HP OpenView Select Access

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

Software Version: 6.0

Integration Paper for Domino Web Application Server 5.0.8

September 2005

Legal Notices

Warranty

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

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

Restricted Rights Legend

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

Hewlett-Packard Company
United States of America

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

Copyright Notices

Trademark Notices

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

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

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

Support

Please visit the HP OpenView web site at:

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

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

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

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

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

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

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

To find more information about access levels, go to:

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

To register for an HP Passport ID, go to:

https://passport2.hp.com/hpp/newuser.do

Contents

1 About this Integration Paper

What is it about?

This Integration Paper describes how to integrate Domino Web server with Select Access.

Select Access 6.0 is the last version HP performed interoperability testing against. If you have any questions regarding the interoperability of your version of Select Access with this third-party product, contact HP's Support Services.

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

Table 1 Integration Paper overview

This chapter...	Covers these topics...
Chapter 2, Technologies overview	• Introduces Select Access: what it is, what it does, and how it works. • Introduces Domino Web server: what it is and what integration issues exist.
Chapter 3, Integration issues	Describes what you need to do with Domino Web server 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 Domino Web server.
- Using Select Access to manage access to Domino Web server resources.

What does it assume you already know?

This Integration Paper assumes a working knowledge of:

- **Select Access**—Ensures that you understand how integration with Domino Web server affects the Select Access components.
- **Domino Web server**—Ensures that you understand how integration with Select Access affect the Domino Web server 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 Domino Web server, 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.

2 Technologies overview

This chapter introduces you to Select Access and Domino Web server. It gives you an overview of the products, what they do, what components are installed with these products, and Domino Web server 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.

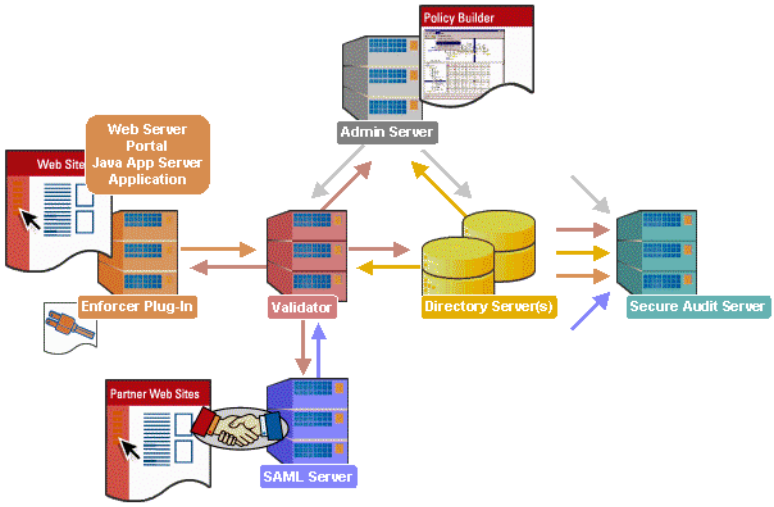

Figure 1 Select Access system architecture

Custom Plugins to Customize Functionality With

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

- Authentication plugins: A custom Policy Builder authentication plugin allows you to tailor which kinds of authentication methods are available to better meet the needs of your organization. A Policy Builder authentication method plugin allows administrators to use and configure the authentication server for this method via a dialog box. As with the decision point plugin, this dialog box is a property editor that allows security administrators to configure the authentication server.
- Decision point plugins: A custom Rule Builder decision point plugin allows you to tailor how rules are built to better meet the needs of your organization. A Rule Builder decision point plugin allows administrators to use and configure the criteria for the decision point via:
  - The icons that represent that decision point on both the toolbar and the rule tree.
  - The dialog box, known as a property editor, that allows security administrators to configure it.
- Policy Validator decider plugins: The Validator-specific counterpart of a decision point plugin, the decider plugin allows you to capture the evaluation logic for your custom decision point (described above), so that the Policy Validator can evaluate users based on the information it collects.
- Resource discovery plugins: These plugins allow you to customize how resources are scanned on your network.

- Enforcer plugins: A new Enforcer plugin allows you to customize the backend application logic by enforcing the decision that the Policy Validator returns to the Enforcer plugin's query.
- Additional Web/Application/Portal/Provisioning server specific plugins: These plugins can be included to handle specific integration details between the third-party technology and Select Access. For example, the Domino server requires a `site_data` plugin if you need to transfer site data between Select Access and Domino.

What is Domino Web server?

The Domino Web server hosts Web sites that both Internet and Intranet users can access. The Domino Web server serves pages that are stored in either the file system or in a Domino database. Using Domino to store Web pages as documents in a database has a major advantage over storing static HTML pages. With Domino, any change that you make to a database is automatically reflected on the Web server.

How does Domino Web server work?

When a Web browser requests a page in a Domino database, the following sequence of events takes place:

1. Domino translates a document into HTML.
2. When a Web browser requests a page in an HTML file, Domino reads the file directly from the file system.
3. Then the Web server uses the HTTP protocol to transfer the information to the Web browser.

The benefits of Select Access's solution

Integrating Select Access with Domino Web server offers the following main benefits:

- **Personalization**—Once users are authenticated, Domino Web server can display personalized content to them.
- **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.

3 Integration issues

When setting up Domino Web server, there are some issues you need to consider:

- Domino Enforcer plugin—The Domino Enforcer plugin is not included in the Setup Tool and Wizard, which means you need to perform a templated Enforcer plugin setup.

The Domino Enforcer plugin handles personalization data differently than the other Select Access Enforcer plugins do.

- The Domino plugin for site data—The mechanism shipped with Select Access for passing data from one Domino DSAPI filter to the Domino site data plugin differs from the other Select Access site data plugins. You need to write your own site data plugin using the `domino_site_data.c` example file.

For details, see *Configuring Domino Web server* on page 10.

Configuring Select Access

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

Table 1 Setting up Select Access

This step...	Details on how to do it...
1 Run the Generic Enforcer plugin setup wizard in the Setup Tool and give it the following name: `enforcer_domino.xml`. **Note:** On the **Pass-through Domains** setup screen, do not configure any settings because the Domino Enforcer plugin does not support virtual Web hosting.	*Configuring the Enforcer Plugin* on page 129 in the *HP OpenView Select Access 6.0 Installation Guide*
2 Create specific network resource entries in the Resources Tree. Do this for every URL that deploys the content stored in a Domino database to which you want to control access.	*To create a new network service* on page 41 in the *HP OpenView Select Access 6.0 Policy Builder Guide*
3 Assign deny or allow access rules to the URLs described in step 2. This creates an access policy that determines if a user can access a specific resource.	Chapter 7, *Controlling Network Access* in the *HP OpenView Select Access 6.0 Policy Builder Guide*

To relocate Select Access files to the corresponding Domino location

1. Locate the Domino files in the following folder:
   `<SA_install_path>\bin`
2. Copy the files to the corresponding Domino folder. Table 2 summarizes which files need to be copied from the `\bin\` folder of the Select Access installation path to the Domino host machine .

Table 2 Moving Select Access files to the Domino folder

Copy this file...	To this Domino location...	What it does...
`domino_web.dll`	`<install_path>\Domino`	**Required**. This file is the Domino Enforcer plugin.
`domino_site_data.c`		Optional. This file is the site data plugin. It is a sample source file for users to consult when they are building their own plugin.

Configuring Domino Web server

You need to use the Domino Administrator to configure the Domino Web server so the Enforcer plugin can control access to content stored in a Domino database. These steps are described in Table 3.

Table 3 Setting up Domino Web server

This step...	Details on how to do it...
1 Install the Domino Web server and the Domino Administrator on your system.	See the *Domino Installation Guide*
2 Configure the authentication settings. You are disabling most of these Domino settings so that only Select Access authenticates users. The procedure varies depending on whether or not your system is configured to use SSL.	*Setting your authentication options* on page 11 OR *To configure your authentication settings for SSL* on page 11

Table 3 Setting up Domino Web server

This step...	Details on how to do it...
3 Register the Domino Enforcer plugin with the Domino Web server so that it automatically starts when the Web server starts.	*To register the Domino Enforcer plugin* on page 11
4 If you need to transfer data between the site data plugin and the Select Access Enforcer plugin, ensure you configure it appropriately. Currently, Select Access supports the following types of data transfers: • Personalization information • Site data	*To obtain personalization information from the environment variable* on page 12 OR *To pass site data to the Domino Enforcer plugin* on page 12

Setting your authentication options

You need to configure your authentication settings so that only Select Access authenticates users.

To configure your authentication settings for non-SSL

1 On the Domino Administrator, click the **Configuration** tab.

2 From the Configuration tree, select which server you want to configure.

3 On the server's configuration page, click the following tabs: **Ports>Internet Ports>Web**.

4 Ensure you set the following settings in the **Authentication options** group:

— In the **Name and password** field, select **No** from the dropdown list.

— In the **Anonymous** field, select **Yes** from the dropdown list.

5 Click **Save and Close** in the top left-hand corner of the dialog box.

To configure your authentication settings for SSL

1 On the Domino Administrator, click the following tabs: **Ports>Internet Ports>Web**.

2 Ensure you set the following settings in the **Authentication options** group:

— In the **Client certificate** field, select **Yes** from the dropdown list.

— In the **Name and password** field, select **No** from the dropdown list.

— In the **Anonymous** field, select **Yes** from the dropdown list.

3 Click **Save and Close** in the top left-hand corner of the dialog box.

Registering your Enforcer plugin

You need to register your Domino Enforcer plugin and ensure that it loaded successfully.

To register the Domino Enforcer plugin

1 On the Domino Administrator, click the **Configuration** tab.

2 From the Configuration tree, select which server you want to configure.

3 On the server's configuration page, click the **Internet Protocols tab** and then click the **HTTP** tab.

4 In the **DSAPI** section of the tab, enter the full path to the Domino Enforcer plugin file in the **DSAPI filter file name** field.

5 Click **Save and Close** in the top left-hand corner of the dialog box.

6 Restart the Domino Web server.

7 Open your Windows event Log to check the state of the registration.

- If it loaded successfully, the following message appears in the **Event Detail**: "Select Access Domino Plugin (Enforcer plugin) Version 6.0."
- If the plugin did not load successfully, an event error appears.
- If Domino cannot locate the Domino plugin file, the following message appears in the Domino console window: "Error loading DSAPI filter. Filter not loaded."

Exchanging data

Outlined below are steps required to ensure successful data transfers between Domino and Select Access.

To obtain personalization information from the environment variable

1 Configure personalization. For details, see Chapter 5, *Authentication Basics: Select Auth & Personalization* in the *HP OpenView Select Access 6.0 Policy Builder Guide*.

2 Write a servlet that is capable of accessing and manipulating personalization information.

3 In your servlet, add the following java code:

```
String p13nInfo = request.getRemoteUser();
```

The `request.getRemoteUser()` method returns encoded personalization data. With Domino, the single string returned from `getRemoteUser()` method contains all the personalization information related to the activated attributes.

4 Decode the variable data. The format of the personalization data is the following:

```
<variable_name>=<value>
```

Multiple variables are delimited by commas.

Commas and equal signs are encoded to the following series of characters respectively: %2c and %3d.

To pass site data to the Domino Enforcer plugin

1 Write a site data plugin and ensure that data passed to the Domino Enforcer plugin is prefixed by the following: `"SITE_DATA="`. For example, `"SITE_DATA=Sales Department"`.

2 Ensure that the Enforcer plugin is passing information to the site data plugin during the authentication phase by checking that the two lines shown in Code example come after `kFilterAuthUser`.

3. Ensure that `kFilterAuthUser` passes the site data through `FilterAuthenticate.authName`. For details, see the `domino_site_data.c` example file.
4. Install the site data plugin you created in steps 1-3.
5. Click the **HTTP** tab in the Domino Administrator.
6. In the **DSAPI filter filename** field, enter the name of the Domino Enforcer plugin after the name of the site data plugin that is passing information to the Domino Enforcer plugin. This ensures that Select Access's Domino site data plugin executes before Select Access's Enforcer plugin.
7. Save your settings and then restart the Domino Web server.

Domino example file

```
case kFilterAuthUser:
     auth = (FilterAuthenticate*) eventData;
     auth->authName = "SITE_DATA=<Sample Domino Site Data from the test plugin>.";
```