web.xml`) file, and set its value to `FORM`. [Example Deployment Descriptor for Form-based Authentication](#) shows how to add this tag to your `web.xml` file.

## Example Deployment Descriptor for Form-based Authentication

An example deployment descriptor is illustrated in the example that follows:

```
<web-app>
...
  <login-config>
    <auth-method>FORM</auth-method>
    <realm-name>SAR realm</realm-name>
    <form-login-config>
      <form-login-page>/my_login.htm</form-login-page>
      <form-error-page>/my_fail_login.htm</form-error-page>
    </form-login-config></login-config>
  </login-config>
...
</web-app>
```

The `form-login-config` and `form-error-page` tags define the path and filename of your own login page and fail login page. For details on how to setup form-based authentication in your Web application, see *Chapter 2, Securing Web Applications*, in the *BEA WebLogic Server Programming WebLogic Security Guide*.



Login pages should typically not include any protected resources. Otherwise, users may not be redirected back to the original page after a successful login. For details, see [Using Graphics on Login Pages](#) on page 35.

## Using Graphics on Login Pages

If your login page has some image files in it, check that those image files are not protected by any Select Access access policies. You can use one of two methods:

- Setting up access in the Policy Builder: Set an Allow access policy for all images on the login page for all unknown users.
- Setting up Select Access' WebLogic Enforcer plugin to ignore all image files with the **Ignored Filenames** setup screen when creating your enforcer configuration XML file. Make sure you check the **Ignore GIF images** and the **Ignore JPEG images** boxes. For details, see [Chapter 8, Configuring the Enforcer Plugins](#) in the *HP OpenView Select Access 6.0 Installation Guide*.

# Setting up Form-based Authentication with Multiple DNS Domain SSO

Multi-Domain SSO allows you to access content that is protected by the same Select Access system even when they exist in different DNS domains. For example If your WebLogic Server is located on `server1.domain1.com`, and another Web server is located on `server2.domain2.com`, you can setup Single Sign-on between them. To setup form-based authentication with Multi-Domain SSO, you need to:

- Define the Select Access login servlet as your Web application's login page.
- Configure the Authentication Server (from the Policy Builder) to use either:
  - The login form template provided by HP.
  - Your own custom login page.

► Remember, your login pages should not include any protected resources. For details, see [Using Graphics on Login Pages](#) on page 35.

## To set up SSO

- 1 Configure each application to use form-based authentication with its `web.xml` file so it uses Select Access's login servlet as the login page.
  - a Open the deployment descriptor `web.xml` file in a text editor.
  - b Add and/or configure the tags to listed in [Table 9](#) to this file.
  - c Save the changes to this file.

**Table 9** `web.xml` Tags Required

Tag	Sub-tag	Description
servlet	servlet-name	Sets name to any string. This string must meet the application's requirements.
	servlet-class	Sets the class of the login servlet. The class must be fully-qualified.
	run-as	Sets the <code>role-name</code> to a WebLogic administrator (with the corresponding role) defined by the default Authentication Provider. The administration role allows Select Access's servlet to perform Perimeter Authentication. <b>Tip:</b> When you created Select Access's security realm, all default user, group, role and policies are added to it. This includes a default user that Select Access uses to boot the WebLogic server. You can use this name as the <code>run-as</code> role name.

**Table 9 web.xml Tags Required (cont'd)**

Tag	Sub-tag	Description
servlet-mapping	servlet-name	This string must: <ul style="list-style-type: none"> <li>• Meet the application's requirements.</li> <li>• Must match the <code>servlet-name</code> in the <code>servlet</code> tag.</li> </ul>
	url-pattern	Maps the servlet to a <code>url</code> string pattern. This string must meet the application's requirements.
login-config	auth-method	Sets the method of authentication. Define this method as <code>FORM</code> .
	realm-name	Sets a specific realm. If you do not supply a realm name, the default realm is used.
	form-login-config	Sets: <ul style="list-style-type: none"> <li>• <code>form-login-page</code> to the same URL pattern as in <code>servlet-mapping</code>.</li> <li>• <code>form-error-page</code> to the application's login error page. Leave the value of this tag empty; Select Access does not use this value.</li> </ul>

See [Example web.xml file](#) for an example of a completed `web.xml` file.

- 2 Configure an Authentication Server and corresponding login form in the Policy Builder. For details, see [Chapter 6, Setting Up Authentication Services](#) in the *HP OpenView Select Access 6.1 Policy Builder Guide*.
- 3 Run the Setup Tool and configure SSO on the Enforcer plugin for each third-party Web server and WebLogic server. For details on how to configure SSO for Enforcer plug-in, see [Chapter 8, Configuring the Enforcer plugins](#), in the *HP OpenView Select Access 6.0 Installation Guide*.

#### Example web.xml file

The following is a complete sample of a server configuration file.

```
<web-app>
  <!-- Define the Servlets within the Web Application -->
  <servlet>
    <servlet-name>LoginServlet</servlet-name>

    <servlet-class>com.hp.ov.selectaccess.solutions.weblogic.securityprovider.login.LoginServlet</servlet-class>
    <run-as>
      <role-name>weblogic</role-name>
    </run-as>
  </servlet>
  <servlet>
    <servlet-name>PersonalizationServlet</servlet-name>
```

```

        <servlet-class>PersonalizationServlet</servlet-class>
    </servlet>
    <!-- Define Servlet mappings to urls -->
    <servlet-mapping>
        <servlet-name>LoginServlet</servlet-name>
        <url-pattern>login.htm</url-pattern>
    </servlet-mapping>
    <servlet-mapping>
        <servlet-name>PersonalizationServlet</servlet-name>
        <url-pattern>PersonalizationServlet</url-pattern>
    </servlet-mapping>
    <login-config>
        <auth-method>FORM</auth-method>
        <realm-name>SAR realm</realm-name>
        <form-login-config>
            <form-login-page>/login.htm</form-login-page>
            <form-error-page></form-error-page>
        </form-login-config>
    </login-config>
</web-app>

```

## Setting up Perimeter Authentication

Perimeter authentication is best used when:

- You do not plan to let users log in from the WebLogic Server.
- Due to a limitation of WebLogic Server's Web container, users who have set up Perimeter Authentication cannot use Forms or HTTP Basic Authentication. Therefore you want users signing in from other systems protected by Select Access to also log into the WebLogic server.

By default, when sessions time out (that is, the token has expired), the WebLogic Server shows users the unauthorized error page (HTTP 401 error page). Note that Select Access' WebLogic Enforcer plugin cannot redirect a user to login server. Instead, you can setup your own 401 error page to replace WebLogic default one. For details, see [To modify your HTTP 401 error page](#) on page 39.

### To set up Perimeter authentication

- 1 Configure the Select Access Identity Assertion Provider as described in [Table 6](#).
- 2 Modify the Web application's deployment descriptor to set authentication method to CLIENT-CERT. Do this by:

- Adding an `auth-method` tag to your `web.xml` file.
- Set its value to `CLIENT-CERT`.

[Example web.xml file](#) shows how to add this tag to your `web.xml` file.

### Example web.xml file

The following sample shows how to add the `auth-method` tag.

```
<web-app>
...
  <login-config>
    <auth-method>CLIENT-CERT</auth-method>
    <realm-name>SAR realm</realm-name>
  </login-config>
...
</web-app>
```

### To modify your HTTP 401 error page

- 1 Create your own 401 error page and then do one of the following:
  - Add a link to the login server.
  - Have the page redirect the user directly to the login server.
- 2 Define custom error pages in the `error-page` tag of the Web application's deployment descriptor (`web.xml`).

For more information about setting up custom error page, see *Customizing HTTP Error Responses* in *Chapter 3, Configuring Web Application Components of Developing Web Applications for WebLogic Server*.

## Setting up Authentication Via a Proxy Server

This method is ideally suited to organizations that:

- Want the proxy server to authenticate users.
- Want full protection to all the resources support by Select Access' WebLogic Enforcer plugin—not only the URL resources protected by proxy server.

### To set up authentication via a proxy

- 1 Set up your WebLogic server to use a Web server as a proxy. For details, see BEA's *Using Web Server Plug-Ins with WebLogic Server* guide.
- 2 Install the corresponding Enforcer plugin on the Web Server proxy.
- 3 In the Policy Builder, set up your required authentication methods for the Web server proxy.
- 4 Install and configure Select Access' WebLogic Enforcer plugin as described in [Setting up Perimeter Authentication](#) on page 38.
- 5 In the Policy Builder, set access policies for all WebLogic resources for the WebLogic service entry. You do not need to set access policies for URL resources for the Web service that is your proxy—except if the URLs are for the static HTML pages on your Web server.

## Setting up Certificate Authentication

To use Certificate Authentication, set up your environment as described in [Setting up Form-based Authentication with Multiple DNS Domain SSO](#) on page 36. However, there are a few differences to take note of:

- You do not need to choose a login form; certificate-based authentication uses digital certificates and not forms.
- Before you can setup the Certificate Authentication Server in the Policy Builder, load the root certificate into the Select Access directory server. For details on how to configure a certificate authentication server, see [Certificate Authentication Service](#) on page 115 the *HP OpenView Select Access 6.1 Policy Builder Guide*.
- Set up your WebLogic Server to use two-way SSL and load the root certificate to WebLogic Server's trust keystore. For details see [Chapter 7, Configuring SSL](#) on page 7-1 in the *BEA WebLogic Server Managing WebLogic Security Release 8.1*.
- Based on your security requirements, you may *optionally* choose to store user certificates in the Select Access directory server. Only if you want to compare each user's certificate with the one stored in Select Access, then you *must*:
  - Upload the user's certificate to the corresponding user's LDAP entry,
  - Check the **Require certificates to be stored on the directory server** box in the **New Certificate Server** dialog box.

## Setting up Multiple Authentication Methods

You can setup multiple authentication methods by adding more than one authentication server to SelectID Properties dialog box. In addition to configuring multiple authentication methods, you also need to use a special login form, `multiauth_form.html`. This form contains multiple authentication fields that correspond the credential collection for specific authentication methods. All authentication form elements are supported by Select Access' WebLogic Enforcer Plugin—except the registration element.

If you use certificate authentication with other authentication methods, Select Access' WebLogic Enforcer Plugin tries certificate authentication first:

- If the user successfully authenticated via his/her certificate, then authentication is considered successful—the Enforcer plugin does not need to display the login form.
- If the user does not successfully authenticate, the Enforcer plugin displays the login form to let user login via other authentication methods.

## Setting up Personalization

Select Access' WebLogic Enforcer plugin supports personalization for JSPs, servlets, and EJBs. With information either obtained from the directory server, or provided in real-time by a registering user, the communications between the WebLogic server 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.



Unlike Select Access' web server-based Enforcer plugins, the WebLogic Enforcer plugin neither adds the prefix `HTTP_SA` to a personalization variable name, nor does it change the variable name to uppercase. The variable name is exactly the same as you defined in the Policy Builder.

For more details about personalization, see Chapter 6, *Authentication fundamentals: Select ID and personalization*, in the *HP OpenView Select Access 6.1 Policy Builder Guide*.

## How it Works in Select Access' WebLogic Enforcer plugin

Personalization data is stored as key/value pairs in the `SAP13n` object, which is part of the Select Access Principal object. WebLogic applications can use this data by giving the corresponding key name to the `SAP13n` object.

### To extract personalization data

- 1 Call the corresponding method:
  - For JSPs and servlets: `getUserPrincipal()` of the request object.
  - For EJB: `getCallerPrincipal()` of the EJB context.
- 2 To extract personalization data, call `getP13n()` by using the Principal object obtained in step [step 1](#).

[Extracting Personalization Data from a Servlet](#) shows how to extract personalization data from a servlet. In this example, the `PersonalizationServlet` displays all personalization data retrieved from Principal in a table.

### Extracting Personalization Data from a Servlet

The following sample shows how personalization data is extracted.

```
import java.io.*;
import java.util.*;
import javax.servlet.*;
import javax.servlet.http.*;
import java.security.Principal;
import com.hp.ov.selectaccess.solutions.weblogic.securityprovider.principal.SAPrincipalImpl;
import com.hp.ov.selectaccess.solutions.weblogic.securityprovider.principal.SAP13n;

/**
 * This is an example to show how a servlet retrieves personalization data.
 */
public class PersonalizationServlet extends HttpServlet {

    public void doGet (HttpServletRequest request, HttpServletResponse response)
    throws ServletException, IOException {
        SAPrincipalImpl saPrincipal = null;
        SAP13n p13n = null;

        // Get principal from http request
        Principal principal = request.getUserPrincipal();
        if (principal != null && principal instanceof SAPrincipalImpl) {
            saPrincipal = (SAPrincipalImpl)principal;
        }
    }
}
```

```

        // Get personalization object from principal
        p13n = saPrincipal.getP13n();
    }

    response.setContentType("text/html");
    PrintWriter out = response.getWriter();

    out.println("<html>" +
        "<head><title>Select Access WebLogic Enforcer plugPersonalization Test</title></
head>");

    if (p13n != null && !p13n.isEmpty()) {

        out.println("<H3>Personalization info in principal:</H3>");
        out.println("<table border=1><tr><td><b>Key</b></td><td><b>Value</b></td></tr>");

        // Get a collection of keys of all personalization attribute
        Set keySet = p13n.keySet();

        Iterator iterator = keySet.iterator();

        while (iterator.hasNext()) {
            String key = (String)iterator.next();
            String value = null;

            // Get personalization attribute by key
            value = (String)p13n.getAttribute(key);
            out.println("<tr><td>" + key + "</td><td>" + value + "</td></tr>");
        }

        out.println("</table>");

    } else {
        out.println("<p>Personalization info not found in principal.</p>");
    }

    out.println("</body></html>");
    out.close();
}
}

```

## Integration with the WebLogic Portal

The Select Access' WebLogic Enforcer Plugin can be integrated with WebLogic Portal Server versions 8.1 SP3 or later.

Since WebLogic Portal Server has its own proprietary authorization management mechanism, which is not accessible to external security providers, the Select Access's WebLogic Enforcer Plugin will only provide authentication support for WebLogic Portal

Server. Thus, access control for portal resources (such as desktop, book, page, portlet, etc) must be managed in the WebLogic Administration Portal. Security rules for other resources will still be managed in Select Access Policy Builder.

In Select Access, multiple groups can have the same name (cn) as long as their DN's are different. However, the WebLogic Portal Server doesn't allow duplicate group names, so you must make sure there are no duplicated group names defined in Select Access. In Select Access Policy Builder, folders are used to organize users and groups. Although folders are similar to groups in some aspects, the Enforcer Plugin doesn't export folder names to the WebLogic Portal, so folders won't appear in the WebLogic Administration Portal.

To integrate Select Access with the WebLogic Portal Server, you simply follow the instructions to integrate the Select Access' WebLogic Enforcer Plugin with WebLogic Server first, and then configure the Enforcer Plugin to work with the WebLogic Portal Server by

following the steps in [Table 10](#).

**Table 10 Configuring Select Access's WebLogic Enforcer plugin for WebLogic Portal**

Step	Configuration Details
<p><b>Step 1:</b> Configure the Enforcer plugin with your Select Access directory server connection information. This information provides user and group information to the WebLogic Portal, the Enforcer Plugin needs</p> <p><b>Note:</b> This solution currently allows for Portal users on a single directory only.</p>	<p>Open the enforcer configuration file <code>bea_enforcer.properties</code>, and add the following configuration items:</p> <ul style="list-style-type: none"> <li>• <code>DirectoryServer</code> — The URL of directory server, including port number. For example: <code>DirectoryServer=ldap://localhost:389</code></li> <li>• <code>DirectoryServerPrincipal</code> — The username for login to directory server. If empty or not defined, the Enforcer Plugin will try to connect to the directory server as an anonymous user.</li> <li>• <code>DirectoryServerCredential</code> —The login credentials necessary to access the directory server.</li> <li>• <code>UserStoreLocation</code> —The Select Access user store location. For example: <code>UserStoreLocation=ou=people,dc=mydomain,dc=mycompany,dc=com</code></li> <li>• <code>UserIDAttribute</code> —The attribute of user entry in LDAP server to uniquely identify a user in WLS. For example: <code>UserIDAttribute=uid</code></li> </ul> <p><b>Note:</b> To make Select Access's WebLogic Enforcer plugin work well with the WebLogic Portal, you have to define the personalization data <code>UID</code> in Policy Builder. You also need to make sure the value of <code>UserIDAttribute</code> is same as the value of <code>UID</code>. For details about setting personalization data <code>UID</code>, see <a href="#">page 37, Table 7, step 3</a>.</p> <ul style="list-style-type: none"> <li>• <code>GroupNameAttribute</code>— The attribute of group entry in LDAP server to uniquely identify a group in WLS. For example: <code>GroupNameAttribute=cn</code></li> </ul>

**Table 10 Configuring Select Access's WebLogic Enforcer plugin for WebLogic Portal**

Step	Configuration Details
<p><a href="#">Step 2: Configure Security Rules in Policy Builder.</a></p>	<p>When the WebLogic Portal Server starts up, the Portal Framework needs to access some resources anonymously. You need to setup proper security policy to allow anonymous access to those resources. Some common resources needed by all portal server include:</p> <ul style="list-style-type: none"> <li>• <b>JNDI Resources:</b> <ul style="list-style-type: none"> <li>lookup/&lt;portal_app_name&gt;</li> <li>lookup/weblogic</li> <li>lookup/portalFrameworkPool</li> <li>lookup/jws</li> <li>lookup/cgDataSource</li> </ul> </li> <li>• <b>JMS Resources:</b> <ul style="list-style-type: none"> <li>receive/queue/cgJWSQueue</li> </ul> </li> <li>• <b>JDBC Resources:</b> <ul style="list-style-type: none"> <li>reserve/ConnectionPool/cgPool</li> </ul> </li> </ul> <p>Other resources may also require to be accessed anonymously during portal server startup depending on the implementation of your portal application. To configure those resources, see <a href="#">Configure Resources Required During Server Startup</a> on page 48.</p>
<p><a href="#">Step 3: Reboot WebLogic Portal Server to implement these changes.</a></p>	<p>N/A</p>
<p><a href="#">Step 4: Configure Security Rules in WebLogic Administration Portal to browse users and groups provided by Select Access Authenticator.</a></p>	<ol style="list-style-type: none"> <li>1 Login to WebLogic Administration Portal.</li> <li>2 In the Service Administration page, click <b>Authentication Hierarchy Service</b> from the left pane.</li> <li>3 Type in <code>SAAAuthenticator</code> in the textbox next to <b>Provider to Add to Build List</b>.</li> <li>4 Click <b>Update &amp; Build Tree</b>.</li> <li>5 In the Users and Groups page, choose <code>SAAAuthenticator</code> from the <b>Browse User-Groups</b> from drop-down list.</li> <li>6 Verify that the Select Access users and groups appear in the screen.</li> </ol>

## Configure Resources Required During Server Startup

If your portal application cannot startup correctly after installing Select Access' WebLogic Enforcer Plugin, it is probably because the anonymous access to some resources were denied by the Select Access Policy Validator.

### To determine resource denials

- 1 Modify the Enforcer plugin's log level to `info`.
- 2 Restart your server.
- 3 Check the Enforcer plugin's audit output to determine which resources were denied by Policy Validator.
- 4 Choose one of the following approaches to solve the problem:
  - Setup a security policy to allow anonymous access to the resources.
  - **(Recommended)** Grant the caller a proper `run-as` role in its deployment descriptor. You can only choose this option if the caller is a component of your application instead of a component of Portal Framework.

## Configure Security Policy and User Profiles in the WebLogic Administration Portal

Once you are able to see Select Access users and groups in the WebLogic Administration Portal, you can:

- Create visitor entitlement based on Select Access users and groups.
- Build security policy by using that entitlement
- Edit user's profiles. Please refer to WebLogic Portal documents for details about management security and user profile in portal.

The Select Access' WebLogic Enforcer plugin only allows read-only access to the Select Access user store. Editing the user, group or group membership information with the WebLogic Administration Portal won't have any effect.