# HP OpenView Select Access

## Integration Paper for Siebel 7.0.4

**Software Version: 5.2**

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


**October 2003**

# 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.

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

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

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

## Trademark Notices

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

## Support

Please visit the HP OpenView Select Access web site at:

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

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

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

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

The support site includes:

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

# Contents

# Chapter 1
# About this Integration Paper

## What is it about?

This Integration Paper describes how to integrate Siebel 7.0.3 with HP OpenView Select Access.

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

**Table 1:** Integration Paper overview

| This chapter ... | Covers these topics... |
|---|---|
| Chapter 2, *Technologies overview* | • Introduces HP OpenView Select Access: what it is, what it does, and how it works.<br>• Introduces Siebel 7: what it is and what integration issues exist. |
| Chapter 3, *Integration issues* | Describes what you need to do with Siebel 7 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 Siebel 7.
- Using Select Access to manage access to Siebel 7's resources.

## What does it assume you already know?

This Integration Paper assumes a working knowledge of:

- ***HP OpenView Select Access*** — Ensures that you understand how integration with Siebel 7 affects the Select Access components.

- ***Siebel 7*—**Ensures that you understand how integration with Select Access affect the Siebel 7.
- ***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 Siebel 7, you may want to begin by familiarizing yourself with the contents of the following documents:

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

# Chapter 2
# Technologies overview

This chapter introduces you to HP OpenView Select Access and Siebel 7. It gives you an overview of the products, what they do, what components are installed with these products, and what Siebel 7 integration issues exist.

## What is Select Access?

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

## What does Select Access do?

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

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

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

### Supports single sign-on

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

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

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

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

## Enables user profiling

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

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

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

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

## Provides user password and profile management

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

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

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

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

### Delegates administration

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

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

### Provides an end-to-end auditing system

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

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

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

### Automates the discovery and maintenance of corporate resources

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

simple typing error can put the security of resources at risk) Select Access saves administrators' time and improves accuracy.

## How does Select Access work?

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

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

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

### The authentication process

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

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

## Other Select Access components

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

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

## Third-party components Select Access integrates with

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

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

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

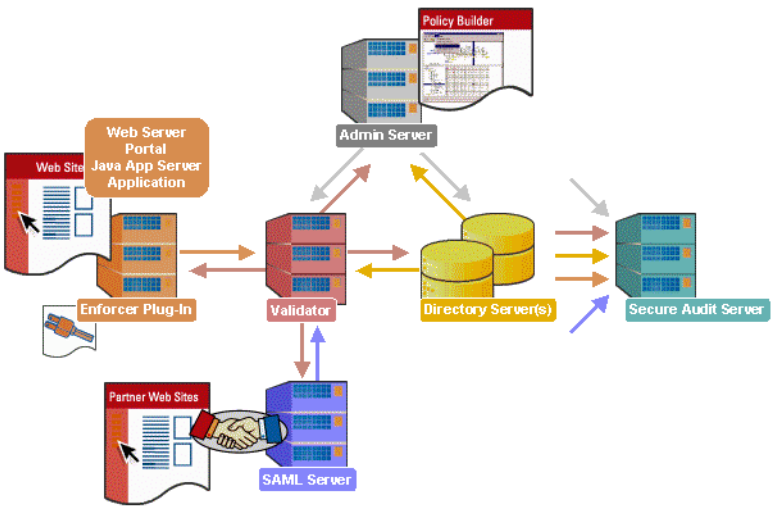



**Figure 1:** Select Access system architecture

### Custom plugins you can customize functionality with

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

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

## What is Siebel 7?

Siebel provides a comprehensive family of multichannel eBusiness applications and services. Siebel 7, one of Siebel's offerings, enables organizations to create a single source of customer information, which facilitates the servicing of customers across multiple channels, such as the Web, call centers, and dealer networks.

## How does SSO integration work with Siebel 7?

You achieve single sign-on (SSO) with Siebel 7 with the Select Access Enforcer plugin and the Siebel 7 server:

- *The Enforcer plugin*—This plugin handles the authentication process by creating and passing a HTTP header variable to the Siebel server. HTTP headers are typically used to enable personalization. However, with Siebel 7 they are also used to gain SSO functionality across these two systems and thereby share a single user source.
- *The Siebel 7 server*—This server is configured to use Siebel SSO, trusts the Select Access authentication system, and uses the HTTP header variable to log into Siebel as the user.

## The authentication process using Siebel 7

Select Access authentication and Siebel 7 with Select Access authentication follow a similar authentication process. What triggers the process is when a user requests the Siebel URL `http://<siebel_server_name>/<siebel_application>/start.swe`. 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 Siebel Web server.

`start.swe` is a file that starts the requested Siebel application. The `.swe` extension is specific to Siebel. It proxies to Siebel's server and asks for the requested Siebel application.

In addition to the steps described in *The authentication process* on page 6, 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 Siebel server receives the HTTP header and trusts the third-party authentication system due to SSO configuration. The security adapter verifies the Siebel SSO trust token sent by the Siebel Web Server Extensions (SWSE) and obtains the database account and possibly roles information from LDAP for the specific user.
2. Siebel contacts the database with the information obtained from LDAP and logs the user into the application.

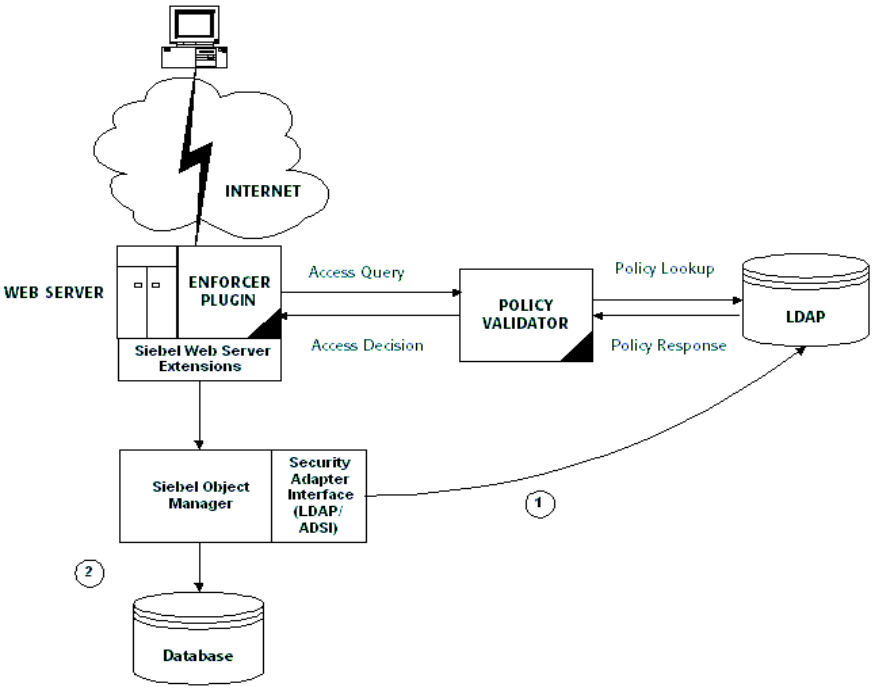



**Figure 2:** Select Access and Siebel 7 architecture overview

## Issues that affect Siebel 7

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 need to disable Siebel 7's security policies. Enabling Siebel SSO overrides Siebel 7's security policies and lets Select Access take over.

Create access policies against any files that you need to protect from user access.

- *SSO*—SSO is the cornerstone of integrating Select Access and Siebel 7. For SSO to work with Select Access and Siebel, 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_SIEBEL_USER` HTTP header variable, which is essential for SSO to work.

## The benefits of Select Access's solution

Integrating Select Access with Siebel 7 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 Siebel 7'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.

# Chapter 3
# Integrating Select Access with Siebel 7

To integrate Siebel 7 with Select Access, your system must meet the minimum hardware and software requirements outlined below.

- *Hardware*—Refer to the Siebel and Select Accesss documentation for details on client and server hardware requirements.
- *Software*—HP recommends the following software combinations to make Siebel 7 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 Siebel-supported databases.
  - One of the following directory servers that are supported by both Select Access and Siebel 7: Netscape Directory Server, Microsoft Active Directory

## Configuring Siebel 7

Table 1 outlines the steps you must perform when setting up Siebel 7 to work with Select Access.

**Table 1:** Setting up Siebel 7

| This step... | For details, see... |
|---|---|
| ***Step 1:*** Install the following Siebel v7 components:<br>• Siebel Gateway Server<br>• Siebel Web Server Extensions<br>• Siebel Database Server<br>• Siebel Application Server<br>• Siebel Call Center<br>**Note:** Ensure you use the fully qualified name for all hostname settings or the Siebel server does not run properly. | A combination of the following guides:<br>*Siebel 7 Installation Guide*<br>*Siebel 7 Release Notes*<br>*Siebel Supported Platform Guide* |
| ***Step 2:*** Configure Siebel 7 to use the Siebel Web Server Extensions. This allows Siebel 7 to run through a Web server, which is necessary for Select Access to protect it. | *Siebel 7 Server Installation Guide* |
| ***Step 3:*** To share a common user base with Select Access, configure Siebel 7 to use Siebel LDAP or ADSI security adapter. | *Siebel 7 Authentication and Access Control Administration Guide* |
| ***Step 4:*** Perform the steps required to configure Select Access. | Table 2, *Setting up Select Access* on page 16 |
| ***Step 5:*** Configure Siebel SSO and personalization for the Siebel applications. This allows user credentials and attributes to be synchronized between both systems and overrides Siebel's security policies with Select Access's. | *The importance of configuring SSO on Siebel 7* on page 14 |
| ***Step 6:*** Configure Siebel Tools to prevent the user from being redirected to a standard Siebel login page upon logout. | *To configure SSO for Siebel* on page 15 |

### The importance of configuring SSO on Siebel 7

Configuring SSO on Siebel 7 allows Select Access to log into the system as the user. This prevents users from logging into Siebel 7 applications multiple times.

The Select Access Enforcer plugin passes the HTTP header variable SSO_SIEBEL_USER to Siebel. Siebel 7 uses the values in this

parameter to determine the custom applets and views the SSO user can view from his browser.

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 Siebel and other Web applications without signing on again until he clicks the logout button. The logout button prompts the Select Access conditional logout rule that deletes the Select Access cookie and fully logs out the user.

### To configure SSO for Siebel

1. Enable SSO for the specific application in the `eapps.cfg` file. When configuring Siebel SSO for Select Access, you need to add the following four lines:

   ```
   SingleSignOn = TRUE
   TrustToken = <shared_secret>
   UserSpec = SSO_SIEBEL_USER
   UserSpecSource = Header
   ```

2. Enable SSO for the specific application in its configuration file. For example, if the application is called eService, the name of this application's configuration file would be `eservice.cfg`. Add the following lines:

   ```
   SingleSignOn = TRUE
   TrustToken = <shared_secret>
   ```

Ensure the shared secret is the same in both files or SSO does not work.

## Configuring Siebel Tools

You need to configure Siebel Tools to ensure that when the user clicks the **Logout** button, the default Select Access login page appears instead of to the standard Siebel login page.

Change the `Logoff Acknowledgement Page` parameter for each Siebel application that is Select Access-protected. For details, see the Siebel Tools Reference guide.

## Configuring Select Access

Table 2 outlines the steps you must perform when setting up Select Access to work with Siebel 7.

**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.<br><br>**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.<br>2. Click **Next** until you reach the **Choose HP OpenView Select Access components** installation screen.<br>3. Install and configure the Enforcer plugin on the Web server that Siebel 7 is using. Choose a **Custom** configuration.<br>4. Enable SSO by configuring the setup screens accordingly, depending on whether you are deploying Siebel 7 across a single domain, multiple domains or virtual domains. For details, see *To perform a Custom Enforcer plugin configuration* on page 128 of the *HP OpenView Select Access v5.2 Installation Guide*.<br>5. Accept the defaults for all the other Select Access custom installation screens.<br>6. Check the following two boxes:<br>— **Update Web server configuration to load the Enforcer plugin**<br>— **Restart Web server**<br>7. Click **Finish**.<br>For details, see Chapter 8, *Configuring the Enforcer plugins* in the *HP OpenView Select Access v5.2 Installation Guide*. |
| ***Step 2:*** Add Siebel 7 to the Resources Tree as a service branch. | 1. Right-click a folder or the root of the Resources Tree.<br>2. Click **Run Discovery>Services.** The **Discover Networks Services** dialog box appears.<br>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 v5.2 Policy Builder Guide*.<br>**Note:** For details on performing this procedure manually, see Chapter 4, *Building your Users and Resources Trees* in the *HP OpenView Select Access v5.2 Policy Builder Guide*. |

**Table 2:** Setting up Select Access

| This step... | Details on how to do it... |
|---|---|
| ***Step 3:*** Add the Siebel 7 resources you want to protect under the services you just created.<br>**Note:** Because the plugin cannot access `start.swe`, you have to add it manually. | 1. Make sure you have configured the network resource plugin. For details, see Chapter 4, *Building your Users and Resources Trees*.<br>2. On the Resources Tree, right-click the service you want to scan for available resources.<br>3. Click **Run Discovery>Resources**. The **Discover Network Resources** dialog box appears.<br>— 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.)<br>— 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.<br>4. Select **Run Resource Discovery Plugin** and fill in any empty fields.<br>5. Select the location on the Resources Tree to add the resources. Do the following:<br>a. Click the **Browse** button beside the **Network Resources Tree Destination** field. The **Select Resource Destination** dialog box appears.<br>b. Select a service, then click **OK**.<br>or<br>a. Select a folder or the root of the Resources Tree.<br>b. Click **New** and create a new service.<br>c. Select it in the **Select Resource Destination** dialog box, then click **OK**.<br>6. Click **OK**.<br>For details, see *Automatically generating a list with a discovery plugin* on page 41 in the *HP OpenView Select Access v5.2 Policy Builder Guide*.<br>7. Manually add `start.swe` to the services you just created.<br>For details, see *Manually adding a network resource to a service* on page 39 in the *HP OpenView Select Access v5.2 Policy Builder Guide*. |

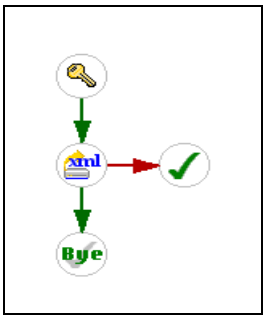
**Table 2:** Setting up Select Access

| This step... | Details on how to do it... |
|---|---|
| ***Step 4:*** You need to configure your authentication server to authenticate the Siebel user and forward the HTTP header, which contains the LDAP user's uid, to the Enforcer plugin. This component, in turn, forwards the header to the Siebel server. Since Siebel SSO is configured, the user contained in the HTTP header gets logged in.<br><br>Configuring SelectID for Siebel 7's resources requires two things:<br>• Configuring an appropriate combination of authentication servers based on the level of security you require.<br>• Enabling and configuring personalization. | 1. On the SelectID column, enable SelectID for Siebel 7's resources. The **Authentication Properties** dialog box appears.<br>For details on SelectID, see *Certificate servers* on page 113 in the *HP OpenView Select Access v5.2 Policy Builder Guide*.<br>2. Click the **Authentication** tab and do the following:<br>a. If you have already configured some authentication servers listed, click **Add**. The **Available Authentication Servers** dialog box appears.<br>b. To configure a combination of authentication servers required by the Siebel 7 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.<br>c. Click **OK**.<br>OR<br>a. If you have never created any authentication servers, click **Servers.** The **Authentication Servers** dialog box appears.<br>b. Click **Add**. The **Authentication Method** dialog box appears.<br>c. In the **Server Name** field, enter a name for the server. The name must contain at least two characters.<br>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. |

**Table 2:** Setting up Select Access

| This step... | Details on how to do it... |
|---|---|
| | 3. Click the **Personalization** tab and do the following:<br>a. On the **User Data** tab, check the **Store user attributes in** box to export the user's activated attributes to environment variables and then click **Add**.<br>**Note:** Activate attributes otherwise they cannot be exported. For details on activating attributes see Appendix A, *User directory entries and attributes* in the *HP OpenView Select Access v5.2 Policy Builder Guide*.<br>b. In the **Directory Attribute Name** column, activate the attribute (usually `uid` or `cn`) used to determine what personalized content is viewed by the user.<br>c. For each activated attribute, enter the corresponding **Environment Variable Name** that it is to be exported to. In this case, it is `SSO_SIEBEL_USER`.<br>d. Click **OK** to finish.<br>For details on enabling personalization, see Chapter 6, *Authentication fundamentals: SelectID and personalization* in the *HP OpenView Select Access v5.2 Policy Builder Guide*. |

**Table 2:** Setting up Select Access

| This step... | Details on how to do it... |
|---|---|
| *Step 5:* Create a conditional rule that contains a query logic decision point and a logout terminal point. Apply the rule to all authenticated Siebel 7 users and all Siebel 7 resources. The Siebel 7 content generally consists of HTML files, JSP files, and any links that launch java servlets. | 1. From the Rule Builder, create a conditional rule that contains the following decision and terminal points, as shown below:<br>— Query attributes<br>— Logout<br>  <br><br>**Figure 1:** Example logout rule<br>2. Add a query attributes decision point that contains the following search expression:<br>— **Query Type**: http_query_list/SWECmd<br>— **Comparison operator**: =<br>— **Query Value**: Logoff<br>For more details on this decision point, see *The evaluate query attributes decision point* on page 161 in Chapter 9, *Creating conditional access rules with the Rule Builder* of the *HP OpenView Select Access v5.2 Policy Builder Guide*.<br>3. Insert an Allow terminal point on the False branch. If the Query Type and Query Value do not match, the user remains logged in.<br>4. Add a logout terminal point beneath the query attributes decision point. This logs out the user and deletes the Select Access cookie.<br>For details on creating conditional rules, see Chapter 9, *Creating conditional access rules with the Rule Builder* in the *HP OpenView Select Access v5.2 Policy Builder Guide*.<br>5. Apply the rule to all authenticated Siebel 7 users and all Siebel 7 resources.<br>**Note:** The rules you apply are inherited across multiple resources. For details, see Chapter 8, *Controlling network access* in the *HP OpenView Select Access v5.2 Policy Builder Guide*. |