HP OpenView Select Access

Release Notes

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.

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 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

Introduction

Important: Read these Release Notes carefully before installing HP OpenView Select Access. See the *HP OpenView Select Access v5.2 Installation Guide* for preinstallation requirements and instructions on installing Select Access.

⚠ HP OpenView Select Access 5.2 is intended exclusively for customers who are new to Select Access. Due to certain backward compatability issues, it should under no circumstances be installed on top of a previous release of Select Access.

This document specifies known issues in version 5.2 of the HP OpenView Select Access product. The information in this document supersedes information in the rest of the Select Access documentation set. These notes may provide corrections or clarifications to the documentation.

Patch availability

Occasionally patches to the Select Access software are made to provide fixes between releases. If you have any problems when using HP OpenView Select Access v5.2:

1. Go to http://support.openview.hp.com/ page.
2. Follow the instructions there to check whether there are any patches available for HP OpenView Select Access v5.2. There may be a solution for your problem.

Hardware/software requirements

For the hardware, software, and third-party requirements, see *System requirements* on page 11 of the *HP OpenView Select Access v5.2 Installation Guide*.

Chapter 2

About HP OpenView Select Access 5.2

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.

⚠ HP OpenView Select Access 5.2 is intended exclusively for customers who are new to Select Access. Due to certain backward compatability issues, it should under no circumstances be installed on top of a previous release of Select Access.

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.

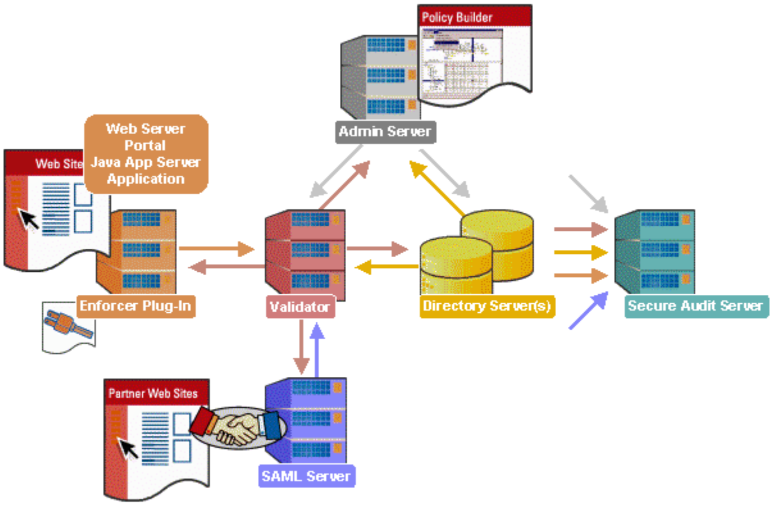

Figure 1: Select Access system architecture

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.

Chapter 3

Known issues

HP OpenView Select Access 5.2 shipped with the following known issues. These issues are categorized by topic:

Documented installer issues

HP has documented and is aware of the following issues with Select Access's installer.

Incorrect display of disk space

Occasionally, the **Pre-Installation Summary** screen incorrectly displays the host machine's current available disk space as "Error".

Partial installation affects uninstall

Problems can occur with the uninstaller if you do the following during the installation of Select Access:

1. Installing all components.
2. Allow files to be 50-75% installed.
3. Click the **Cancel** button at this incomplete stage.

While this halts the installation of the product, all files transferred to that point remain on the host computer's hard drive. Note that if you then try to uninstall the files from the Control Panels **Add/Remove Programs** application, you cannot actually run the uninstaller because the files needed to accomplish this task were not installed on the host machine.

Running Control Panel applications

If you are uninstalling and/or installing and/or configuring Select Access components on a Windows host computer, ensure that you do not have the Services window — or any other Control Panel application — open. This open Control Panel application triggers conflicts that cause the installer and Setup Tool to behave abnormally.

Not all IIS-related services restarted

If you leave the IIS Web service running during an installation, the installer automatically shuts it down as well as its dependencies (for example, FTP). However, while the Setup Tool automatically restarts the server, it does not necessarily restart all of IIS' dependencies. Following an installation, check to see that all IIS-related services are running again. If not, restart them manually.

Documented directory server issues

HP has documented and is aware of the following issues with supported directory servers.

Microsoft Active Directory

Due to known issues with Microsoft Active Directory (ADS), several functions can be problematic:

- *Schema management*: You must enable schema management with ADS. To enable schema management, run the registry file we provide for this purpose, before you install Select Access. You can find this file on the Select Access product CD in the following location:

  ```
  \schema\Active-Directory\adupdate.reg
  ```

- *Password management*: Users can only change passwords if ADS is running over SSL. Therefore, you cannot create accounts that require passwords, modify passwords, or use password management, unless SSL is enabled.
- *Entry size restriction*: Microsoft has placed a size limit on LDAP records. This limitation creates further issues with the activation of *all* available attributes. Because Microsoft will not be changing this size limitation, you cannot activate all available attributes. However, this is typically not a problem since most deployments do not require all user attributes activated.
- *User object class*: The user object class is `User` not `inetOrgPerson`, which is the object class used by all other directory servers. The difference in user object class impacts the following components and features, because the number and the types of user attributes between these two classes vary:
  - How the Policy Validator performs password-based authentication.
  - How the Policy Validator registers new users.

– Password management of users.

ℹ If an attribute is not available in the `User` class, you can add it by clicking the **Advanced** button of the **User** properties dialog box, and modifying the **Attributes** tab accordingly. ADS does not allow you to add an attribute that is contrary to the schema definition for user entries. For details, see *Configuring advanced user entry properties* in the *HP OpenView Select Access v5.2 Policy Builder Guide*.

ℹ Microsoft will support both object classes in a future release.

- *Group creation restriction*: ADS does not allow you to create an `ADS group` within another ADS group. This is because this group type is a container for users only. It will not allow you to add other groups of the same native type.
- *Directory referral support over SSL*: An ADS issue causes directory referrals on an SSL system to refer to a non-SSL location, which causes referrals to fail on Select Access. This issue is expected to be fixed in a future release of ADS.

Novell NDS eDirectory server

HP has documented that LDAP messages can occasionally become truncated if they are larger than 64K. Truncated messages can be problematic with Select Access components.

Oracle Internet Directory

HP has documented the following issues with Oracle Internet Directory (OID):

- *Nonce secrets not updating properly*: When using an OID in a multi-Policy Validator deployment, an error is generated when a Policy Validator tries to update a nonce secret. Because attribute matching fails with binary attribute values on OID, the Policy Validator does not delete old nonce secrets on this server, but instead just adds new ones. HP is currently investigating this issue.
- *Encryption algorithm incompatibility*: Oracle uses MD4 as its default encryption algorithm. HP recommends that you use the Oracle Directory Manager to change the default algorithm to one of the following:

  – MD5

  – Unix CRYPT

  – SHA-1
- *Entry size restriction*: Oracle database prior to v9.0.2 has a size limit of 2000 bytes for LDAP string attributes. With v9.0.2, the limit increases to 4000 bytes. This limit of Oracle databases prior to v9.0.2 imposes a restriction on the following:

- *The number of user locations* to a maximum of three or possibly four if you use this directory server as your Policy Store as well. This is because a user location uses approximately 500 bytes per definition on this server.

ℹ If you intend to install and configure a SAML server, note that the length of the nxXml attribute value exceeds the limit of 2000 bytes with v9.0.2.

If you need to increase the number of user locations to a maximum of seven or possibly eight, upgrade to v.9.0.2. If you need to increase the number of user locations further, move your Policy Store to a non-Oracle server as well.

ℹ Oracle intends to support a larger byte size limit with its Oracle database v10i.

- *The size of the CA certificate used with SSL*: Since the CA certificate used for this purpose can exceed the 2000 byte entry size limit, user location definitions on these databases will fail. This is another reason why HP recommends that you upgrade to v9.0.2.

These directories also generate protocol errors when you try to setup a SAML server. For details, see *Documented SAML server issues* on page 21.

Siemens DirX

HP has documented the following issues with DirX servers:

- *Schema updates:* You must update this directory server's schema manually. Select Access cannot automatically change the schema. For details, see Chapter 5, *Preconfiguring a directory server* in the *HP OpenView Select Access v5.2 Network Integration Guide*.
- *Operator inconsistency*: Due to the way in which comparison operators in LDAP searches are implemented on DirX, roles and the LDAP attribute decision point behave inconsistently from other supported directory servers. In particular, less than (<), greater than (>), less than or equal to (<=), and greater than or equal to (>=) tend to be the most inconsistent operators.

CA eTrust

HP has documented the following issue with eTrust servers:

- *Schema updates:* You must update this directory server's schema manually. Select Access cannot automatically change the schema. For details, see Chapter 5, *Preconfiguring a directory server* in the *HP OpenView Select Access v5.2 Network Integration Guide*.

Critical Path

HP has documented the following schema issues with Critical Path (CP) v4.x servers:

- *Schema updates:* For both the 4.0 and 4.1 versions of this directory, you must update this directory server's schema manually. You can only do this by using files from the Select Access's product CD, rather than from Select Access's installation folder (which is `<install_path>/schema/Critical-Path/Cp4.x/` by default). For details, see Chapter 5, *Preconfiguring a directory server* in the *HP OpenView Select Access v5.2 Network Integration Guide*.
- *Operator inconsistency*: Due to the way in which comparison operators in LDAP searches are implemented on CP, roles and the LDAP attribute decision point behave inconsistently from other supported directory servers. In particular, less than (<), greater than (>), less than or equal to (<=), and greater than or equal to (`>=`) tend to be the most inconsistent operators.
- *Index node values*: A misconfigured CP property can cause the Policy Builder to throw an exception. Policy Builder throws an exception because the index node value is too low. For details, see *To set the correct maximum CP index node value when necessary* below.

To set the correct maximum CP index node value when necessary

1. Open the following file in a text editor of your choice:

   ```
   <CP_install_path>/ds.properties
   ```

2. Look for the following parameter and ensure that it has the corresponding value:

   ```
   directory.indexNodeMax=524288
   ```

If this parameter does not exist, ensure you add it.

3. Restart your directory server to ensure it uses the new parameter value.

Aphelion

If you use an Aphelion directory server (non-SSL), and you enable data signing in the Administration server's configuration using your own imported certificate that includes an email address in it, the XML for that setting is not recorded to the Policy Store properly. This prevents the Policy Validator from starting up.

If you must use an Aphelion directory server and also require data signing, you can circumvent this issue by:

- Allowing Select Access to handle its own data signing certificates.
- Use this certificate but delete the email address from it.

Documented Administration server/Setup Tool issues

HP has documented and is aware of the following issue with the Administration server.

User credentials and international characters

After configuring the Administration server's login credentials with international characters in Setup Tool, you are warned that the user name and password you entered when configuring the remaining Select Access components do not match. However, if you return to the Administration server's configuration screens and re-enter the same credentials, credential verification does not generate a warning. This inconsistent treatment of credential verification is likely attributable to the manner in which international characters are being set in the Administrator's cookie. HP recommends that you avoid using international characters when configuring the Administration server's login credentials.

This issue is limited to the Administration server/Setup Tool only. Delegated administrators can have user credentials that include international characters.

Documented Policy Builder applet issues

HP has documented and is aware of the following issues with the Policy Builder applet.

Pass-through domain change

Removing an Enforcer plugin's pass-through domain with the **Component Configuration** window and then clicking the **Edit>Refresh** command, suggests that the update is immediately used by the Enforcer plugin. In reality, the Enforcer plugin does not use the updated list of pass-through domains until it intercepts a request for a non-pass-through site.

Verifying an audit trail in the middle of a signing interval

If you try to verify an audit trail in the Report Viewer that the Secure Audit server is still appending data to, the server cannot apply the required closing signature. This happens because the server has not yet reached the signing interval value you configured (that is, applies a signature every n^{th} message). Consequently, the Report Viewer flags the entries in this incomplete interval as having been tampered with.

Delegated administration and user entry changes

If delegated administrators try switching the user's **Identifier** from User ID to Common Name on the **Directory Information** tab of the **User Properties** dialog box, a permission denied message is displayed. However, once this message appears, the Policy Builder running in delegated administration mode behaves abnormally. HP recommends that administrators who have permission to modify user entries avoid changing the user's **Identifier** field when running in delegated administration mode. For details, see *To change directory information* on page 74 in the *HP OpenView Select Access v5.2 Policy Builder Guide*.

Delegated policy change causes data signing error

Data signing fails in the following situation:

1. If you are running the Policy Builder in delegated administration mode.
2. The Administration server is hosted on Solaris computer.
3. The Administration server's host computer is connected to an Aphelion directory server.
4. A delegated administrator makes a policy change against a specific resource.

This failure occurs because delegated administrators cannot flush the cache immediately after making a change in delegated administration mode. Consequently, if the user tries to access a resource before the Policy Builder automatically flushes the Policy Validator cache, a data signature failure occurs.

Resource discovery problematic

Depending on the configuration of your Web server, the resource plugin's resource lists can be unreliable if you specify a directory to start scanning from. For example, if Web server either does not specify a start page, or does not permit virtual directory listings, the plugin cannot accurately detect all files in the starting folder.

Expired credentials generates Help error

Allowing your credentials to expire in the Policy Builder generates an error when you try to launch the online help after having logged on a second time. If this occurs, HP recommends that you end your Policy Builder session, flush your Java cache, and start a new administration session.

Role membership tab behaves unexpectedly

If you display the **Role Properties** dialog box and click on the **Membership** tab, the **Search** dialog box appears instead of displaying the members. This issue is limited to Select Access deployments where the user location for the role is in the same directory server area as the policy data location.

Netscape browser versions

You can run the Policy Builder in Netscape v6.x and Internet Explorer browsers. Certain versions of Netscape have cookie vulnerabilities. Therefore, HP recommends the following:

- On Windows, use Netscape v6.2.2.
- On Solaris, use Netscape v6.2.3.

Additionally, data imported into the Audit Report Viewer does not display correctly in Netscape browsers running on Solaris platforms.

Printing ability disabled

Due to a known JRE v1.3.1_02 issue, printing via Java applets is not possible on Windows platforms. Therefore, the **Print** command for the Policy Matrix and conditional access rules has been disabled.

Because the Audit Report Viewer does not use the JRE printing mechanisms, the ability to print reports remains enabled.

Verifying an audit trail in the middle of a signing interval

If you are using Windows 2000 (Chinese), an issue exists with audit trails that have been generated and signed by the Secure Audit server. On this platform, the Secure Audit server is unable to successfully verify the audit signature. As a result, the Report Viewer results in the Report Viewer and the Policy Builder will hang whenever you try to open a signed audit trail. HP is investigating this issue.

Naming rules using international characters

The Policy Builder's Rule Builder utility does not allow you to name rules using international characters.

Documented Enforcer plugin issues

HP has documented and is aware of the following issues with the following Enforcer plugins.

IIS plugin and truncated hostnames

If a directory server is truncating hostnames due to character limitation on your directory server, the IIS plugin generates errors. These errors make it seem as if Select Access has a hostname limitation, which is not the case.

Denying access to suspicious URLs

The Enforcer plugin considers the following URLs as suspicious:

- If the path requested by a user contains the substrings "/..", "/./", or "//".
- If the path requested by a user looks like an 8.3 truncation (for example, certain HTML editors truncate `abcdefghijklmnop.html` to `abcdef~1.htm`).

The only time the Enforcer plugin does not consider a URL with a tilde (~) character as suspicious, is when the tilde is the first character position. For example:

<*protocol*>://<*URL_path*>/~myhomepage.

In these cases, the Enforcer plugin denies access immediately. In the latter case, because of the dangers associated with 8.3 filename remapping.

To determine whether or not your Web content is affected by suspicious URLs

1. Open logs generated by the Enforcer plugin in the location it has been outputted to.
2. Search your logs for the following string:

   `“rejecting suspicious url <actual_URL_requested>”.`

Configuring for failover/round-robining

If you do not configure all your Policy Validators before configuring Enforcer plugins, the Enforcer plugin’s bootstrap XML configuration file only includes the name of Policy Validators that were available at that time.

This can be problematic if you create a test/pilot deployment that initially includes only one Policy Validator, but add multiple new Policy Validators during a full Select Access deployment. Potentially any test Enforcer plugins (as well as your delegated administration Enforcer plugin) will not be able to failover and/or round robin to the new Policy Validators if the test Policy Validator fails. If you must stagger your deployment, you should re-run the Setup Tool for your existing Enforcer plugin to ensure all new Policy Validators are written to its `enforcer.xml` file.

Delegated Enforcer plugin issues

The following issues have been reported with the Enforcer plugin for the Policy Builder in delegated administration mode:

- *Logging*: The Enforcer plugin for delegated administration seems not to output events and messages according to the audit settings you configure.
- *Configuration changes*: When you enable delegated administration and configure authentication servers for the Policy Builder running in this mode, Select Access creates an Enforcer plugin to control its delegated administration mode. This Enforcer plugin appears in the **Component Configuration** window that appears when you click **Tools>Component Configuration**.

  While the Enforcer plugin for delegated administration appears in this window, HP suggests that you avoid modifying its configuration. This Enforcer plugin has been configured specifically for delegated administration mode. Modifying its configuration parameters can result in unpredictable behaviors.
- *Certificate regeneration*: When you enable delegated administration and then run the Setup Tool to regenerate the Administration server’s certificate as well as the certificates for the Policy Validator, the Enforcer plugin for delegated administration mode fails to connect to it.

  When you run the Policy Builder in delegated administration mode, your browser displays a “404 Not Found” message. This is because the certificate was regenerated for the Policy Validator, but not the Enforcer plugin for the Policy Builder in delegated administration mode. To solve this problem you can disable delegated administration mode and then re-enable it in the Policy Builder in full administration mode.

Documented Web server issues

HP has documented and is aware of the following issues with the following Web server.

Apache hangs on HP–UX

Before configuring Select Access's Apache Enforcer plugin, HP recommends that you recompile Apache Web server modules with the `-Bsymbolic` option. This procedure is described in *To build Apache on HP-UX* below. Otherwise, the Apache Enforcer plugin will have symbols that conflict with the Web server that causes it to hang suddenly without any error messages or exceptions.

To build Apache on HP-UX

1. Prepare an Apache build as usual. Typically, this requires that you:
   a. Obtain the packages (for example, `apache`, `mod_ssl`, `mm`, `openssl`).
   b. Configure and build `openssl`.
   c. Configure and build `mod_ssl`, which applies a required patch to the Apache source. Run `Configure`.
2. Change to the Apache distribution directory, and open the following file in a text editor of your choice:
   `src/Configure`
3. Locate the entry that sets `LDFLAGS_SHLIB` value for HP–UX systems:
   - In 1.3.19 it is line `1312`
   - In 1.3.22 it is line `1341`
4. Change the value from `-b` to `-b -Bsymbolic`.
5. Run `Configure` by running `sh ./config.status.`
6. Build Apache with either the `make` or `make install` command.

Documented personalization issues

HP has documented and is aware of the following issues with personalization.

Personalization prefix modification for HTTP headers

To maintain security for Select Access's implementation of personalization, Enforcer plugins export personalization attributes as variables that are prefixed with HTTP_SA.

With this prefix, the Apache Enforcer plugin and Sun ONE Enforcer plugins can check HTTP requests to see if they have been forged to inject personalization settings. If an Enforcer plugin determines that an HTTP header has been forged, it automatically denies the request.

⚠ Because IIS cannot detect attempts to inject personalization settings, you should use the COM interface to access personalization attributes in a security-sensitive way. The COM interface is not susceptible to fraudulent header injections.

For details on how to access and decode personalization variables as well as how to use the COM interface, see Chapter 7, *Using Select Access personalization information*, in the *HP OpenView Select Access v5.2 Network Integration Guide*.

Attribute value limitation

You cannot use binary attribute values with attribute names you have activated for personalization. The only attributes that are supported are simple string attributes.

Documented SAML server issues

HP has documented and is aware of the following issues with the SAML server.

Early versions of Oracle directories not supported

If you are using Oracle with a SAML server, Select Access only supports Oracle directory servers that are version 9.0.2 or later. Previous versions have an entry size limit of 2000 bytes. Because this limit is insufficient for SAML servers, the Setup Tool displays a error message when you click the **Finish** button. For other incompatibilities caused by these version of Oracle, see *Oracle Internet Directory* on page 13.

Documented documentation issues

HP has documented and is aware of the following issues with elements of the Select Access documentation set.

Logging ports for the Secure Audit server

The documentation for the Secure Audit server's **Address and Port** setup screen incorrectly states that you can leave the **SOAP/RPC Port** field blank to disable backwards-compatible/third-party logging. You must have a port configured for both logging ports, otherwise the Setup Tool displays an error message.

PDF previous to v5.0.5 shows symbols

Certain versions of Adobe Acrobat Reader may display text symbols in the bookmarks listed in the **Bookmarks** tab. HP recommends that you use the Acrobat Reader v5.0.5 or later. To upgrade to Acrobat

Reader v5.0.5, download the new reader from the following page: http://www.adobe.com/products/acrobat/readermain.html.

JavaHelp redraw issue

Sun's JavaHelp v1.1 includes a known issue that causes redraw problems within its help browser. Documented behaviors include:

- The help window to contain duplicate topics.
- The help window to split content so paragraphs not exactly align.