HP OpenView Select Access

Integration Guide for the Apache 2.0 Web server

Software Version: 6.0

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

March 2004

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

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

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

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

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

Trademark Notices

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

Support

Please visit the HP OpenView Select Access web site at:

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

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

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

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

The support site includes:

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

Contents

Chapter 1
About this Integration Paper

What is it about?

This Integration Paper describes how to integrate the Apache v2.0 Web server with Select Access 6.0. Select Access automatically integrates with Apache v1.3.x servers. If you are installing an Enforcer plugin on this server, integration is seamless. See the *HP OpenView Select Access 6.0 Installation Guide* for details.

Table 1 gives an overview of this document's contents.

Table 1: Integration Paper overview

This chapter...	Covers these topics...
Chapter 2, *Technologies overview*	• Introduces Select Access: what it is, what it does, and how it works. • Introduces Apache v2.0 server: what it is and what integration issues exist.
Chapter 3, *Integrating Select Access with the Apache v2.0 server*	Describes what you need to do with this version of Apache so that Enforcer plugins can successfully protect these servers.

Who is it for?

This Integration Paper is intended to instruct individuals or teams responsible for integrating Select Access with the Apache v2.0 server.

What does it assume you already know?

This Integration Paper assumes a working knowledge of:

- ***Select Access***—Particularly Select Access's Enforcer plugin technology. This ensures that you understand how integration with Apache v2.0 server affects the Select Access components.

- ***LDAP directory servers*—**Helps ensure that information in the Policy Builder is set up correctly.
- ***Building modules/libraries on Apache*—**Familiarity with the build process on Linux, ensures you know the basics required to complete many of the tasks outlined in this paper.

Related references

Before you begin to integrate Select Access with Apache v2.0 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.

Chapter 2
Technologies overview

This chapter introduces you to Select Access and the Apache v2.0 server. It gives you an overview of the products: what they do, what components are installed with these products, and what Apache v2.0 server integration issues exist.

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.

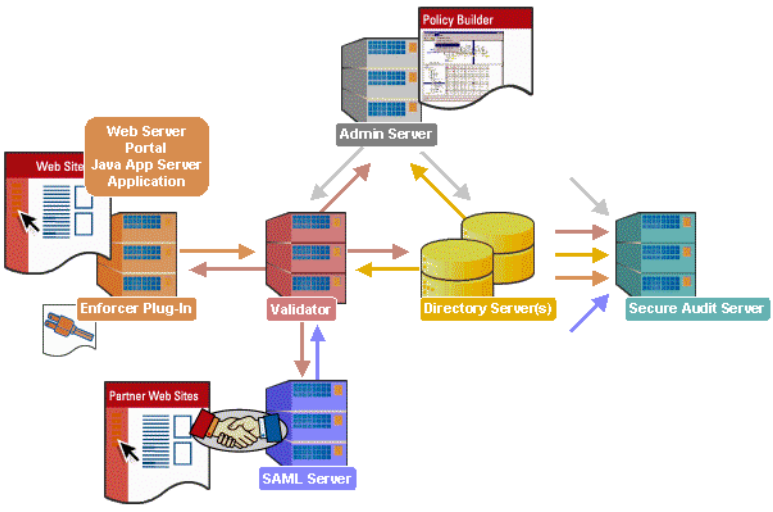

Figure 1: Select Access system architecture

Custom plugins you can customize functionality with

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

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

What is the Apache v2.0 server?

The Apache v2.0 server is an open-source HTTP server for operating systems that include UNIX and Windows NT. The previous version of this server was v1.3.x. Support of this older version of Apache is seamless. However, because of the new features and upgrade

modules added by the Apache Group in this latest release, HP requires that you integrate this server by-hand.

How the Select Access and Apache v2.0 server solution works

The Apache v2.0 server works in the same way as it does on the Apache v1.3.x servers: that is, an Enforcer plugin acts as the access control agent that integrates with the rest of the Select Access system. However, unlike the Apache Enforcer plugin for Apache v1.3.x servers, the Enforcer plugin module for the Apache v2.0 server is not installed by default and consequently the module cannot be automatically integrated with the new server simply by running the Setup Tool.

Issues that affect Apache v2.0 server

There are three main issues that affect the Apache v2.0 server with Apache:

- This integration of Apache has only been tested against the RedHat 7.2 Linux operating system with version 2.0.40 of the Apache Web server. It has not been tested on Solaris, HP-UX, nor WindowNT. Therefore HP recommends that you only integrate Select Access on this version of Linux.
- In order to integrate the Apache v2.0 server with Select Access, you need to rebuild the binaries with the corresponding modules.
- Depending on whether or not you have upgraded Apache on a network that already has Select Access installed, you may not need to configure the Enforcer plugin.

Chapter 3
Integrating Select Access with the Apache v2.0 server

Integrating these two technologies requires that you perform specific integration tasks against both Apache and Select Access technologies. This ensures both products function properly as a unit. Table 1 summarizes the configuration steps you must take to ensure you can successfully SelectAccess-protect your Apache v2.0 server.

Table 1: Integrating Select Access with the Apache v2.0 server

For this step...	Do this...
Step 1: If you have not already done so, install the Apache Enforcer plugin (for Apache v1.3.x). **Note:** If you have upgraded your Apache Web server to version 2 from version 1.3.x, and you already have this Apache Enforcer plugin installed, skip to Step 3. Your existing configuration will work seamlessly with the new plugin for the Apache v2.0 server.	Depending on whether or not you have installed any Select Access components on this host computer, do one of the following: • *If components are already installed*: From the command line, enter the following: `<install_path>/UninstallerData/Uninstaller`. Then run the program in **Modify** mode. You need to add the Apache Enforcer plugin to the components that already exist on this host. • *If no components are installed*: Run the installer from the product CD. Ensure the Apache Enforcer plugin is one of the components you install on this host. For details, see Chapter 3, *Installing Select Access* in the *HP OpenView Select Access 6.0 Installation Guide*. **Note:** You do not need to have Apache v1.3.x installed on the host computer to install and configure this version of the plugin.

Table 1: Integrating Select Access with the Apache v2.0 server

For this step...	Do this...
Step 2: If you have installed the Apache Enforcer plugin for the first time, configure it using the Setup Tool. Both the installer and maintenance program automatically launch the Setup Tool when the installation of Select Access components is complete. The Apache v2.0 plugin seamlessly uses the `enforcer_apache.xml` configuration file the Setup Tool generates.	1. Click **Next** until you reach the Apache Enforcer plugin setup screen. 2. Configure the plugin for your deployment of Select Access with the subsequent configuration screens. For details, see Chapter 8, *Configuring the Enforcer plugins* in the *HP OpenView Select Access 6.0 Installation Guide*. 3. When you reach the **Finish** setup screen, do not check either of the following options: — **Update the Web server configuration to load the Enforcer plugin** — **Restart Web server** This is because the `httpd.conf` files between the two versions of Apache vary slightly. Version 1.3.x of the file contains an `AddModule` line that does not exist in version 2. Therefore, if you restart the Apache v2.0 server and this line exists in its `httpd.conf` file, the Web server fails.

Step 3: Build the Apache v2.0 server for use with Select Access.	Compile your Web server with all modules shared and include SSL module. The sequence of commands to accomplish this is:
	`./configure --prefix=/usr/local/apache2 \`
	`--enable-mods-shared=all \`
	`--enable-ssl --with-ssl=/usr`
	`make`
	`make install`

Step 4: Copy the Enforcer plugin for the Apache v2.0 server. Because this file is not installed, you need to copy it from the product CD.	1. Locate the `../solutions/Apache2/` folder on the Select Access CD. 2. Copy the `mod_enforcer2.so` binary file to your Apache host machine in the following location: `/opt/OV/SelectAccess/bin/` This binary file is your Apache Enforcer plugin for this version of Apache.
Step 5: Modify the Apache v2.0 server's `httpd.conf` file to load the file you copied in the previous step.	Add the following `LoadModule` statement. If you are using an SSL-enabled installation of the Apache server, place this line after the `LoadModule` statement that loads the SSL module (`mod_SSL.so`). `LoadModule enforcer_module /opt/OV/SelectAccess/bin/mod_enforcer2.so`