HP OpenView Select Access

Integration Paper for Microsoft Outlook 2000 Web Access

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 Microsoft Outlook Web Access 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. • Introduces Microsoft Outlook Web Access: what it is and what integration issues exist.
Chapter 3, *Integration issues*	Describes what you need to do with Microsoft Outlook Web Access 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 Microsoft Outlook Web Access.
- Using Select Access to manage access to Microsoft Outlook Web Access 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 Microsoft Outlook Web Access affects the Select Access components.
- ***Microsoft Exchange Server*—**Ensures that you understand how integration with Select Access affects the server and other components like Microsoft Outlook Web Access.
- ***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 Microsoft Outlook Web Access, 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 Microsoft Outlook Web Access. It gives you an overview of the products, what they do, what components are installed with these products, and what Microsoft Outlook Web Access 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.

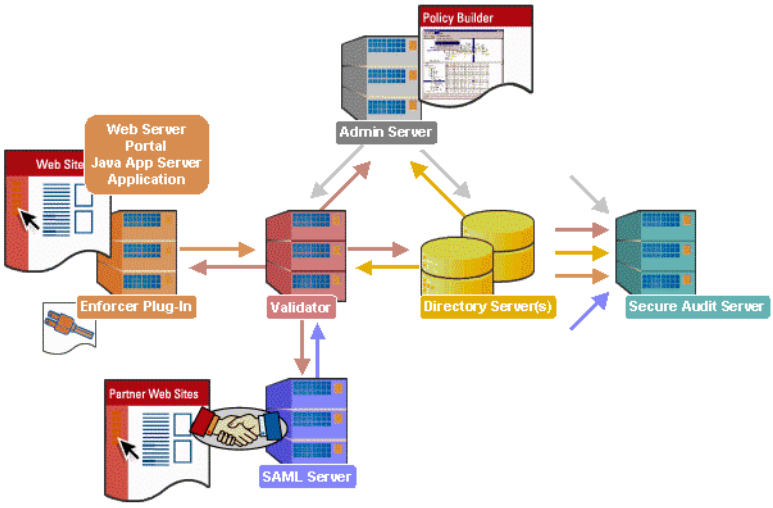

Figure 1: Select Access system architecture

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 Microsoft Outlook Web Access?

Microsoft Outlook Web Access is a feature of the Microsoft Exchange server that allows you to retrieve and work with data (usually your email) using your Web browser. The feature looks and works much like Microsoft Outlook; you can log onto your personal account to read email, send messages, create contacts, and schedule appointments.

How does authentication work on an integrated system?

When a user tries to access Web-ready Outlook content via an Internet Explorer browser, the following Select Access authentication process occurs:

1. Depending on whether the domain of the computer accessing Outlook, one of the following occurs:
   - *When the client computer is on the same domain as the Outlook server* the IIS Web server automatically detects the user's Windows credentials. This makes it unnecessary for the user to log in again.
   - *When the client computer is on the different domain than the Outlook server* the IIS Web server prompts the user for her username and password.
2. The Enforcer plugin uses these credentials and performs the action defined by the policy set in the Policy Builder.
3. Only if the policy is an Allow, does the user gains immediate access to the content.

The benefits of Select Access's solution

Integrating Select Access with Microsoft Outlook Web Access offers the following benefits:

- **Consolidated policy management**—You can set all the policies and resources for your corporate site using only Select Access. Using only one policy management tool makes policy administration easier.

- **Single sign-on (SSO)**—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 using Windows Integrated Authentication, a user's credentials act like a passport, giving users access to distributed portal content, groupware, workflow or client/server applications.

Chapter 3
Integration issues

Integrating Select Access with Microsoft Outlook Web Access requires that you perform specific actions on both the Outlook server machine as well as the Select Access system. For details, see both:

- *Configuring the Outlook host computer* on page 17
- *Configuring Select Access* on page 18

Configuring the Outlook host computer

Microsoft Outlook Web Access uses the IIS v5.0 Web server. Therefore, all configuration steps revolve around preparing that Web server for integration with Select Access. Table 1 summarizes these steps you need to perform to integrate Microsoft Outlook Web Access with Select Access.

Table 1: Preparing Outlook's IIS Web server

This step ...	Details on how to do it...
Step 1: Install and configure the IIS Enforcer plugin on Outlook's IIS Web server. **Note:** The Select Access Administration server and the Policy Validator must already be running on your network.	1. Run the Select Access installer. 2. Click **Next** until you reach the **Choose HP OpenView Select Access components** installation screen. 3. Install and configure the IIS Enforcer plugin on the Microsoft Outlook Web Access host. Choose a **Typical** installation. 4. Check the following two boxes: — **Update Web server configuration to load the Enforcer plugin** — **Restart Web server** 5. Click **Finish**. For details, see Chapter 8, *Configuring the Enforcer plugins* in the *HP OpenView Select Access v5.2 Installation Guide*.

Table 1: Preparing Outlook's IIS Web server

This step ...	Details on how to do it...
Step 2: Run the **IIS Console** and re-configure the **Authentication Methods** for all of the Exchange folders. For example, `Exchweb, Exchange, Exadmin`.	1. Display the **Authentication Methods** dialog box. For details on how to display this dialog, see the IIS Web server's documentation. 2. In the Authentication access group box, make sure you check the following boxes: — **Basic authentication** — **Integrated Windows authentication**

Configuring Select Access

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

Table 2: Setting up Policy Builder to protect Outlook's content

This step ...	Details on how to do it...
Step 1: Run Policy Builder and add your IIS Web server to the Resources Tree as a service branch.	1. Right-click a folder or the root of the Resources Tree. 2. Click **Run Discovery>Services.** The **Discover Networks Services** dialog box appears. 3. Provide the required information on the **Networks** and **Protocols** tabs and then click **OK**. For details, see Chapter 4, *Building your Users and Resources Trees* in the *HP OpenView Select Access v5.2 Policy Builder Guide*. **Note:** For details on performing this procedure manually, see Chapter 4, *Building your Users and Resources Trees* in the *HP OpenView Select Access v5.2 Policy Builder Guide*.

Table 2: Setting up Policy Builder to protect Outlook's content

This step ...	Details on how to do it...
Step 2: Add Exchange's resources you want to protect under the service you just created. Ensure you add all of the Exchange folders that you configured authentication methods for in Step 2 of Table 1. For example, `Exchweb, Exchange, Exadmin`.	1. Make sure you have configured the network resource plugin. For details, see Chapter 4, *Building your Users and Resources Trees*. 2. On the Resources Tree, right-click the service you want to scan for available resources. 3. Click **Run Discovery>Resources**. The **Discover Network Resources** dialog box appears. — Information about the service's representative server is entered automatically in the **Protocol**, **Hostname**, and **Port Number** fields. (This information is taken from the service's properties.) — If you have configured a plugin for the protocol used by the service, the plugin's configuration details are entered automatically in the **Plugin Settings** field. 4. Select **Run Resource Discovery Plugin** and fill in any empty fields. 5. Select the location on the Resources Tree to add the resources. Do the following: a. Click the **Browse** button beside the **Network Resources Tree Destination** field. The **Select Resource Destination** dialog box appears. b. Select a service, then click **OK**. or a. Select a folder or the root of the Resources Tree. b. Click **New** and create a new service. c. Select it in the **Select Resource Destination** dialog box, then click **OK**. 6. Click **OK**. For details, see Chapter 4, *Building your Users and Resources Trees* in the *HP OpenView Select Access v5.2 Policy Builder Guide*. **Note:** For details on performing this procedure manually, 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 Policy Builder to protect Outlook's content

This step ...	Details on how to do it...
Step 3: Manually add the Active Directory user location that Microsoft Exchange currently uses. That way, the user entries are shared by both systems.	1. Right-click the **Known Users** column and select **New>User Location** from the popup menu. The **New User Location Configuration** dialog box appears displaying the **General** tab. 2. If the user location is the same as the location of your policy data, check the **Same directory server as policy data** box, and skip to step 4. 3. If the user location is not the same as the location of your policy data, configure the fields in the **Directory Server** group. 4. Click the **Browse** button and select the area of the directory where the user data is stored. The DN of this location appears in the **Directory** field. 5. If the user location has been replicated to other directory servers, click the **Replicated Servers** tab. — To add a directory server that shares the same user location and data, click **Add**, then configure the host name (or IP address) and port the server runs on. — To delete a directory server that no longer shares the same user location and data, select the corresponding row and click **Delete**. 6. Click **OK** to add this location to the global list. For details, see Chapter 4, *Building your Users and Resources Trees* in the *HP OpenView Select Access v5.2 Policy Builder Guide*.
Step 4: Set your access policies against the following Microsoft Outlook Web Access URLs: • `http://hostname/exchange` • `http://hostname/exchweb`	Set allow, deny, and conditional rules on resources as needed. For details, see Chapter 8, *Controlling network access* in the *HP OpenView Select Access v5.2 Policy Builder Guide*. **Note:** The rules you apply are inherited across multiple resources. Ensure you understand how policies are inherited. For details, see Chapter 8, *Controlling network access* in the *HP OpenView Select Access v5.2 Policy Builder Guide*.

Table 2: Setting up Policy Builder to protect Outlook's content

This step ...	Details on how to do it...

Step 5: Create an Integrated Windows authentication server to authenticate users trying to access Outlook content.
 	
Note: For Windows Integrated authentication to work, users must access Outlook with an Internet Explorer browser.
	1. Click **Tools>Authentication Servers.** The **Authentication Server** dialog box appears.
	2. Click the **Add** button. The **Authentication Method** dialog box appears.
	3. Enter a server name and click the **Integrated Windows** option before clicking **OK**. This displays the **New Integrated Windows Server** dialog box.
	4. In the **Specify location for user lookups** pull-down list, select a lookup destination from your global user location list, for this server.
	5. If your server performs user lookups against a data source other than one of your configured directory user locations in your global list, click **Browse** and select the group or folder in the **Specify policy location for newly authenticated users without user entry** field.
	This group or folder acts as the repository for the access policy *only*. Once a user is authenticated by this server, the Policy Validator checks this location for the corresponding access policy.
	6. Click **OK** to commit these configuration parameters.
	7. Because you intend to use this authentication server with SelectID (set against a resource, rather than a service branch), you need to ensure you set the **w3svc/AuthPersistSingleRequest** to **True**. Otherwise, authentication method information cannot persist beyond the first request. This causes users to be denied access irrespective of the policy you set. To set this value, enter the following command at an MS-DOS prompt:
	`cd Inetpub\Adminscripts`
	`cscript adsutils.vbs set w3svc/AuthPersistSingleRequest True`
	For additional configuration details, see Chapter 7, *Setting up authentication servers* in the *HP OpenView Select Access v5.2 Policy Builder Guide*.

Table 2: Setting up Policy Builder to protect Outlook's content

This step ...	Details on how to do it...
Step 7: Configure SelectID to use the Integrated Windows authentication server you configured in Step 5.	1. Right-click the square in the **SelectID** column beside the entry, then click **Enable SelectID**. The **SelectID Properties** dialog box appears. 2. Click the **Authentication** tab. This tab allows you to determine which authentication server(s) to use to authenticate the unauthenticated user. 3. Click **Add**. The **Available Authentication Servers** dialog box appears. 4. In the **Available Servers** list, select the Integrated Windows authentication server and at least one other authentication server and click **Add**. These servers appear in the **Selected Servers** list. 5. Click **OK** to close the **Available Authentication Servers** dialog box.