HP OpenView Select Access

Integration Paper for Plumtree Corporate Portal 4.5

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

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 Plumtree Corporate Portal with Select Access.

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

Table 1: Plumtree Corporate Portal & 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 Plumtree Corporate Portal: what it is and what integration issues exist.
Chapter 3, *Integrating Select Access with Plumtree Corporate Portal*	Describes what you need to do with both Plumtree Corporate Portal and Select Access to integrate these technologies.

Who is it for?

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

- Integrating Select Access with their Plumtree Corporate Portal.
- Using Select Access to manage access to Plumtree Corporate Portal resources.

What does it assume you already know?

This guide assumes a working knowledge of:

- ***Select Access***—Ensures that you understand how integration with Plumtree Corporate Portal affects the *Select Access* components.
- ***Plumtree Corporate Portal***—Ensures that you understand how integration with Select Access affects the Plumtree Corporate Portal components.
- ***LDAP directory servers***—Helps ensure that information in the Policy Builder is set up correctly.
- ***Web server and plugin technology***—Combinations that are used to add a specific feature or service to a larger system. This helps you understand how different components of Select Access communicate with each other and with your existing network.

Related references

Before you begin to integrate Select Access with Plumtree Corporate Portal, 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 Plumtree Corporate Portal. It gives you an overview of the products, what they do, what components are installed with these products, and Plumtree Corporate Portal integration issues.

What is Select Access?

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

What does Select Access do?

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

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

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

Supports single sign-on

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

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

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

Enables user profiling

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

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

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

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

Provides user password and profile management

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

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

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

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

Delegates administration

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

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

Provides an end-to-end auditing system

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

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

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

Automates the discovery and maintenance of corporate resources

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

How does Select Access work?

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

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

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

The authentication process

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

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

Other Select Access components

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

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

- *Secure Audit server*: Collects and manages incoming log messages from Select Access components on a network.

Third-party components Select Access integrates with

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

- *Directory server – LDAP v3.0 compliant*: is the foundation of a Select Access-protected system. It acts as the repository of information. Depending on how you have set up your directory system, Select Access can use one or more directory servers to store:
  - A single policy data location
  - One or more user data locations
- *Web/Application/Portal/Provisioning servers*: are third-party technologies that use Select Access as their authorization and access management system. Depending on your server technology, you can use Select Access's native SSO and/or personalization solution rather than use the server's built-in alternative for a more robust solution.

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

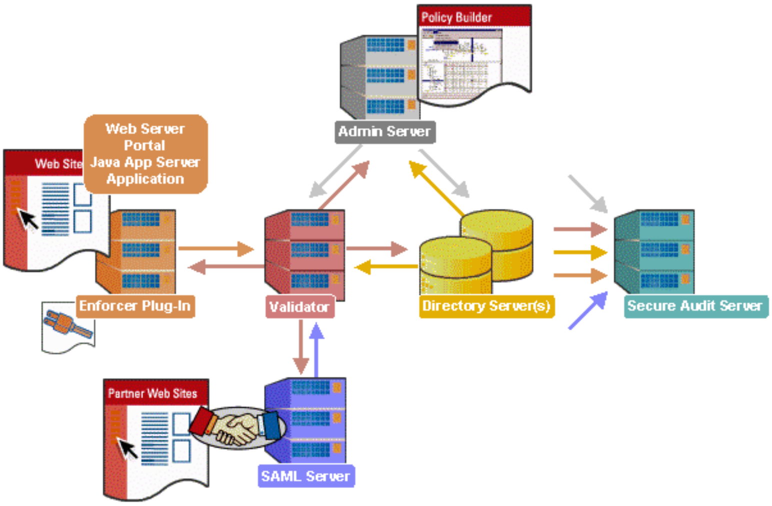


Figure 1: Select Access system architecture

Custom plugins 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 Plumtree Corporate Portal?

Plumtree Corporate Portal centralizes access to information and applications for employees and customers. It has a directory of links to Web pages, documents and reports, and gadgets. Plumtree brings a wide range of electronic resources together on a single Web platform, allowing you to project a complete view of your business across the extended enterprise. Plumtree Corporate Portal is available for both Windows NT/2000 and Sun Solaris platforms.

Issues that affect Plumtree Corporate Portal

Because data needs to be synchronized between Select Access and Plumtree Corporate Portal, there are three main issues you need to consider. The following issues affect both Plumtree Corporate Portal and Select Access, which requires that you make specific configurations on each:

- *Single sign-on*—You need to delegate Select Access as Plumtree Corporate Portal's SSO vendor. That way, users only need to authenticate once to access local or remote resources, including gadgets, depending on the policy that you assign.
- *Plumtree Gadget Web Services*—When integrating Select Access with Plumtree Corporate Portal, you need to protect gadgets with appropriate policies.

- *User data*—When integrating Select Access with Plumtree Corporate Portal, administrators need to remember the following:
  - Export all your Plumtree Corporate Portal users to your LDAP directory server so each data source shares the same set of user entries.
  - Synchronize the Plumtree Corporate Portal user database with Select Access so that user data can still determine what personalized data they see.

For details, see *Setting up Select Access to integrate with Plumtree Corporate Portal* on page 11 and *Setting up Plumtree Corporate Portal to integrate with Select Access* on page 17.

The benefits of Select Access' solution

Integrating Select Access with Plumtree Corporate Portal offers many benefits:

- **Authentication types**—Select Access offers a wide variety of authentication types that are configured centrally for one or many applications.
- **Decision/Policy criteria points**—Select Access offers a fine granularity of policy for control of both network resource access and administrative access.
- **Consolidated policy management**—You can set all the policies for your corporate site using only Select Access. Using only one policy management tool makes policy administration easier.
- **Single sign-on (SSO)**—This key technology is required for distributed systems like Plumtree Corporate Portal. SSO is an 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. SAML-based single sign-on is also enabled with Select Access.
- **Personalization**—Once authenticated, the portal can display personalized content to a user which is sent to it by Select Access.
- **Auditing & Alerts**—Select Access offers centralized auditing and real-time alerts.
- **Security**—Select Access was built as a security product. Security comes first, whereas a portal server is a functional product. Compliance with security standards and best practices comes as an afterthought.

Chapter 3

Integrating Select Access with Plumtree Corporate Portal

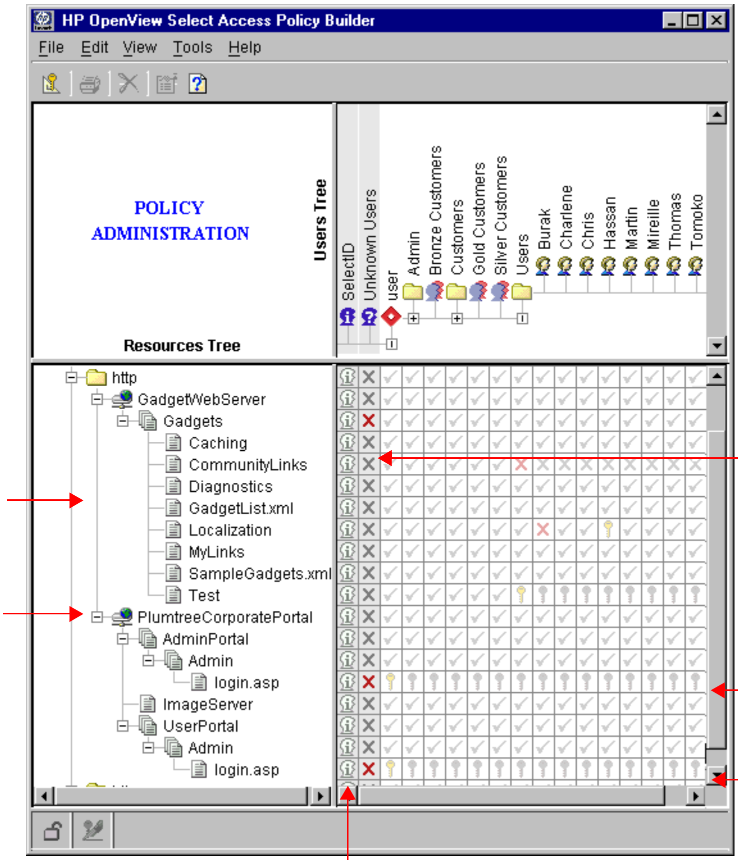
There are two sides to integration:

- Select Access requires specific settings to enable SSO, add Plumtree Corporate Portal services and resources, enable personalization, and set access policies against Plumtree Corporate Portal’s content.
- Plumtree Corporate Portal needs to be configured so it can delegate SSO functions to Select Access, differentiate between Select Access and Plumtree Corporate Portal users, and delegate authentication responsibility to Select Access.

For details, see the corresponding section that follows.

Setting up Select Access to integrate with Plumtree Corporate Portal

Setting up Select Access with Plumtree Corporate Portal not only requires that you use products features, but it also requires that you make custom settings to get Select Access to integrate and function with Plumtree Corporate Portal successfully. Table 1 describes the steps you need to take to set up Select Access with Plumtree Corporate Portal. When you are finished, your Policy Matrix might look similar to the one shown in Figure 1.



Plumtree Corporate Portal services and resources are added to the Policy Matrix's Resources Tree.

Access denied to Unknown Users to remote gadget resources, requiring them to be authenticated.

A logout user terminal point in a conditional rule forces users to log out of a shared machine so subsequent users cannot take advantage of the session cookie.

SelectID is enabled for all resources to ensure users are authenticated before they gain access to resources. Enabling SelectID also ensures the Select Access username environment variable is passed to Plumtree Corporate Portal via personalization.

Figure 1: Example Policy Matrix

Table 1: Setting up Select Access to work with Plumtree Corporate Portal

This step...	Details on how to do it...
Step 1: Add your Plumtree Corporate Portal users to your LDAP directory server.	1. Replicate all user entries to an LDAP directory server. This ensures both data sources have the same user set. 2. Ensure you add this Plumtree Corporate Portal-specific user location as a branch on your Users Tree. For details, see Chapter 4, *Building your Users and Resources Trees* in the *HP OpenView Select Access 6.0 Policy Builder Guide*.
Step 2: Install an Enforcer plugin on each machine that hosts a Web-based Plumtree Corporate Portal component.	1. Run the Select Access installer. 2. Click **Next** until you reach the **Choose Select Access components** installation screen. 3. Install and configure one of the following Enforcer plugins on each Plumtree Corporate Portal host: — Apache Enforcer plugin — IIS Enforcer plugin— The Windows version of Plumtree Corporate Portal supports versions 4.0 and 5.0 with Microsoft Transaction Server or COM+. — Sun ONE (iPlanet) Enforcer plugin For details, see the *HP OpenView Select Access 6.0 Installation Guide*.

Step 3: Edit your `enforcer.conf` file for your plugins to enable SSO.	To configure SSO,
	1. On the server where the Enforcer plugin is installed, copy this file:
	`C:\Program Files\HP OpenView\Select Access\conf\enforcer.conf-nt.example`
	to:
	`C:\Program Files\HP OpenView\Select Access\bin\enforcer.conf`
	2. Modify the following parameters as needed:
	— `cookie_domain`
	— `protected_domain`
	Note: To configure M-D SSO, you need to modify the `enforcer.conf` files on Web servers, so that they all share a mutually inclusive list of protected domains that allows analogous M-D SSO, register all Policy Validators with the same directory server, and ensure distributed Web servers use the same authentication method.
	For details, see Chapter 8, *Enabling single sign-on* in the *HP OpenView Select Access 6.0 Network Integration Guide*.

Table 1: Setting up Select Access to work with Plumtree Corporate Portal

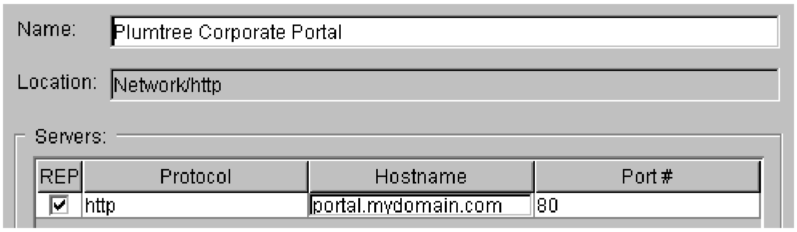
This step...	Details on how to do it...
Step 4: Add your Plumtree Corporate Portal services so they are added to the Resources Tree. Since the number of services are known, you can manually create them.	1. Right-click a folder or the root of the Resources Tree. 2. Click **New>Service**. The **New Service** dialog box appears. 3. In the **Name** field, enter a name for the local or remote service to be used on the Resources Tree. For example, if you are creating a service for Plumtree Corporate Portal, you could use the host machine's name to describe the service. 4. Click **Add** and configure the **REP**, **Protocol**, **Hostname**, and **Port** cells as needed, as shown in the figure below.  Name: Plumtree Corporate Portal Location: Network/http Servers: REP | Protocol | Hostname | Port # ☑ | http | portal.mydomain.com | 80 **Note:** To automate this procedure, perform step 1 and then click **Run Discovery>Services.** 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*.
Step 5: Due to limitations of the built-in HTTP/HTTPS plugin, you need to manually add the resources you want to protect under the services you just created.	1. Right-click the service under which you want to add resources. 2. Click **New>Resource**. The **New Resource** dialog box appears. 3. In the **Name** field, type in the name of the resource you want to protect. 4. Click **OK.** **Note:** Since the number of Plumtree Corporate Portal resources you have may be extensive, you may want to automate the discovery of them. 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*.

Table 1: Setting up Select Access to work with Plumtree Corporate Portal

This step...	Details on how to do it...
Step 6: Define the environment variable required to transfer data to Plumtree Corporate Portal. Not only does personalization allow a user to authenticate once, but, once authenticated, your Plumtree Corporate Portal can display personalized content to that user. For additional details on how Select Access supports personalization, see Chapter 6, *Authentication fundamentals: SelectID and personalization* in the *HP OpenView Select Access 6.0 Policy Builder Guide*. **Note:** The last decision point with personalization configured determines which environment variables and their corresponding set of attributes are used.	1. Enable SelectID for all resources to ensure the Select Access username environment variable is passed to Plumtree Corporate Portal via personalization. For details, see Chapter 7, *Setting up authentication servers* in the *HP OpenView Select Access 6.0 Policy Builder Guide*. **Note:** For SSO to work, you must define the same authentication server for SelectID for local and remote Plumtree Corporate Portal resources. 2. In the **Authentication Properties** dialog box, click the **Authentication** tab and select which authentication server you want to use to authenticate users. For details, see Chapter 7, *Setting up authentication servers*. 3. Click the **Personalization** tab. This tab contains three subtabs that export data from Select Access' directory server into the environment variables required to generate dynamic, personalized Plumtree Corporate Portal content. 4. Click the **User Data** tab. This tab allows you to define the variable that is used to export user data to Plumtree Corporate Portal's database. 5. Check the **Store user attributes in** box. 6. Click and type `cn` in the **Directory Attribute Name** cell. **Note:** This attribute must be activated otherwise it cannot be exported. For details on activating attributes see Appendix A, *User directory entries and attributes* in the *HP OpenView Select Access 6.0 Policy Builder Guide*. 7. Click and type `SA_USERNAME` in the **Environment Variable Name** cell and then click OK. **Note:** You can define other environment variables to export the user data that is required to determine which personalized data is displayed.

Table 1: Setting up Select Access to work with Plumtree Corporate Portal

This step...	Details on how to do it...
Step 7: Set up an authentication server.	Enter the authentication server you want to use with Plumtree Corporate Portal in the **Authentication Servers** dialog box. The Policy Builder allows you to enter five 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 8: Set your access policies against Plumtree Corporate Portal's content.	1. For users that only exist in the Plumtree Corporate Portal database, allow access for Unknown Users for `login.asp`. 2. When the user clicks the **Login as a different user** link, she logs in via Plumtree Corporate Portal's login page instead of one of Select Access's forms. 3. If you want to create policy for users that only exist in a directory server used by Select Access, you need to also: a. Create a conditional logout rule. For details, see the *HP OpenView Select Access 6.0 Policy Builder Guide*. b. Apply the logout rule against the `login.asp` resource and apply it to all users in the Policy Matrix. The user can now log on as a different user and be re-authenticated. Ensure that you have modified `login.asp` as described in Code example 2. 4. Set allow, deny, and conditional rules on remaining resources as needed. For details, see Chapter 8, *Controlling network access* in the *HP OpenView Select Access 6.0 Policy Builder Guide*. **Note:** The rules you apply are inherited across multiple resources. Ensure you understand how policies are inherited.

Setting up Plumtree Corporate Portal to integrate with Select Access

You need to perform specific configuration steps on Plumtree Corporate Portal. Table 2 describes what you need to do to synchronize data between Select Access and Plumtree Corporate Portal.

Table 2: Setting up Plumtree Corporate Portal to work with Select Access

This step...	Details on how to do it...
Step 1: Modify parameters in the `config.xml` file to: • delegate SSO functions to Select Access • differentiate between Select Access and Plumtree Corporate Portal users.	1. Open the `config.xml` file in the following location: `<install_path>\4.5\PortalPages` where `<install_path>` is the location where Plumtree is installed. 2. Modify the parameters listed in Table 3. 3. Save the `config.xml` file and restart your Web server. When you have finished making changes to the `config.xml` file, your file looks similar to Code example 1.
Step 2: Modify the `login.asp` file.	1. Open the `login.asp` file in the following location: `<install_path>\4.5\PortalPages\PortalPages\admin`. 2. Add the lines shown in Code example 2 immediately below the following tag that starts the script: `<%Response.Expires = -1`. 3. Surround the lines with comments to highlight this modification for future reference. 4. Save and close the `login.asp` file.

Table 2: Setting up Plumtree Corporate Portal to work with Select Access

This step...	Details on how to do it...
Step 3: Delegate Select Access as your SSO vendor.	1. Login to Plumtree Corporate Portal. 2. Click the **Authentication Sources** link in the left navigation and then click **Add SSO Authentication Source.** 3. Under the **General Info** section, fill out the following fields: — **Authentication Source Name:** `Select Access` — **Authentication Source Description:** `Select Access SSO` 4. Click **Next**. 5. Under the **Options** section, enter the same password, in the **SSO Password** field, that you entered on the **Single Sign-on** tab of the Plumtree Administrator Control Panel application on each portal server that uses SSO. For details, see *Integrating SSO with Plumtree* in the *Plumtree Corporate Portal Administrator's Guide.* 6. Click **Next**. 7. Under the **Synchronization Settings** section, ensure the **Authentication Only** is option is enabled and then click the **Next** button. 8. Under the **Security Settings** section, accept the defaults that appear and then click the **Finish** button.
Step 4: Synchronize the Plumtree Corporate Portal user database with Select Access.	Steps on how to set this up are beyond the scope of this document. For comprehensive information, see the section *Creating an LDAP authentication source* in the *Plumtree Corporate Portal Administrator's Guide.* **Note:** If you frequently delete or add users, HP recommends that you use the **Job Editor** to set your job to run every few minutes.
Step 5: Set up gadgets to allow Select Access to protect them.	1. Disable Plumtree Corporate Portal's login gadgets. 2. Disable remote gadget caching. This allows Select Access to protect the remote gadgets. For details, see the documentation that accompanies your remote gadgets.

Table 3: config.xml parameters

Setting...	Value and parameter...	Description...
Single sign-on	Set INTSSOVENDOR to 100. For example, the syntax would be: <I N=”INTSSOVENDOR”>100<I>	Plumtree Corporate Portal has assigned the following generic SSO vendor number: 100. **Note:** A specific vendor number will be assigned to Select Access in a future release. Contact Plumtree Corporate Portal's technical support for details.
Single sign-on	Set STRSSOCOOKIEDOMAIN to *<gadget_domain_name>* where, *<gadget_domain_name>* is the domain where you installed remote gadgets. For example, the syntax would be: <S N="STRSSOCOOKIEDOMAIN"> *<gadget_domain_name>*</S>	Together with STRSSOCOOKIEPATH, these two values are the path and domain that is used for your secure SSO cookies. The Plumtree Web server sends your secure SSO cookies to any remote gadget server whose URL matches the path and domain specified here. Be sure to include the port number in the path.
Single sign-on	Set STRSSOCOOKIEPATH to *</gadget_folder>* where, *</gadget_folder>* is the location where you installed remote gadgets. For example, the syntax would be: <S N="STRSSOCOOKIEPATH"> *</gadget_folder>*</S>	
Single sign-on	Set INTSSOCOOKIEISSECURE to 1. For example, the syntax would be: <I N="INTSSOCOOKIEISSECURE">1</I>	Tells Plumtree Corporate Portal to send cookies over an SSL connection.
Login	Set STRDEFAULTAUTHSOURCEPREFIX to SelectAccess. For example, the syntax would be: <I N=”STRDEFAULTAUTHSOURCEPREFIX”> <SelectAccess></S>	Allows Plumtree Corporate Portal to differentiate between Plumtree Corporate Portal native users and Select Access users.

Code example 1: Example `config.xml` file

```
<!-- Single Sign-on Settings -->
<I N="INTSSOVENDOR">100</I>
<!-- If you are not using SSO on this web server, then this value should be 0.
If you are using SSO, then this value should be: 1 for NT (Kerberos, NTLM,
Windows Integrated, or Basic Auth) if you imported your users from NT, 2 for
Netegrity SiteMinder, 3 for Oblix Netpoint, 4 for Securant, 5 for NT
(Kerberos, NTLM, Windows Integrated, or Basic Auth) if you imported your users
from Active Directory via LDAP, 100 or greater for a custom solution. -->
<S N="STRSSOCOOKIEPATH">/</S>
<!-- See comment below for STRSSOCOOKIEDOMAIN.-->
<S N="STRSSOCOOKIEDOMAIN">.mycompany.com</S>
<!-- This setting will be used only if you are using an SSO product. Together
with STRSSOCOOKIEPATH, above, these two values are the path and domain that
will be used for your secure SSO cookies. The Plumtree web server will send
your secure SSO cookies to any remote gadget server whose URL matches the path
and domain specified here. Be sure to include the port number in the path.-->
<I N="INTSSOCOOKIEISSECURE">1</I>
<!-- This setting will be used only if you are using an SSO product. Set this
to 1 (TRUE) if your secure SSO cookies should be sent only over a secure SSL
connection. Set this to FALSE otherwise. -->


<!-- Login Settings -->
<S N="STRDEFAULTAUTHSOURCEPREFIX">SelectAccess</S>
<!-- This is the default auth source prefix that will be prepended to the
login name when users log into your system, unless they pick another auth
source from the drop down box on the login page.  In the case of SSO, this is
the auth source category for all of your SSO users. -->
<S N="INTALLOWDEFAULTLOGINPAGEAUTHSOURCE">0</S>
<!-- This setting controls the use of the default authentication source for
non SSO portals on the Login Page and Login Gadget.  -->
<!-- 0 = (the Default Value) Don't use the default AuthSource; 1 = yes use
default Auth Sourceand hide the Auth Source Dropdown. 2= Use the default but
do not hide the drop down -->
<!-- Selecting either 1 or 2 requires that caching be turned off on the
Plumtree login Gadget or the Gadget be disabled.  -->
```

Code example 2: Additional lines required for `login.asp`

Code example 3: `<!-- #include file = "../common/securebeginpage.asp" -->`

```
<!-- #include file = "../common/DebugLogFileFns.asp" -->
<!-- Login Page Start -->
<!--START:INC\admin\login.asp-->
<%Response.Expires = -1
'SelectAccess modification begins here
If CLng(Application("intSSOVendor")) = 100 Then
Response.Redirect Application("strApplicationBaseUrl") & "sso/sso.asp"
end if
'SelectAccess modification ends here
```