

HP OpenView Select Access

Integration Paper for Oracle9i Application Server

Software Version: 5.2

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



October 2003

© Copyright 2000-2003 Hewlett-Packard Development Company, L.P.

Legal Notices

Warranty

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

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

Restricted Rights Legend

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

Hewlett-Packard Company
United States of America

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

Copyright Notices

© Copyright 2000-2003 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.

OpenView Select Access includes software developed by third parties. The software 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 OpenView Select Access's `<install_path>/3rd_party_license` directory.

Trademark Notices

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

Support

Please visit the HP OpenView Select Access web site at:

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

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

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

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

The support site includes:

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

Contents

Chapter 1: About this Integration Paper	1
What is it about?	1
Who is it for?	1
What does it assume you already know?	2
Related references	2
Chapter 2: Technologies overview	3
What is Select Access?	3
What does Select Access do?	3
Supports single sign-on	3
Enables user profiling	4
Provides user password and profile management	4
Delegates administration	5
Provides an end-to-end auditing system	5
Automates the discovery and maintenance of corporate resources	5
How does Select Access work?	6
Other Select Access components	6
Third-party components Select Access integrates with	7
Custom plugins you can customize functionality with	7
What is Oracle9i application server?	8
Issues that affect Oracle9i application server	8
The benefits of Select Access's solution	9
Chapter 3: Integrating Select Access with Oracle9i application server	11
Configuring Select Access	11
Configuring Oracle9i application server	14

What is it about?

This Integration Paper describes how to integrate Oracle9i application server with HP OpenView Select Access.

An overview of this document's contents is listed in Table 1.

Table 1: Integration Paper overview

This chapter ...	Covers these topics...
Chapter 2, <i>Technologies overview</i>	<ul style="list-style-type: none">• HP OpenView Select Access: what it is, what it does, and how it works.• Oracle9i application server: what it is and what integration issues exist.
Chapter 3, <i>Integrating Select Access with Oracle9i application server</i>	Describes what you need to do with Oracle9i application server and Select Access to integrate these technologies.

Who is it for?

This Integration Paper is intended to instruct individuals or teams responsible for the following:

- Integrating Select Access with their Oracle9i application server.
- Using Select Access to administer policies to users registered in your Oracle9i application server.

What does it assume you already know?

This Integration Paper assumes a working knowledge of:

- *HP OpenView Select Access* – Ensures that you understand how integration with Oracle9i application server affects the Select Access components.
- *Oracle9i application server* – Ensures that you understand how integration with Select Access affects the Oracle9i application server components.
- *Web server and plugin technology* – Combinations that are used to add a specific feature or service to a larger system. This helps you understand how different components of Select Access communicate with each other and with your existing network.

Related references

Before you begin to integrate Select Access with Oracle9i application server, you may want to begin by familiarizing yourself with the contents of the following documents:

- *HP OpenView Select Access v5.2 Network Integration Guide*, © Copyright 2000-2003 Hewlett-Packard Development Company, L.P.
(network_integration_guide.pdf)
- *HP OpenView Select Access v5.2 Installation Guide*, © Copyright 2000-2003 Hewlett-Packard Development Company, L.P.
(installation_guide.pdf)
- *HP OpenView Select Access v5.2 Policy Builder Guide*, © Copyright 2000-2003 Hewlett-Packard Development Company, L.P.
(policy_builder_guide.pdf)
- *HP OpenView Select Access v5.2 Developer's Guide*, © Copyright 2000-2003 Hewlett-Packard Development Company, L.P.
(developers_guide.pdf)

Chapter 2

Technologies overview

This chapter introduces you to HP OpenView Select Access. It gives you an overview of the product, what it does, and what components are installed with this product

What is Select Access?

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

What does Select Access do?

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

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

Together, this extended functionality provides a simplified experience for both the end user and those responsible for managing the user's experience.

Supports single sign-on

To improve user satisfaction, Select Access incorporates a Web Single Sign-On (SSO) capability. This means users can sign on once to access the

appropriate resources and have their information stored for future access. Select Access supports transparent navigation between:

- Multiple proprietary domains: For organizations with ownership of multiple Web sites.
- Multiple partnering domains: For on-line business partners so they can securely share authentication and authorization information across corporate boundaries that have separate:
 - user databases
 - authorization policies
 - access management products

These different SSO methods means that users do not have to remember multiple passwords or PINs nor do they have to call your help desk because they have forgotten their passwords or PINs.

Enables user profiling

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

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



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

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

Provides user password and profile management

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

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

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

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

Delegates administration

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

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

Provides an end-to-end auditing system

Select Access can record all access and authorization actions, as well as all policy administrative change to any number of output to:

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

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

Automates the discovery and maintenance of corporate resources

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

How does Select Access work?

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

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

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

The authentication process

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

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

Other Select Access components

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

- **Administration server & Setup Tool:** As a mini Web server, the Administration server is responsible for the configuration of core components and deployment of the Policy Builder applet in a user's browser. The Setup Tool is a client of the Administration server: it is the interface that allows you to quickly set up and deploy Select Access.

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

Third-party components Select Access integrates with

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

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

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

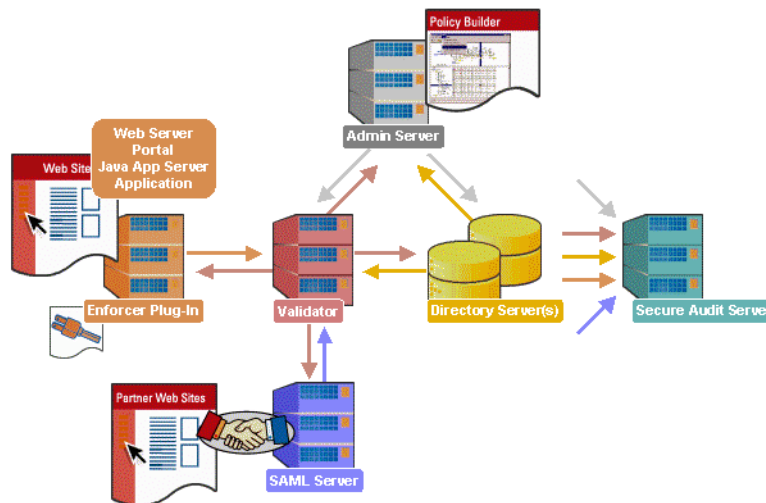


Figure 1: Select Access system architecture

Custom plugins you can customize functionality with

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

- Authentication plugins: A custom Policy Builder authentication plugin allows you to tailor which kinds of authentication methods are available to better meet the needs of your organization. A Policy Builder authentication method plugin allows administrators to use and configure the authentication server for this method via a dialog box. Like the decision point plugin, this dialog box is known as a property editor, that allows security administrators to configure it.

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

What is Oracle9i application server?

The Oracle9i application server is a set of services that allows for the deployment of applications in a distributed computing environment. This server sits between the client and the directory server database and manages application logic from this central location. The communication of user requests and responses is typically in HTTP format and is handled by Oracle's HTTP Server, which is powered by Apache. Oracle9i application server is available for both Windows NT/2000 and Sun Solaris platforms.

Issues that affect Oracle9i application server

There are two main issues you need to consider:

- *Access policies* – You can only use Select Access's policies for security purposes. Oracle9i application server's security policies are disabled once Oracle is integrated with Select Access.
- *Protected resources* – You can only protect content that users try to access via the HTTP Server. This content generally consists of HTML files, JSP files, and any links that launch java servlets.

For details, see *Configuring Select Access* on page 11 and *Configuring Oracle9i application server* on page 14.

The benefits of Select Access's solution

Integrating Select Access with Oracle9i application server offers the following main benefits:

- **Consolidated policy management** – You can set all the policies and resources for your corporate site using only Select Access. Using only one policy management tool makes policy administration easier.
- **Consolidated user management** – You can use the users from the Select Access Policy Store without being required to replicate them across different Policy Stores.
- **Single sign-on (SSO)** – SSO is an important feature of Select Access that allows users to authenticate once to any number of servers (for example, Web or java servers) on single or multiple domains, despite being on different hosts. Once authenticated by Select Access, a user's credentials act like a passport, giving users access to distributed portal content, groupware, workflow or client/server applications.

Integrating Select Access with Oracle9i application server

There are two sides to integrating Select Access with Oracle9i application server on Windows and Solaris:

- **Configuring Select Access:** This requires that you:
 - Add Oracle9i application server services and resources
 - Set access policies against Oracle9i application server's content.For details, see *Configuring Select Access* on page 11.
- **Configuring Oracle9i application server:** This requires that you:
 - Install an Apache Enforcer plugin on Oracle9i application server
 - Manually edit Oracle9i application server's configuration file `httpd.conf` so that it automatically loads the Enforcer plugin upon startup.

For details, see *Configuring Oracle9i application server* on page 14.

Configuring Select Access

Setting up Select Access with Oracle9i application server only requires standard settings to get Select Access to integrate and function with Oracle9i

application server successfully. Table 1 describes the steps you need to take to set up Select Access with Oracle9i application server.

Table 1: Setting up Select Access

This step ...	Details on how to do it...
<p>Step 1: Add your Oracle HTTP server to the Resources Tree as a service branch.</p>	<ol style="list-style-type: none"> 1. Right-click a folder or the root of the Resources Tree. 2. Click Run Discovery>Services. The Discover Networks Services dialog box appears. 3. Provide the required information on the Networks and Protocols tabs and then click OK. For details, see Chapter 4 , <i>Building your Users and Resources Trees in the HP OpenView Select Access v5.2 Policy Builder Guide</i>. <p>Note: For details on performing this procedure manually, see Chapter 4 , <i>Building your Users and Resources Trees in the HP OpenView Select Access v5.2 Policy Builder Guide</i>.</p>
<p>Step 2: Add the resources you want to protect under the services you just created.</p>	<ol style="list-style-type: none"> 1. Make sure you have configured the network resource plugin. For details, see Chapter 4 , <i>Building your Users and Resources Trees</i>. 2. On the Resources Tree, right-click the service you want to scan for available resources. 3. Click Run Discovery>Resources. The Discover Network Resources dialog box appears. <ul style="list-style-type: none"> – Information about the service’s representative server is entered automatically in the Protocol, Hostname, and Port Number fields. (This information is taken from the service’s properties.) – If you have configured a plugin for the protocol used by the service, the plugin’s configuration details are entered automatically in the Plugin Settings field. 4. Select Run Resource Discovery Plugin and fill out the fill in any empty fields. 5. Select the location on the Resources Tree to add the resources. Do the following: <ol style="list-style-type: none"> a. Click the Browse button beside the Network Resources Tree Destination field. The Select Resource Destination dialog box appears. b. Select a service, then click OK. <p>or</p> <ol style="list-style-type: none"> a. Select a folder or the root of the Resources Tree. b. Click New and create a new service. c. Select it in the Select Resource Destination dialog box, then click OK. 6. Click OK. <p>For details, see <i>Automatically generating a list with a discovery plugin</i> on page 41 in the <i>HP OpenView Select Access v5.2 Policy Builder Guide</i>.</p> <p>Note: For details on performing this procedure manually, see <i>Manually adding a network resource to a service</i> on page 39 in the <i>HP OpenView Select Access v5.2 Policy Builder Guide</i>.</p>

Table 1: Setting up Select Access (Continued)

This step ...	Details on how to do it...
<p><i>Step 3:</i> Set up an authentication server.</p>	<p>Enter the authentication server you want to use with Oracle9i application server in the Authentication Servers dialog box. The Policy Builder allows you to enter four types of authentication servers:</p> <ul style="list-style-type: none"> • Certificate • Password • RADIUS • Registration • SecurID <ol style="list-style-type: none"> 1. Click Tools>Authentication Servers, then in the Authentication Servers dialog box, click the Add button. The Authentication Method dialog box appears. 2. In the Server Name box, enter a name for the server. The name must contain at least two characters. 3. In the Authentication Methods group, determine what method the server uses to authenticate users. 4. Click OK to configure the server properties for the corresponding authentication server.
<p><i>Step 4:</i> Set your access policies against Oracle9i application server's content.</p>	<p>Set allow, deny, and conditional rules on resources as needed. For details, see Chapter 8, <i>Controlling network access in the HP OpenView Select Access v5.2 Policy Builder Guide</i>.</p> <p>Note: The rules you apply are inherited across multiple resources. Ensure you understand how policies are inherited.</p>

Configuring Oracle9i application server

You need to perform specific configuration steps on Oracle9i application server. Table 2 describes what you need to do to synchronize data between Select Access and Oracle9i application server.

Table 2: Setting up Oracle9i application server

This step...	Details on how to do it...
<p>Step 1: Install an Enforcer plugin on the machine running Oracle9i application server's HTTP Server.</p>	<ol style="list-style-type: none"> 1. Run the Select Access installer. 2. Click Next until you reach the Choose HP OpenView Select Access components installation screen. 3. Install and configure the Apache Enforcer plugin on the Oracle9i application server host. 4. Do not check either of the following two boxes: <ul style="list-style-type: none"> – Update Web server configuration to load the Enforcer Plugin – Restart Web server 5. For Windows users only: <p>Copy the <code>oracle_apache_web32.dll</code> file from the <code>Solutions/Oracle</code> directory on the Select Access Installation CD to <code>C:\Program Files\HP OpenView\Select Access\bin</code>.</p> <p>For details, see the <i>HP OpenView Select Access v5.2 Installation Guide</i>.</p>
<p>Step 2: Edit the <code>httpd.conf</code> file so that it automatically loads the Enforcer plugin upon startup.</p>	<ol style="list-style-type: none"> 1. Open the <code>httpd.conf</code> file in the following locations, depending on the platform you are running on: <ul style="list-style-type: none"> – On Windows: <pre><Oracle_install_path>\Apache\Apache\conf</pre> – On Solaris: <pre><Oracle_install_path>/Apache/Apache/conf</pre> – where <code><install_path></code> is the location where Oracle is installed. 2. In the <code>LoadModule enforcer_module</code> section of the file, add the following line to the beginning of the list, depending on which platform you are running on: <ul style="list-style-type: none"> – On Windows: <pre>C:\Program Files\HP OpenView\Select Access\bin\oracle_apache_web32.dll</pre> – On Solaris: <pre>/opt/OV/SelectAccess/bin/mod_enforcer.so</pre> 3. In the <code>ClearModuleList</code> section, type the following line as the last list entry: <pre>AddModule mod_enforcer.c</pre> 4. Save the <code>httpd.conf</code> file and restart your Oracle9i application server for these changes to take effect.

