HP OpenView Select Access

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

Software Version: 6.0

Integration Paper for Sun ONE Application Server

September 2005

Legal Notices

Warranty

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

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

Restricted Rights Legend

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

Hewlett-Packard Company
United States of America

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

Copyright Notices

Trademark Notices

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

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

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

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

To register for an HP Passport ID, go to:

https://passport2.hp.com/hpp/newuser.do

Contents

1 About this Integration Paper . . . 3
What is it about? . . . 3
Who is it for? . . . 3
What does it assume you already know? . . . 3
Related references . . . 4

2 Technologies overview . . . 5
What is Select Access? . . . 5
What does Select Access do? . . . 5
Supports Single Sign-on . . . 5
Enables User Profiling . . . 6
Provides User Password and Profile Management . . . 6
Delegates Administration . . . 7
Provides an End-to-end Auditing System . . . 7
Automates the Discovery and Maintenance of Corporate Resources . . . 7
How does Select Access work? . . . 7
Other Select Access Components . . . 8
Third-party Components Select Access Integrates With . . . 8
Custom Plugins to Customize Functionality With . . . 9
What does Sun ONE application server support? . . . 10
The benefits of Select Access' solution . . . 10

3 Integrating Select Access with Sun ONE application Server . . . 13

1 About this Integration Paper

What is it about?

This Integration Paper describes how to integrate Sun ONE application server with Select Access.

Select Access 6.0 is the last version HP performed interoperability testing against. If you have any questions regarding the interoperability of your version of Select Access with this third-party product, contact HP's Support Services.

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

Table 1 Select Access & Sun ONE application server Integration Paper overview

This chapter...	Covers these topics...
2, *Technologies overview*	• Introduces Select Access: what it is, what it does, and how it works. • Introduces Sun ONE application server: on which platforms it is supported.
3, *Integrating Select Access with Sun ONE application Server*	Describes what you need to do with Sun ONE application server and Select Access to integrate these technologies.

Who is it for?

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

- Integrating Select Access with their Sun ONE application server.
- Using Select Access to manage access to Sun ONE application server resources.

What does it assume you already know?

This guide assumes a working knowledge of:

- **Select Access**—Ensures that you understand how integration with Sun ONE application server affects the Select Access components.
- **Sun ONE application server**—Ensures that you understand how integration with Select Access affect the Sun ONE application server components.
- **LDAP directory servers—**Helps ensure that information in the Policy Builder is set up correctly.
- **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 Sun ONE application server, you may want to begin by familiarizing yourself with the contents of the following documents:

- *HP OpenView Select Access 6.0 Installation Guide*, © Copyright 2000-2004 Hewlett-Packard Development Company, L.P. (`installation_guide.pdf`)
- *HP OpenView Select Access 6.0 Network Integration Guide*, © Copyright 2000-2004 Hewlett-Packard Development Company, L.P. (`network_integration_guide.pdf`)
- *HP OpenView Select Access 6.0 Policy Builder Guide*, © Copyright 2000-2004 Hewlett-Packard Development Company, L.P. (`policy_builder_guide.pdf`)
- *HP OpenView Select Access 6.0 Developer's Tutorial Guide*, © Copyright 2000-2004 Hewlett-Packard Development Company, L.P. (`dev_tut_guide.pdf`)
- *HP OpenView Select Access 6.0 Developer's Reference Guide*, © Copyright 2000-2004 Hewlett-Packard Development Company, L.P. (`dev_ref_guide.pdf`)
- Hewlett-Packard, Application/portal servers *Integration Papers*, © Copyright 2000-2004 Hewlett-Packard Development Company, L.P.

2 Technologies overview

This chapter introduces you to Select Access and Sun ONE application server. It gives you an overview of the products, what they do, what components are installed with these products, and Sun ONE application server integration issues.

What is Select Access?

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

What does Select Access do?

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

- *Supports Single Sign-on*
- *Enables User Profiling*
- *Provides User Password and Profile Management*
- *Delegates Administration*
- *Provides an End-to-end Auditing System*
- *Automates the Discovery and Maintenance of Corporate Resources*

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

Supports Single Sign-on

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

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

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

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

Enables User Profiling

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

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

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

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

Provides User Password and Profile Management

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

- *Password administration*: Allows you to set the policies and expiration times for user passwords. Select Access automates reminders and messages. Other administration features include:
  - Profile lockout and re-activation
  - Password history lists
- *Self-servicing*: Allows users to initiate:
  - The definition of new or existing passwords, which are controlled by the password policy you create.
  - The modification of profile data, which is predefined by the attributes you select. Typically, these attributes are the same attributes the user provides when they register with your organization. If the user is already known to you (like an employee or a supplier), you can pre-populate the values for them.

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

Delegates Administration

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

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

Provides an End-to-end Auditing System

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

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

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

Automates the Discovery and Maintenance of Corporate Resources

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

How does Select Access work?

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

- Policy Builder: Allows full or delegated administrators to define the authentication methods and authorization policies with an easy-to-use administration grid.

- Policy Validator: Serves the access decision to the Enforcer plugin after it accepts and evaluates the user's access request with the policy information retrieved from the directory server that holds your Policy Store.
- Enforcer plugin: Acts as the agent for Select Access on the Web/application server. The Enforcer plugin enforces the outcome of the access request that has been evaluated by the Policy Validator.
- SAML server: Handles the logistics of transferring users between your web sites and those of your partners.

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

The Authentication Process

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

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

Other Select Access Components

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

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

Third-party Components Select Access Integrates With

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

- Directory server—LDAP v3.0 compliant: is the foundation of a Select Access-protected system. It acts as the repository of information. Depending on how you have set up your directory system, Select Access can use one or more directory servers to store:
  - A single policy data location
  - One or more user data locations

- Web/Application/Portal/Provisioning servers: are third-party technologies that use Select Access as their authorization and access management system. Depending on your server technology, you can use Select Access's native SSO and/or personalization solution rather than use the server's built-in alternative for a more robust solution.

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

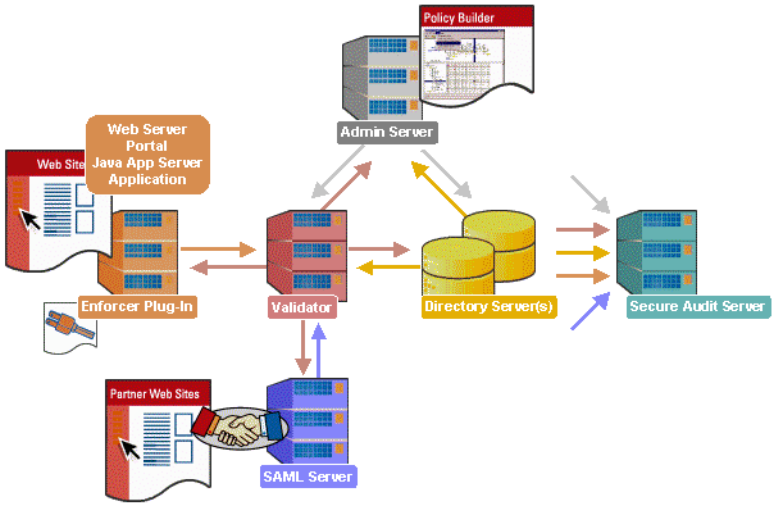

Figure 1 Select Access system architecture

Custom Plugins to Customize Functionality With

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

- Authentication plugins: A custom Policy Builder authentication plugin allows you to tailor which kinds of authentication methods are available to better meet the needs of your organization. A Policy Builder authentication method plugin allows administrators to use and configure the authentication server for this method via a dialog box. As with the decision point plugin, this dialog box is a property editor that allows security administrators to configure the authentication server.
- Decision point plugins: A custom Rule Builder decision point plugin allows you to tailor how rules are built to better meet the needs of your organization. A Rule Builder decision point plugin allows administrators to use and configure the criteria for the decision point via:
  - The icons that represent that decision point on both the toolbar and the rule tree.
  - The dialog box, known as a property editor, that allows security administrators to configure it.
- Policy Validator decider plugins: The Validator-specific counterpart of a decision point plugin, the decider plugin allows you to capture the evaluation logic for your custom decision point (described above), so that the Policy Validator can evaluate users based on the information it collects.
- Resource discovery plugins: These plugins allow you to customize how resources are scanned on your network.

- Enforcer plugins: A new Enforcer plugin allows you to customize the backend application logic by enforcing the decision that the Policy Validator returns to the Enforcer plugin's query.
- Additional Web/Application/Portal/Provisioning server specific plugins: These plugins can be included to handle specific integration details between the third-party technology and Select Access. For example, the Domino server requires a `site_data` plugin if you need to transfer site data between Select Access and Domino.

What does Sun ONE application server support?

The Sun ONE application server is a J2EE-compliant application server, which means it supports JSPs, servlets, and EJB applications. It features load-balancing, failover, and high availability which allows J2EE applications to scale as demand increases.

The Sun ONE application server is available for the following platforms:

- Solaris
- Windows NT and 2000

The benefits of Select Access' solution

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

- **Consolidated policy management**—You can set all the policies for your Web site and applications using Select Access. Using only one policy management tool makes policy administration easier.
- **Single sign-on (SSO)**—This key technology is required for distributed systems like Sun ONE application server. SSO is an important feature of Select Access that allows users to authenticate once to any number of servers (for example, Web or application 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 application server content, groupware, workflow or client/server applications.

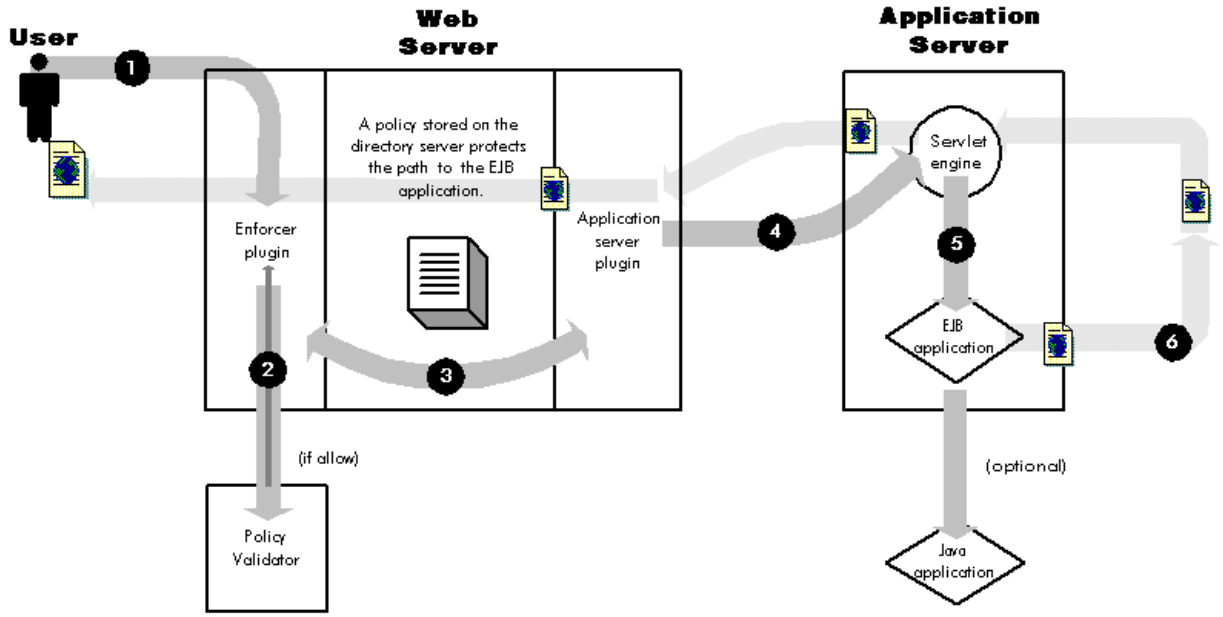

Figure 2 Select Access-protected application server

3 Integrating Select Access with Sun ONE application Server

Setting up Select Access with the Sun ONE application server not only requires that you use default features, but it also requires that you make minimal custom settings to get Select Access to integrate and function with Sun ONE application server.

The application server ships with an LDAP server. However, you must use a separate LDAP server to store your Select Access configuration, or else policy information overwrites the Sun ONE-specific LDAP configuration.

Table 2 describes the steps you need to take to set up Select Access.

Table 2 Setting up Select Access

This step...	Details on how to do it...
Step 1: Install an enforcer plugin on each machine that hosts an Sun ONE application server.	1 Run the Select Access installer. 2 Click **Next** until you reach the **Choose Select Access** installation screen. 3 Install and configure the Sun ONE (iPlanet) Enforcer plugin. For details, see the *HP OpenView Select Access 6.0 Installation Guide*.

Step 2: If you have more than one Sun ONE application server running, edit your `enforcer.xml` file for your plugins to enable SSO.	To enable single sign-on (SSO):
	1 On the server where the Enforcer plugin is installed, copy this file:
	`C:\Program Files\HP OpenView\Select Access\bin\enforcer.xml-nt.example`
	to:
	`C:\Program Files\HP OpenView\Select Access\bin\enforcer.xml`
	2 Modify the following parameters as needed:
	— `cookie_domain`–If set to `<string>`, then all session cookies use the given domain. This can be used to provide SSO in a multiple Web server environment.
	— `protected_domain`–This tag allows the Enforcer plugin to identify the subsequent value as a protected domain. This can be used to provide multi-domain SSO.
	Note: Depending on the domain your application server is on, you may need to set both of these parameters.
	Note: To configure MD SSO, you need to modify the `enforcer.conf` files on Web servers, so that they all share a mutually inclusive list of protected domains that allows analogous M-D SSO, register all Policy Validators with the same directory server, and ensure distributed Web servers use the same authentication method.
	For details, see the *HP OpenView Select Access 6.0 Installation Guide*.
	3 Save changes.

Table 2 Setting up Select Access

This step...	Details on how to do it...
Step 3: Create a new set of services for Sun ONE application server components on the Resources Tree.	Since you are adding a known number of services, you can manually add them to the Resources Tree. **Note:** Add Sun ONE application server's dynamic resources (for example, EJB applications, servlets, and JSPs) to the Resources Tree while maintaining their Sun ONE deployment description. The deployment description refers to the path by which your browser can locate the application resources. 4 Right-click a folder or the root of the Resources Tree. 5 Click **New>Service**. The **New Service** dialog box appears. 6 In the **Name** field, enter a name for the service to be used on the Resources Tree. For example, if you are creating a service `Server`, you could use the host machine's name to describe the service (for example, `myServer.mydomain.com`). 7 Click **Add** and configure the **REP**, **Protocol**, **Hostname**, and **Port** cells as needed. For details, see the *HP OpenView Select Access 6.0 Policy Builder Guide*.
Step 4: Add Sun ONE application server's application resources to the Policy Builder's Resources Tree.	Because Select Access' network discovery plugin does not discover resources on Sun ONE application server, you need to add Sun ONE application server's resources to the Resources Tree in one of the following two ways: • Write your own plugin to scan for Sun ONE application server's resources. • Add application resources manually. To do this: a Right-click the service under which you want to add resources. b Click **New>Resource**. The **New Resource** dialog box appears. c In the **Name** field, type in the name of the resource you want to protect. d Click **OK**. For details, see Chapter 3, *Building your Identities and Resources Trees* in the *HP OpenView Select Access 6.0 Policy Builder Guide*.
Step 5: Set your access policies against Sun ONE application server's applications.	Enable SelectID for the applications that you want Select Access to protect. For details, see Chapter 6, *Setting Up Authentication Services* in the *HP OpenView Select Access 6.0 Policy Builder Guide*.