HP OpenView Select Access

Integration Paper for Apache 1.3 configured as a Reverse Proxy 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 Apache Reverse Proxy server with 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, *Technologies overview*	• Introduces Select Access: what it is, what it does, and how it works. • Introduces Apache Reverse Proxy server: what it is and what integration issues exist.
Chapter 3, *Integrating Select Access with Apache Reverse Proxy server*	Describes what you need to do with Apache Reverse Proxy server and Select Access to integrate these technologies.

Who is it for?

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

- Integrating Select Access with Apache Reverse Proxy server.
- Using Select Access to manage access to Apache Reverse Proxy server's resources.

What does it assume you already know?

This Integration Paper assumes a working knowledge of:

- ***Select Access*** — Ensures that you understand how integration with Apache Reverse Proxy server affects the Select Access components.
- ***Apache Reverse Proxy server*** — Ensures that you understand how integration with Select Access affects Apache Reverse Proxy server.
- ***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.
- ***Building modules/libraries on Apache*** — Familiarity with the build process on different operating systems (that is, Linux and Solaris), 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 Reverse Proxy 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 Apache Reverse Proxy server. It gives you an overview of the products, what they do, what components are installed with these products, and what Apache Reverse Proxy 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.

ℹ 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.

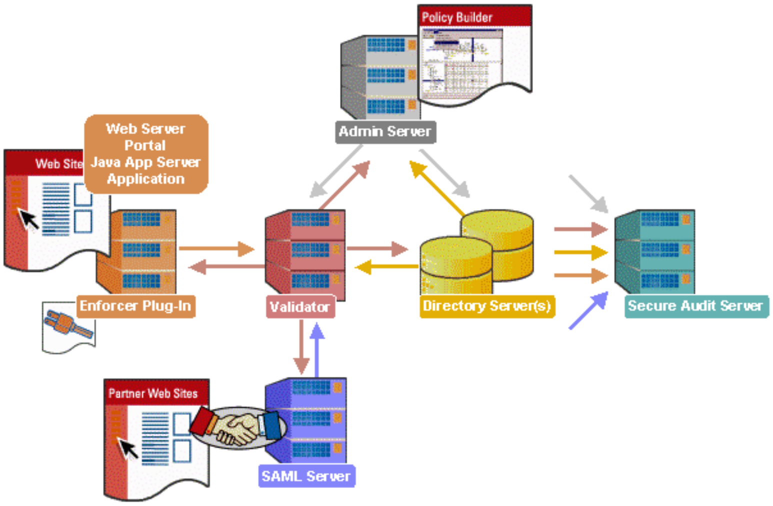

Figure 1: Select Access system architecture

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 Apache Reverse Proxy server?

Apache Reverse Proxy server is an Apache HTTP 1.3.x Web server that has been modified to act as a proxy server. It allows:

- Remote servers to be mapped into the space of the local server.
- Apache to adjust the URL in the location header on HTTP redirect responses.

As a result, the Apache Reverse Proxy server does the following:

- Uses caching features to provide load balancing on a heavily used server.
- Runs outside the firewall to represent a secure content server to outside clients, preventing direct, unmonitored access to your server's data from outside your company. Users cannot get to the real content server because the firewall passage only allows access to the proxy server.
- Filters client transactions by controlling access to remote servers and protocols and by limiting access to specific documents or sites based on usernames, URLs, and client hostnames (or IP addresses).

System requirements

The versions of Apache outlined in Table 1 are supported by Select Access.

Table 1: Select Access-supported versions of Apache

Operating system	Apache version
Windows NT, Windows 2000	IBM HTTP Web server distributed with WebSphere
HP-UX 11	1.3.19
Solaris 2.8, Linux 7.2	1.3.22

The benefits of Select Access's solution

Integrating Select Access with Apache Reverse Proxy server offers the following main benefits:

- *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, multiple domains, or virtual 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. Once users are authenticated, Apache Reverse Proxy server can display personalized content to them, if you have configured the unique user attribute values.
- *Multiple levels of access* – Using a combination of allow, deny and conditional policies ensures user access is restricted to meet your business requirements.
- *Multiple authentication methods*—Select Access's multiple authentication methods (digital certificates, RADIUS, SecurID, and password authentication) extend Apache Reverse Proxy server's security architecture.

- *Load balancing*—Apache Reverse Proxy server uses its caching feature to provide load balancing on a heavily used server.

Chapter 3
Integrating Select Access with Apache Reverse Proxy server

Integrating Select Access with Apache Reverse Proxy server involves installing the Apache Reverse Proxy server with the `mod_proxy` module. To complete the integration, you also need to configure Select Access, which involves:

- Installing and configuring a Select Access Enforcer plugin.
- Adding Apache Reverse Proxy server to the Resources Tree.
- Adding Apache Reverse Proxy server's resources you want to protect under the services you created.
- Setting up an authentication server.
- Setting access policies against Apache Reverse Proxy server's content.

For details, see *Configuring Apache Reverse Proxy server* on page 11 and *Configuring Select Access* on page 12.

Configuring Apache Reverse Proxy server

Table 1 gives an overview of the steps you need to perform to integrate Apache Reverse Proxy server with Select Access. Each step includes more specific details to help you accomplish each integration task.

Table 1: :Setting up Apache Reverse Proxy server

This step...	Details on how to do it...
Step 1: Install Apache on your system with the `mod_proxy` module. For details, see http://httpd.apache.org. This is the standard Apache install procedure.	1. Load the Apache source code onto your system. 2. Run the `configure` command and specify how to install the proxy module. For example: `./configure --prefix=<install_location> --enable-module=so --enable-module=proxy --enable-shared=proxy` 3. Run the `make` command. 4. Run the `make install` command. For details, see *Configuring the Apache Web server* on page 88 of the *HP OpenView Select Access 6.0 Network Integration Guide*.
Step 2: Add `mod_proxy` directives to the reverse proxy server.	Follow the instructions outlined on http://httpd.apache.org/docs/mod/mod_proxy.html and add the following two `mod_proxy` directives to the reverse proxy server: • `ProxyPass` — Allows remote servers to be mapped into the space of the local server. • `ProxyPassReverse`–Lets Apache adjust the URL in the location header on HTTP redirect responses. This is essential when Apache is used as a reverse proxy to avoid by-passing the reverse proxy because of HTTP redirects on the backend servers which stay behind the reverse proxy.

Configuring Select Access

Table 2 gives an overview of the steps you need to perform to integrate Select Access with Apache Reverse Proxy server. Each step includes more specific details to help you accomplish each integration task.

Table 2: Setting up Select Access

This step...	Details on how to do it...
Step 1: Install and configure a Select Access Enforcer plugin. **Note:** This step assumes that a Select Access Administration server and Policy Validator are already installed on your network.	1. Run HP's Select Access installer. 2. Click **Next** until you reach the **Choose Select Access components** installation screen. 3. Install and configure the Enforcer plugin on the Apache Reverse Proxy server host. Choose a **Typical** installation. 4. Check the following two boxes: — **Update Web server configuration to load the Enforcer plugin** — **Restart Web server** 5. Click **Finish**. For details, see Chapter 8, *Configuring the Enforcer plugins* in the *HP OpenView Select Access 6.0 Policy Builder Guide*.
Step 2: Add your Apache Reverse Proxy server to the Resources Tree as a service branch.	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, *Building your Users and Resources Trees* in the *HP OpenView Select Access 6.0 Policy Builder Guide*. **Note:** For details on performing this procedure manually, see Chapter 4, *Building your Users and Resources Trees* in the *HP OpenView Select Access 6.0 Policy Builder Guide*.

This step...	**Details on how to do it...**
Step 3: Add the Apache Reverse Proxy server resources you want to protect under the service you just created.	1. Make sure you have configured the network resource plugin. For details, see Chapter 4, *Building your Users and Resources Trees*. 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. – 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 in any empty fields. 5. Select the location on the Resources Tree to add the resources. Do the following: 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**. or 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**. For details, see *Automatically generating a list with a discovery plugin* on page 44 in the *HP OpenView Select Access 6.0 Policy Builder Guide*. **Note:** For details on performing this procedure manually, see *Manually adding a network resource to a service* on page 43 in the *HP OpenView Select Access 6.0 Policy Builder Guide*.

This step...	Details on how to do it...
Step 4: Set up an authentication server.	Enter the authentication server you want to use with Apache Reverse Proxy server in the **Authentication Servers** dialog box. The Policy Builder allows you to enter five supported types of authentication servers: • Certificate • Password • RADIUS • Registration • SecurID 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.
Step 5: Set your access policies against Apache Reverse Proxy server's content.	Set allow, deny, and conditional rules on resources as needed. For details, see Chapter 8, *Controlling network access* in the *HP OpenView Select Access 6.0 Policy Builder Guide*. **Note:** If you have configured your Apache Reverse Proxy server to map a URL to another URL, set access control on the originally requested URL. For example, if you map all requests from http://www.abc.com`/mycompany/employees/` folder to the http:`/internal123.abc.com/yourcompany/prices/` folder, you need to set permissions on the `/mycompany/employees` folder of the `http://www.abc.com` service. Ensure you set policy on the first resource only. As a rule, the second resource is not managed by Select Access. **Note:** The rules you apply are inherited across multiple resources. Ensure you understand how policies are inherited. For details, see Chapter 8, *Controlling network access* in the *HP OpenView Select Access 6.0 Policy Builder Guide*.