HP OpenView Select Access

For the Windows® Operating System

Software Version: 6.0

Integration Paper for Microsoft Outlook Web Access for Exchange Server 2000/2003 and Microsoft Sharepoint Service 2.0

September 2005

Legal Notices

Warranty

Hewlett-Packard makes no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

A copy of the specific warranty terms applicable to your Hewlett-Packard product can be obtained from your local Sales and Service Office.

Restricted Rights Legend

Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause in DFARS 252.227-7013.

Hewlett-Packard Company
United States of America

Rights for non-DOD U.S. Government Departments and Agencies are as set forth in FAR 52.227-19(c)(1,2).

Copyright Notices

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

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

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

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

Trademark Notices

Support

Please visit the HP OpenView web site at:

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

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

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

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

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

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

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

To find more information about access levels, go to the following URL:

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

To register for an HP Passport ID, go to:

https://passport.hp.com/hpp2/newuser.do

Contents

1 Understanding Your Select Access Integration

Select Access is an integral part of HP's comprehensive Identity Management suite. It delivers a full solution for complex access management across the enterprise. Select Access:

- Automates access control and user life-cycle management.
- Extends the enterprise through federation.
- Delegates management to business owners and the end users themselves.

Along with robust workflow, user self-service, reporting, and delegated administration capabilities, Select Access is the most comprehensive access control system available. Select Access simplifies your ability to secure user access to Microsoft Outlook Web Access (OWA) for Exchange Server 2000/2003 and Microsoft Sharepoint 2.0 services and resources.

Requirements of this Integration

This integration requires:

- That you have either OWA and/or Sharepoint installed and running on your network.
- That end-users request online assets with Internet Explorer browsers.

Assumptions in this Document

This document assumes the following:

- That you understand the features and functions of Select Access.
- That if you want to integrate with OWA, that you want to synchronize user entries between your Exchange server and Select Access.
- That you have a working knowledge of Select Access and LDAP 3.0-compliant directory servers.

Integrating Select Access and OWA and/or Sharepoint Applications

To understand the integration between Select Access and these Microsoft applications, you need to understand where critical integration points lie.

Understanding the Key Components of this Integration

Both OWA and Sharepoint 2.0 use an IIS 5.0/6.0 Web server. Depending on the application you are integrating Select Access with, the function of that server varies:

- For OWA, it enables Web-based e-mail collaboration so users gain always-available access to critical business communications while still delivering security and reliability.
- For Sharepoint, it enables the sharing of documents, messages, or photos across a local network or Internet over Web browsers. This server allows users to upload and download assets, and versions files as assets vary.

These Web servers must be coupled with the Select Access's architecture. Unique features and important components that are affected by this integration include:

- A Temporary Password store—That allows OWA and Sharepoint to achieve Single Sign-on (SSO). For details, see What's Unique to this Integration on page 4.
- An LDAP 3.0-compliant directory server—That allows you to create user accounts for Select Access administrators and OWA/Sharepoint users. Information in the directory allows Select Access to manage authentication and authorization policies for explicit user/resource combinations.

You can configure Select Access to use the same user entries used by the Exchange server. You simply need to add the Active Directory server used by Exchange as a new user location in the Policy Builder. For details, see Using Exchange User Entries on page 11.

- An IIS Enforcer plugin—That intercepts all access requests on OWA/Sharepoint's Web server. The IIS Enforcer plugin enforces the outcome of the access request that has been evaluated by the Policy Validator
- The Policy Builder—The Java GUI that provides you with a view of all users and available online assets. The combination is displayed as a hierarchical matrix which can be easily expanded and contracted to facilitate quick navigation.

For a complete overview of all Select Access components, refer to the *HP OpenView Select Access 6.0 Installation Guide*.

What's Unique to this Integration

The password in the Temporary Password store—along with the userID and domain—is used by the IIS Enforcer plugin. The plugin uses this information to set HTTP Basic Authentication details each time a user requests a protected asset. This new mechanism enables SSO to OWA and Sharepoint assets—as well as other Microsoft products that require IIS authentication.

Compared to other deployments of Select Access, deployments with OWA and/or Sharepoint require that user credentials be stored in a secure location so they can be recovered and transferred between these systems.

However, an issue exists with the storage of passwords in a recoverable format: brute force techniques to obtain passwords in this format poses a security threat. To solve this SSO-related issue with these non-one-way hash passwords, HP has created an feature known as a Temporary Password store.

Achieving Secure SSO with the Select Access Temporary Password Store

This unique password retrieval mechanism uses strong encryption to store the session password in the directory server for the duration of the session.

The encrypted temporary passwords are stored in Select Access's Policy Store. The key for decrypting the password in the session is unique for each session, and is not stored on the directory server.

When the session expires, the password entry is removed from the directory server. This removal minimizes security risks related to typical password storage mechanisms. Because directory entries are keyed on the generated session key, they cannot be referenced back to a specific user DN. Passwords, consequently, have no meaning.

Figure 1 illustrates how Select Access uses this Temporary Password store to achieve SSO among Microsoft products using HTTP Basic Authentication details.

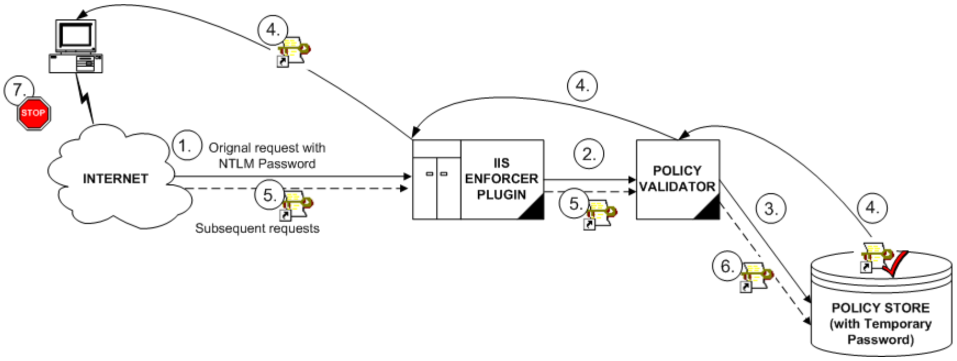

Figure 1 Using the Temporary Password Store

The steps illustrated in this figure are described below:

1 The user makes an original resource request and is authenticated with the NTLM password. The IIS Enforcer plugin intercepts the request.

2 The IIS Enforcer plugin collects and passes details of the request to the Policy Validator. The details include any authentication information collected by the NTLM login page (that is, the domain, userID and password).

3 The Policy Validator performs two the following activities:

- It encrypts the authenticated user's NTLM password with a session key, and stores it in the Temporary Password location in the Policy Store used by Select Access.
- It searches for the user account and checks the policy data for the asset requested. The Policy Validator caches the data from the directory for future retrieval.
- Ultimately, based on this combination of information, it returns a policy decision to the IIS Enforcer plugin, including relevant personalization information.

4 The Policy Validator forwards the key used to encrypt the password to the plugin, which then returns it to the user's browser.

5 The browser sends this key with subsequent asset requests.

6 The Policy Validator uses this key to decrypt password in the Temporary Password store and writes the HTTP Basic Authentication header.

7 When the user ends the session, the temporary password is deleted from the Policy Store. Otherwise, the IIS Enforcer plugin, along with the Policy Validator, continue to regulate activities on your network.

➤ You can use an IIS Enforcer plugin with multiple Policy Validators. For details, refer to the *HP OpenView Select Access 6.0 Installation Guide*.

2 Integrating These Products

Integrating Select Access with OWA and/or Sharepoint requires that you perform specific actions on the IIS server machine as well as the Select Access system. For details, see both:

- Deploying the IIS Enforcer Plugin on page 8
- Select Access-Protecting Collaboration Assets on page 10

Deploying the IIS Enforcer Plugin

OWA and Sharepoint serve assets over IIS. Therefore, all configuration steps revolve around preparing that Web server for integration with Select Access. Table 1 summarizes the steps you need to perform deploy the IIS Enforcer plugin on this server's host computer.

Table 1 Preparing Your IIS Web Server for Deployment

Setup Task	Deployment Details
Step 1: Install and configure the IIS Enforcer plugin on OWA's/Sharepoint'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 Select Access components** installation screen. 3 Install and configure the IIS Enforcer plugin on the OWA/Sharepoint host. Choose a **Custom** configuration. Note: You can accept defaults provided by the Setup Tool or you an use custom settings. 4 In **Single Signon Using Basic Authentication** screen, check the **Temporarily Store Password** box. 5 When you reach the **Finish/Update Configuration** setup screen, check the following two boxes: — **Update Web server configuration to load the Enforcer plugin** — **Restart Web server** 6 Click **Finish**. For details, see the *HP OpenView Select Access 6.0 Installation Guide*.
Step 2: Run the **IIS Console** and re-configure the **Authentication Methods** for: • All of the OWA URLs. For example: — `http://myhost/Exchweb` — `http://myhost/Exchange` — `http://myhost/Exadmin` • All of Sharepoint's Web sites. For example: — `http://myhost/<sharepoint_root>/` — `http://myhost/<sharepoint_root >/Shared%20Documents` — `http://myhost/<sharepoint_root>/Lists` — `http://hostname/<sharepoint root directory>/_layout`	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 to enable these methods: — **Basic authentication** — **Anonymous access** 3 Uncheck all other boxes to disable these methods.

Select Access-Protecting Collaboration Assets

Securing the assets that enable corporate collaboration with Select Access requires that you register its OWA and Sharepoint resources with the Policy Matrix, the grid-like interface that is the main administrative element in the Policy Builder. Table 2 lists the tasks required to accomplish this task.

Table 2 Securing Collaborative Resources in the Policy Builder

Task	Details
1 Register security sensitive resources with Select Access by adding them to the Resources Tree in the Policy Matrix.	Registering Microsoft Collaborative Resources on page 10
2 For OWA, you can build the Users Tree by using the directory server already used by the Exchange server. That way, you share the same set of user records with Select Access.	Using Exchange User Entries on page 11
3 Create the appropriate authentication policies that allow users to validate their identities with the integrated authentication (NTLM) method.	Authenticating Users in an NTLM Environment on page 11
4 Assign authorization policies to your user and Microsoft resource combinations.	Setting Policy on Specific Microsoft Resources on page 12

Registering Microsoft Collaborative Resources

The Policy Builder allows you to build a representative view of the Microsoft OWA and Sharepoint resources you want to control access to. Select Access-protecting these resources requires that you:

- Add the IIS servers you have Enforcer protected.
- List the resources that are of a security-sensitive nature.

This effectively registers the services and assets in the directory server so you can then manage access to these service and/or assets through one or more policies.For details, see To register Microsoft services and resources on page 10.

To register Microsoft services and resources

1. If you want to organize these servers by folder, create one with a representative name for these servers. Do this by:
   a. Right-clicking Resource Access branch and clicking **New** → **Folder**. The **New Folder** dialog appears.
   b. Typing a name for the folder. For example “Collaboration Servers”.
2. Create a service entry. Do this by:
   a. Right-clicking on the folder you just created and clicking **New** → **Service**. The **New Service** dialog appears.
   b. In the **Name** field, typing a name for the appropriate service entry that you need to Select Access-protect.

c. Configuring the IIS server's contact information:
   - Click the **Add** button to create a new server definition.
   - Select **HTTP** as the protocol
   - Type the hostname/IP address and port number.

3. Register Microsoft assets and add them to the service branch you created. Because the Select Access HTTP resource discovery plugin cannot enumerate resources on servers that require Basic Authentication, you must add the resources to the Resources Tree manually. For details, see Adding Network Resources to the Resources Tree in the *HP OpenView Select Access 6.0 Policy Builder Guide*.

Using Exchange User Entries

Manually add the Active Directory user location that Microsoft Exchange currently uses. That way, the user entries are shared by both systems.

To build a Users Tree with Exchange data

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.
   - 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.
   - If the user location is not the same as the location of your policy data, configure the fields in the **Directory Server** group.
2. 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.
3. 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**.
4. Click **OK** to add this location to the global list.

Authenticating Users in an NTLM Environment

NTLM is used throughout Microsoft's systems as an integrated single sign-on mechanism. In an NTLM environment, users using an Internet Explorer browser can use their Microsoft desktop credentials to gain access to Internet resources without needing to re-enter passwords and userIDs.

NTLM authentication is a secure form of authentication. The Internet Explorer browser exchanges desktop credentials cryptographically, by hashing details before sending them. NTLM is the recommended authentication when integrating with Select Access.

When configuring Select Access to use integrated Windows authentication, you must:

- Create an NTLM server to authenticate users trying to access OWA and/or Sharepoint content. For details, see To create an authentication server to accept NTLM credentials below.

- Configure SelectID to use this NTLM authentication server to authenticate users on Select Access. For details, see To configure SelectID to authenticate users with desktop credentials on page 12.

To create an authentication server to accept NTLM credentials

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 **NTLM** option before clicking **OK**. This displays the **NTLM 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.

To configure SelectID to authenticate users with desktop credentials

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 NTLM server you created in To create an authentication server to accept NTLM credentials on page 12, and click **Add**. These servers appear in the **Selected Servers** list.
5. Click **OK** to close the **Available Authentication Servers** dialog box.

Setting Policy on Specific Microsoft Resources

You can set allow, deny, or conditional policies as your sensitivity of resources require. Using built-in inheritance rules, the Policy Builder allows you to set policy for all your known users quickly and easily. For an overview, refer to the *HP OpenView Select Access 6.0 Policy Builder Guide*.

However, as documented in the procedure in To set specific access policies on page 12, certain resources with OWA require a specific policy to control access. Additionally, you may also require a logout conditional rule that also logs the user out of Select Access and thereby destroys the cookie that gives them access to other network resources on SSO-enabled servers. For details, see this procedure that follows.

To set specific access policies

1. For the `http://hostname/exchange` resource:

   - Where the Unknown Users column and this resource intersect, right-click the cell and click **Deny Access**.

- Where the Known Users column and this resource intersect, right-click the cell and click **Allow Access**.

2 For the `http://hostname/exchweb` resource:

- Where the Unknown Users column and this resource intersect, right-click the cell and click **Deny Access**.
- Where the Known Users column and this resource intersect, right-click the cell and click **Allow Access**.

3 To logout users from Select Access to remove the session cookie in a more timely manner, create a Conditional Rule that logs these users out. This prevents the user from accessing other SSO-enabled servers. Where the Known Users column and resources requiring logout intersect, right-click the cell and click **Conditional Rule**.

- If you have already created a rule with a standalone logout terminal point in it, choose this rule from the list now.
- Otherwise, create a rule that only includes a logout terminal point.