HP OpenView Select Access

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

Software Version: 6.0

Integration Paper for PeopleSoft

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.

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

Support

Please visit the HP OpenView web site at:

http://www.managementsoftware.hp.com/

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

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

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

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

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

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

To find more information about access levels, go to:

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 is PeopleSoft? . . . 10
How does SSO integration work with PeopleSoft? . . . 10
The authentication process using PeopleSoft . . . 10
Issues that affect PeopleSoft . . . 11
The benefits of Select Access's solution . . . 12

3 Integrating Select Access with PeopleSoft . . . 13
Configuring PeopleSoft . . . 14
Configuring third-party authentication . . . 14
Configuring Select Access . . . 16

1 About this Integration Paper

What is it about?

This Integration Paper describes how to integrate PeopleSoft 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 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 PeopleSoft: what it is and what integration issues exist.
Chapter 3, Integrating Select Access with PeopleSoft	Describes what you need to do with PeopleSoft 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 their PeopleSoft.
- Using Select Access to manage access to PeopleSoft'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 PeopleSoft affects the Select Access components.
- **PeopleSoft**—Ensures that you understand how integration with Select Access affect the PeopleSoft.
- **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 PeopleSoft, you may want to begin by familiarizing yourself with the contents of the following documents:

- *HP OpenView Select Access 6.0 Installation Guide*, © Copyright 2001-2004 Hewlett-Packard Development Company, L.P. (`installation_guide.pdf`)
- *HP OpenView Select Access 6.0 Network Integration Guide*, © Copyright 2001-2004 Hewlett-Packard Development Company, L.P. (`network_integration_guide.pdf`)
- *HP OpenView Select Access 6.0 Policy Builder Guide*, © Copyright 2001-2004 Hewlett-Packard Development Company, L.P. (`policy_builder_guide.pdf`)
- *HP OpenView Select Access 6.0 Developer's Tutorial Guide*, © Copyright 2004 Hewlett-Packard Development Company, L.P. (`dev_tut_guide.pdf`)
- *HP OpenView Select Access 6.0 Developer's Reference Guide*, © Copyright 2004 Hewlett-Packard Development Company, L.P. (`dev_ref_guide.pdf`)
- Hewlett-Packard, Application/portal servers *Integration Papers*, © Copyright 2001-2004 Hewlett-Packard Development Company, L.P.

2 Technologies overview

This chapter introduces you to Select Access and PeopleSoft. It gives you an overview of the products, what they do, what components are installed with these products, and what PeopleSoft integration issues exist. This integration is targeted at PeopleSoft applications running on the PeopleTools 8.42 platform.

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.

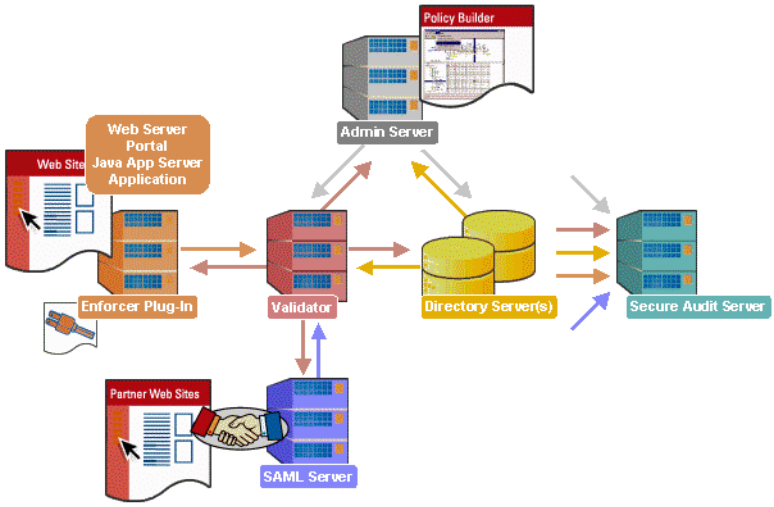

Figure 1 Select Access system architecture

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 is PeopleSoft?

PeopleSoft is one of the largest enterprise application software companies in the world. They offer a broad range of applications including Human Resource Management, Manufacturing, Customer Relationship Management, Real Estate, Analytics, Financial Management, Supplier Relationship Management, Distribution, and Asset Management.

This integration is targeted at PeopleSoft applications running on the PeopleTools 8.42 platform.

How does SSO integration work with PeopleSoft?

You achieve single sign-on (SSO) by employing the following components:

- *The Enforcer plugin*—This plugin handles the authentication process by creating and passing a HTTP header variable to the PeopleSoft application server. HTTP headers are typically used to enable personalization. However, with PeopleSoft they are also used to gain SSO functionality across these two systems and thereby share a single user source.
- *A proxy server*—A Web server used to host the Enforcer plugin and allows the plugin to approve and deny access requests to the PeopleSoft applications.
- *The PeopleSoft application server*—You configure this server to trust Select Access as its third-party authentication system. You must use `SignOn PeopleCode` to extract a user ID from the HTTP header variable and log into the PeopleSoft application as the desired user.

The authentication process using PeopleSoft

PeopleSoft with Select Access authentication follows a similar authentication process to that of a standalone deployment of Select Access. The process is triggered by a resource request:

`http://<psoft_server_name>/psp/ps/?cmd=start`

Select Access issues a prompt with a login form to enter specific credentials. In the case of a certificate server, a certificate is installed in the browser instead and no login form appears. If the user enters correct credentials, Select Access allows the HTTP request to proceed to the PeopleSoft server.

In addition to the steps described in *The authentication process using PeopleSoft* on page 10, two additional steps are required after a policy decision is returned to the Enforcer plugin. These steps are described and illustrated below, as shown in Figure 2.

1. The PeopleSoft server receives the HTTP header and signs in with a default user ID. The `SignOn PeopleCode` verifies the default user has been logged in and obtains the proper user ID and/or possibly other personalization information from the HTTP header.
2. The PeopleSoft server contacts the database with the information obtained from Select Access and logs the user into the application.

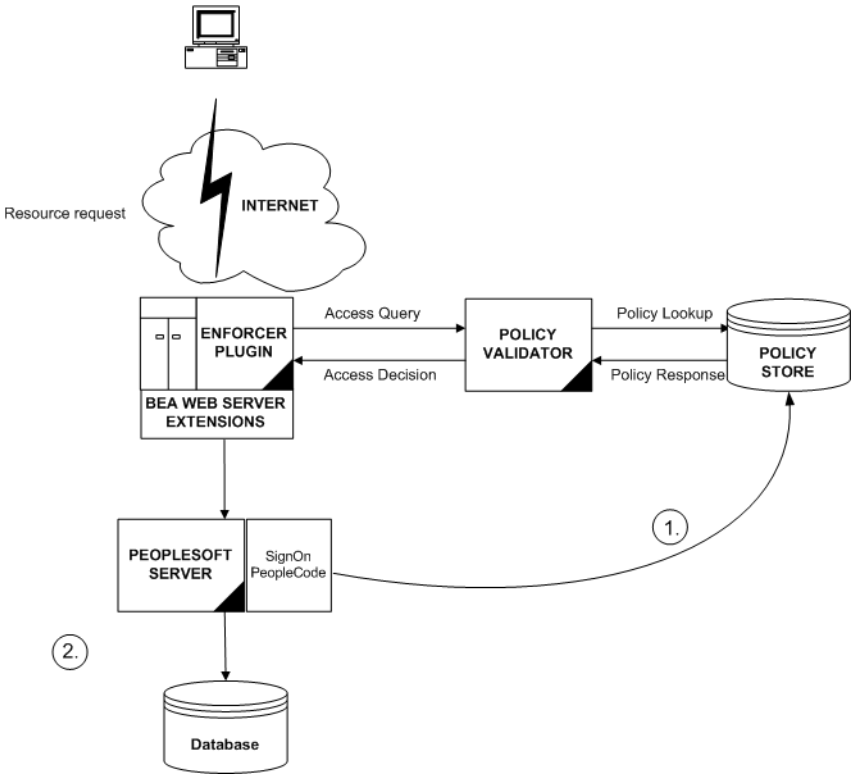

Figure 2 Select Access and PeopleSoft architecture overview

Issues that affect PeopleSoft

There are three main issues you need to consider:

- *Access policies*—Select Access's policies should only be used for controlling access. Since Select Access's policies are easier to manage and more robust, you should require users to log onto PeopleSoft through Select Access. PeopleSoft's internal security is still used to control the user's access to application menus.
- *SSO*—SSO is the cornerstone of integrating Select Access and PeopleSoft. For SSO to work with Select Access and PeopleSoft, you need to configure SSO on both products and enable and configure personalization on Select Access. Personalization is a function of authentication and therefore depends on using user attributes to tailor networked content for each customer, supplier, employee, vendor, and so on. Select Access creates the `SSO_PSFT_USER` HTTP header variable, which is essential for SSO to work.

The benefits of Select Access's solution

Integrating Select Access with PeopleSoft offers the following main benefits:

- *Consolidated policy management*—Using only Select Access, you can set all the policies and resources for your corporate site. Using only one policy management tool makes policy administration easier.
- *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.
- *Multiple authentication methods*—Select Access's multiple authentication methods (digital certificates, RADIUS, SecurID, and password authentication) extend PeopleSoft's security architecture. This allows administrators to do the following:
  - Tier security based on the sensitivity of the resource.
  - Use more than one authentication method to create a more secure multi-authentication mechanism.

3 Integrating Select Access with PeopleSoft

To integrate PeopleSoft with Select Access, your system must meet the minimum hardware and software requirements outlined below.

- *Hardware*—Refer to the PeopleSoft and Select Accesss documentation for details on client and server hardware requirements.
- *Software*—HP recommends the following software combinations to make PeopleSoft and Select Access integration possible:
  - One of the following Web servers: Microsoft IIS 5.0 on Windows 2000 or Sun ONE Web server 4.0 or Apache on other platforms.
  - Microsoft SQL 2000 or any PeopleSoft-supported databases.
  - Any one of the directory servers that is supported by Select Access.

Configuring PeopleSoft

Table 1 outlines the steps you must perform when setting up PeopleSoft to work with Select Access.

Table 1 Setting up PeopleSoft

This step...	For details, see...
Step 1: Configure BEA Weblogic to use a proxy server. This allows PeopleSoft to run through a Web server, which is necessary for Select Access to protect it.	BEA Weblogic documentation
Step 2: To share a common user base with Select Access, configure either of the following in the directory server: • PeopleSoft user IDs. • Information that allows the system to determine the database location of the PeopleSoft user ID in the directory server.	PeopleSoft documentation and Directory documentation
Step 3: Configure third-party authentication and implement the necessary `Signon PeopleCode`. This allows user credentials and attributes to be synchronized between both systems and provides single-signon (SSO) between PeopleSoft and your other applications.	*Configuring third-party authentication* on page 14
Step 4: Perform the steps required to configure Select Access.	*Setting up Select Access* on page 16

Configuring third-party authentication

Configuring third-party authentication on PeopleSoft allows Select Access to log into the system as the default user. This prevents users from logging into PeopleSoft applications multiple times.

The Select Access Enforcer plugin passes the HTTP header variable to PeopleSoft. PeopleSoft uses the values in this parameter to log into PeopleSoft as the appropriate user.

If there is another Web resource protected by Select Access, the same user is not required to reauthenticate since SSO is enabled. The user is automatically passed to the protected Web application and can go between PeopleSoft and other Web applications without logging in again.

PeopleSoft's system timeout values are still in effect. If you have been idle, your session will close. Login is then required.

To configure SSO for Select Access in PeopleSoft

1. Create a default PeopleSoft user with no roles or user permissions. This user will be used to log into PeopleSoft automatically by the system once you are authenticated by Select Access.
2. Enable remote authentication by setting the `ByPassSignOn` setting in the `configuration.properties` file to `true`. By default, this file is installed to:

   `...\bea\wlserver6.1\config\peoplesoft\applications\PORTAL\psftdocs\ps`
3. Store the default user ID and password described in step 1 in this file. For example:

   ```
   defaultUSERID=select_access
   defaultPWD=ekdJl3838**&^^%kdjflsdkjfJHJIK
   ```
4. Save the changes in this file.
5. Create a `Signon PeopleCode` program that extracts the header information provided by Select Access and logs the user into PeopleSoft.

   You can add this program with PeopleSoft's Application Designer, by modifying the `PeopleCode` associated with the `FUNCLIB_LDAP` record. Code example gives an example of a program that extracts the PeopleSoft user name from the HTTP header `SAUSER`.

This code sample is for a system with an IIS proxy server. Select Access's Personalization feature varies from server-to-server because of differences among the different server types. For details on your specific deployment, see Chapter 6, Using Personalization Attributes: the Personalization API, in the *HP OpenView Select Access 6.1 Developer's Tutorial Guide*.

6. Enable `Signon PeopleCode` to run:
   a. Click **PeopleTools> Security>Security Objects>Signon PeopleCode**.
   b. Add the new program you created in step 5 to the security objects for PeopleSoft.
   c. Check the **Enabled** box.
   d. If applicable, uncheck the **Exec Auth Fail** box to ensure the application only runs when Select Access successfully logs in with the default user.

Sample Signon PeopleCode program

```
Function SelectAccess_Authentication()

    /* Make sure code is only applied to logons using the default user. */
   If Upper(%SignonUserId) = Upper("select_access") Then
      &pslogin_userID = %Request.GetHeader("SAUser");
      If &pslogin_userID <> "" Then
         &UserID = &pslogin_userID;
         SetAuthenticationResult( True, &UserID, "", False);
      Else
         SetAuthenticationResult( False, &UserID, "", False);
      End-If;
```

```
   End-If;
End-Function;
```

Configuring Select Access

Table 2 outlines the steps you must perform when setting up Select Access to work with PeopleSoft.

Table 2 Setting up Select Access

This step...	Details on how to do it...
Step 1: Install and configure a Select Access Enforcer plugin for the Web server. **Note:** This step assumes that a Select Access Administration server and Policy Validator are already installed and configured, and running on your network.	1 Run the 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 Web server that you are using in conjunction with PeopleSoft. Choose a **Custom** configuration. 4 Enable SSO by configuring the setup screens accordingly, depending on whether you are deploying PeopleSoft across a single domain, multiple domains or virtual domains. For details, see Chapter 8, *Configuring the Enforcer Plugins* of the *HP OpenView Select Access 6.0 Installation Guide*. 5 Accept the defaults for all the other Select Access custom installation screens. 6 Check the following two boxes: — Update Web server configuration to load the Enforcer plugin — Restart Web server 7 Click **Finish**. For details, see Chapter 8, *Configuring the Enforcer Plugins* in the *HP OpenView Select Access 6.0 Installation Guide*.
Step 2: Protect the PeopleSoft proxy server.	1 Ensure you have configured an Enforcer plugin for this server. It is required to protect all PeopleSoft resources a user might try to access. **Note:** Users should use the following URL as their PeopleSoft access point: `<server_name>/psp/ps/?cmd=start` PeopleSoft's native login page should not be used. 2 Right-click a folder or the root of the Resources Tree. 3 Click **New>Service**. 4 Configure the **New Service** dialog box as required. For details, see Chapter 3, *Building your Identities and Resources Trees*, in the *HP OpenView Select Access 6.0 Policy Builder Guide*

Table 2 Setting up Select Access

This step...	Details on how to do it...
Step 4: Configure your authentication server to authenticate the PeopleSoft user and forward the HTTP header, which contains the PeopleSoft User ID, to the Enforcer plugin. This component, in turn, forwards the header to the PeopleSoft server. Since PeopleSoft third-party authentication is configured, the user contained in the HTTP header gets logged in. Configuring SelectID for PeopleSoft's resources requires two things: • Configuring an appropriate combination of authentication servers based on the level of security you require. • Enabling and configuring personalization.	1 On the SelectID column, enable SelectID for the PeopleSoft proxy server. The **Authentication Properties** dialog box appears. For details on SelectID, see *Certificate Authentication Service* on page 115 in the *HP OpenView Select Access 6.0 Policy Builder Guide*. 2 Click the **Authentication** tab and do the following: a If you have already configured some authentication servers listed, click **Add**. The **Available Authentication Servers** dialog box appears. b To configure a combination of authentication servers required by the PeopleSoft resources, select one or more server names from the list of **Available Servers** and click **Add.** The server names appear in the **Selected Servers** window. To reorder the servers, select a server in the **Selected Servers** list and click the up arrow or down arrow buttons. c Click **OK**. OR a If you have never created any authentication servers, click **Servers.** The **Authentication Servers** dialog box appears. b Click **Add**. The **Authentication Method** dialog box appears. c In the **Server Name** field, enter a name for the server. The name must contain at least two characters. d In the **Authentication Methods** group, determine what method the server uses to authenticate users and then click **OK** to configure the server properties for the corresponding authentication server. **Note:** With this configuration, you are controlling access to PeopleSoft via the service entry. All resources, therefore, inherit this access policy. You can restrict access to individual components if you manually add each resource as a URL, and then configure SelectID accordingly.

Table 2 Setting up Select Access

This step...	Details on how to do it...
	3 Click the **Personalization** tab and do the following: a On the **User Data** tab, check the **Store user attributes in** box to export the user's activated attributes to environment variables. b Click **Add**. **Note:** Activate attributes otherwise they cannot be exported. a In the **Directory Attribute Name** column, activate the attribute (usually `uid` or `cn`) used to determine what personalized content is viewed by the user. b For each activated attribute, enter the corresponding **Environment Variable Name** that it is to be exported to. For example, you could export the common name (CN) field to the variable `USER`. This would appear as `SAUSER` on IIS or as `SA_USER` on other systems c Click **OK** to finish. For details on enabling personalization, see Chapter 5, *Authentication Basics: Select Auth & Personalization* in the *HP OpenView Select Access 6.0 Policy Builder Guide*. **Note:** If you are using IIS, you need to install an updated version of the IIS plugin that supports HTTP headers.