HP OpenView Select Access

Release Notes

Software Version: 6.0

for HP-UX, Linux, Solaris, and Windows operating systems

March, 2004

Legal Notices

Warranty

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

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

Restricted Rights Legend

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

Hewlett-Packard Company
United States of America

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

Copyright Notices

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 Select Access offers.

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

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

The support site includes:

- Downloadable documentation
- Troubleshooting information
- Patches and updates
- Problem reporting
- Training information
- Support program information
- Security bulletins

Contents

Chapter 1

Introduction

Important: Read these Release Notes carefully before installing Select Access. See the *HP OpenView Select Access 6.0 Installation Guide* for preinstallation requirements and instructions on installing Select Access.

This document specifies new features and updates that have been added to version 6.0 of HP's Select Access product. It also summarizes the changes between this and the previous release. 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.

Previous version

Select Access 6.0 is a full release and includes all patches provided for Select Access 5.2. Future patches will be made available for Select Access 6.0 as required.

Compatibility with previous versions

Select Access 6.0 does not support upgrading from a release previous to Select Access 5.0.

If you are upgrading from Select Access 5.0 or later, the installer manages most compatibility issues.

Hardware/software requirements

For the hardware, software, and third-party requirements, see *System requirements* on page 11 of the *HP OpenView Select Access 6.0 Installation Guide*.

Chapter 2

New in Select Access 6.0

SelectAccess 6.0 includes the following new features:

- *New policy support for delegated Policy Builder functions*
- *New Administration server services*
- *New Enforcer plugins*
- *Simplified Enforcer plugin installation and configuration*
- *New conditional rule to capture administration workflow*

For more information on these features, see the corresponding section that follows.

Key features of Select Access 6.0

Select Access has been upgraded to include the features documented in the sections that follow.

New policy support for delegated Policy Builder functions

The Policy Matrix has been enhanced to include important changes to the Resources Tree. With this change, administrators can now apply access policies against Policy Builder administrative functions as well as network resources. This new functionality impacts delegated administration in the following ways:

- Use of a single **Delegated Administration Port** (by default, port 9987) for all administrators. The senior administrator should use the same port—except to initially setup Select Access (including enabling delegation) or resolve product-related issues. In this case the senior administrator uses the default **Administration Port** (by default, port 9986). You configure both ports in the Setup Tool for the Administration server. For details, see Chapter 5, *Configuring the Administration server* in the *HP OpenView Select Access 6.0 Installation Guide*.
- The Delegated Administration Matrix has been amalgamated with the Policy Matrix. The Policy Builder administrative elements that are delegable are now listed as entries on a branch of the Resources Tree called Administrative Access. Network

Resources are added to the Resource Access branch of the same tree. Elements you can delegate include:

- Read/write access to user attributes (for example, UID and SN)
- Access to administration functions (for example, subdelegation, authentication method management, and password management)
- Network management
- User management

For details on how to delegate administration in the enhanced, single-view Policy Matrix, see Chapter 11, *Controlling administrative access* in the *HP OpenView Select Access 6.0 Policy Builder Guide*.

- A new default folder has been added to the Resource Access tree in full administration mode of the Policy Builder containing the Administration server services. These entries allow you to use SelectID to enable/disable the various administration levels of the Administration server and allow you to set which users can access them. Administration server services include:
  - Delegated administration
  - Web Administration
  - Self-Administration, which contains two resources: Self-Management and Self-Registration

  For more information on these services, see *New Administration server services*.

New Administration server services

Two new administrative services are available through the Administration server. Each of these services accesses the Administration server via a unique port, configured in the Setup Tool. New Administration server services include:

- Web Administration: Allows administrators who have been delegated the appropriate permissions to access the Administration server remotely to manage user entries. Using this service, they can add, modify, rename or delete users, groups or folders. By default, this service is accessed via port 9991.
- Self Administration: Allows users to set or modify their own user profile attributes. By default, this service is accessed via port 9992.

  Self Administration is comprised of two resources, each of which is accessed via its own URL on the Self Administration port:
  - Self-Management: Allows users to modify their user own profile attributes.
  - Self-Registration: Allows users to register themselves as Select Access users.

In order to use Self-Management or Self-Registration, a JSP resource must exist for each. These resources must be named as follows:

— `modify.jsp` for Self Management

— `register.jsp` for Self Registration

Select Access ships a default page for each Self Administration resource. You can modify these pages or create your own using the Web Administration API, available with the Select Access SDK. Once created, these resources should be copied into their respective folders (specified in the Administration server setup; by default, named `self_management` and `self_registration` respectively). These folders can be found in:

`<install_path>/shared/jetty/policy_builder/webadmin`

Once added, you can add links to these pages in other resources where self-administration is required or useful. In addition, adding them as resources in the Policy Builder allows you to set access policy for these resources just as you can for any other network resource.

New Enforcer plugins

Select Access now includes two new Enforcer plugins:

- *WSE*: Protects .NET Web services. You must have the .NET Framework and WSE enhancements installed on your machine in order to install this Enforcer plugin.
- *Axis*: Protects J2EE Web services. The Axis Enforcer plugin is installed into the Axis Engine.

For details on how to configure one of these new Enforcer plugins, see Chapter 8, *Configuring the Enforcer plugins* in the *HP OpenView Select Access 6.0 Installation Guide*.

Simplified Enforcer plugin installation and configuration

All Select Access Enforcer plugins now use the Select Access installer and Setup Tool to install and configure the plugins you require. That means manual installation and configuration of less-frequently-used Enforcer plugins is no longer required. For details on how to install and configure any of the Enforcer plugins that required manual intervention in version 5.0 of Select Access, see Chapter 8, *Configuring the Enforcer plugins* in the *HP OpenView Select Access 6.0 Installation Guide*. For a complete list of Enforcer plugins shipped in this release of Select Access, see Chapter 2, *Select Access: components and requirements* in the *HP OpenView Select Access 6.0 Installation Guide*.

New conditional rule to capture administration workflow

The Policy Builder now includes a new conditional rule that can be triggered against specific delegated administrator and resource tree entry combinations that require approval for any change the administrator tries to submit for that entry. This workflow conditional rule is created and set in a similar manner as other policy rules. The workflow condition adds an additional layer of security in business

environments that require multiple levels of delegation to prevent inadvertent or deliberate loss of corporate assets and information. For more information on workflow, see Chapter 2, *Using administration workflow* in the *HP OpenView Select Access 6.0 Policy Builder Guide*.

Chapter 3

Known issues

Select Access 6.0 shipped with the following known issues. These issues are categorized by topic:

Documented installer/uninstaller issues

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

Enforcer plugin libraries not properly installed on Solaris/Linux

When installing Select Access on Solaris or Linux, if you choose to install only the TCP Enforcer plugin, not all the required C/C++ libraries are installed.

To ensure that the necessary libraries are installed, you should install at least one other C/C++ Enforcer plugin, which include the Apache, IIS, Sun ONE, Domino or Oracle plugins.

Unable to view the log file on Windows

Upon completion of the Select Access installation, if errors were generated, the installer displays a **View install log** box so that you can review the messages for those errors. However, on Windows, checking this option does not automatically display the log file.

The problem is that the Windows installer is not correctly identifying the state of the check box rather than a problem generating the log file. To view this file, you can open it manually from the following location:

```
<install_path>\log files\install_log.txt
```

Not all files removed during an uninstallation

At the completion of the unistallation process, the Select Access uninstaller may leave a number of files on your machine. Note that this is intentional. The uninstaller only removes those files that were installed by the Select Access installer. Because configuration, log and initialization files are user-created files that were not installed by the installer, they are left behind.

If you want to remove these files, you must do so manually after the uninstaller has completed the removal of Select Access.

Out of memory error when installing on HP-UX

When installing Select Access on HP-UX, an out of memory error may sometimes be generated. If this occurs, you will need to adjust the `maxdsiz` parameter in the kernel configuration in the HP-UX System Administration Manager (SAM) to increase the size of the kernel. To adjust this parameter, follow these steps:

1. Start the System Administration Manager.
2. Double-click **Kernel Configuration**.
3. Double click **Configurable Parameters**.
4. Double click on the `maxdsiz` parameter.
5. Change the value of `maxdsiz`. HP recommends a value of 2 063 835 136 to ensure that the installer does not run out of memory.
6. Exit the SAM and create a new kernel, then reboot.

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.

Partial installation affects uninstall

Problems can occur with the uninstaller if you do the following during the installation of Select Access 6.0:

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.

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:

- *Password management*: Users can only change passwords if ADS is running over SSL. Therefore, you cannot create user accounts that require passwords, modify passwords, or use password management, unless SSL is enabled.
- When logging on to ADS, note that Select Access must logon as local user. This is because standard user privileges do not allow Select Access components the read/write/modify schema access they require for all the entries accessed in ADS.
- *Schema management*: You must enable schema management with ADS. To enable schema management, run the registry file we provide for this purpose before installing Select Access. You can find this file on the Select Access product CD in the following location:

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

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 6.0 Policy Builder Guide*.

- *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

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 6.0 Network Integration Guide*.

- *Authentication servers names cannot use umlauts when data signing is enabled:* DirX servers do not allow you to include umlauts in the names of authentication server when Data Signing is enabled. This is because data signing uses a case sensitive string type and DirX does not allow umlauts for case-sensitive string types.
- *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 6.0 Network Integration Guide*.
- *Authentication servers names cannot use umlauts when data signing is enabled*: eTrust servers do not allow you to include umlauts in the names of authentication server when Data Signing is enabled. This is because data signing uses a case sensitive string type and eTrust does not allow umlauts for case-sensitive string types.

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. For details, see Chapter 5, *Preconfiguring a directory server* in the *HP OpenView Select Access 6.0 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 generate an error because the index nodel value is too low. If you encounter this problem, you must reconfigure this setting.

  To set the correct maximum CP index node value:

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

     `<CP_install_path>/ds.properties`

  b. Locate the following parameter and ensure that it has the corresponding value:

```
directory.indexNodeMax=524288
```

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

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

Syntegra Aphelion

As of Select Access 6.0, Syntegra Aphelion is no longer a supported directory server.

Documented Administration server/Setup Tool issues

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

Policy Validator inherits audit settings from Administration server setup

An issue exists when you are configuring the Select Access components for the first time after an installation. If, during this initial component setup, you configure the Administration server's audit settings, then configure the Policy Validator during the same Setup Tool session, the Policy Validator configuration inherits the audit settings you configured for the Administration server.

In most cases, these settings do not cause a problem; these settings can be modified, or may be your preferred settings anyway. However, if you configured the Administration server to log to a database, a problem arises because the Policy Validator is not capable of logging to a database. In this case, you cannot modify the offending entry in the Policy Validator's audit configuration; you must manually delete it. Otherwise an error is generated and messages are automatically logged to the system log.

Delegated Administrators cannot rename entries

An issue exists when running the Policy Builder in delegated mode. Delegated administrators who have been given permission to modify specific entries cannot rename the entry (that is, modify the cn attribute) unless they have been given access to the parent entry. However, they are permitted to modify any other attribute.

Password policy issues when the first name is blank

An issue exists with the Administration server in which it does not always enforce password policy when a user's first name is left blank. This may allow users to specify passwords that include part of their name or user id.

To avoid this issue, administrators should ensure that they provide a first name for all users. In addition, when setting up self-registration for users, the **First Name** field should be made a mandatory field.

CA certificate is not exported

When you attempt to export the properties of a SAML partner to a file in the **Setup SAML Server's Assertion Properties** dialog, the Setup Tool does not insert the CA certificate associated with the connection into the file. This functionality works as intended; the CA certificate should not be exported.

Registration via the Administration server does not work in Chinese

An issue exists when user tries to register through the Administration server when the registration authentication server has a chinese name. Users cannot access the registration page in order to register because the correct name of the registration authentication server is not provided.

Self-Management URLs must be lowercase

When defining the URL for the Self-Management resource in the Administration server setup, you must use all lowercase. If you attempt to use a URL with mixed case or upper case, a 404 error (resource not found) is returned.

Error when restarting IIS during Enforcer plugin setup

An issue exists on Windows 2003 when configuring the IIS Enforcer plugin for an existing IIS Web server. Upon the completion of the Enforcer plugin setup process, if you check the **Restart Web Server** option and click **Finish**, the Setup Tool will occasionally generate an error stating that the IIS Web Server is not installed.

However, if you click **Continue** in the error dialog, then re-click **Finish** to complete the setup process, the Setup Tool is able to successfully complete the configuration and restart the Web server.

Workflow Administration screens show incorrect number of approvers

When viewing a workflow change request, or checking the status of a previously submitted request, the incorrect number of approvers is shown if one or more of the approvers is a group, role or folder. This is because the Administration server does not know how many members are contained in these entries, or which approvers are included more than once. The following pages are affected:

- On the **Workflow Change Description** page, the **Approvals** field is incorrect. Each role, group, and folder is calculated as a single approver.
- On the **Workflow Approval Status** page, the following fields are incorrect:
  - **Decision Point Requirements**. Each role, group, and folder is calculated as a single approver.
  - **Not Responded**. The field shows the folder's DN as an approver DN.

Browsing issue in Workflow Administration screens

An issue exists when using the > and >> links to browse through multiple pages of workflow change requests. After approving a change request, these links do not function as expected, bringing you back to the main **Workflow Change Request** page instead of the next page in the list of requests. However, from this page, they again function as intended.

Web Administration display of entries can be unclear

In Web Administration, the hostname of the user location is not displayed when you attempt to locate an entry using the **Show All Entries** option, which may lead to confusing results. This option returns a flat list of entries with the names of the user locations.

A problem could arise if multiple user locations exist with similar hierarchy and entry names. Entries from two different user locations could appear identical. In this case, you should use the **Browse** option to locate your entries.

User added to group before workflow request is approved

An issue exists with Web Administration when workflow is applied. When an administrator who has been configured with workflow uses Web Administration to add a user to a group, the user appears to be added to the group before the change request has been approved.

This is an issue with the Web Administration JSP. Despite appearing as added in Web Administration, the group is not modified on the directory server until the change is approved.

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. 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.

Limitations after directory data upgraded

When you first run the new Administration server, it automatically connects to the directory server and detects if data from a previous installation exists. If so, it updates the data to use Select Access 6.0 formats as well as upgrading the schema to support new features (if permitted by the directory server).

Once this upgrade process happens, you cannot use an earlier version of Select Access with this data.

Documented Policy Validator issues

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

Policy Validator not automatically clearing cache

When administrators use the Web Administration application to add or modify user entries and workflow is not applied, the application does not force the Policy Validator to clear the cache. Clearing the cache forces the Policy Validator to retrieve the latest data from the directory server. Until its cache is cleared, the Policy Validator will be unaware of any changes to the User Store, and therefore may be validating users based on old information.

In this case, you must clear the cache manually in order for your changes to take effect immediately. You can clear the cache by selecting **Tools>Clear Validator Cache(s)**.

Note that this does not pose a security risk. Because the Web Administration only modifies user entries and cannot set policy, the problem is restricted to denying access where it should be allowed, rather than mistakenly allowing users to access to restricted resources.

Incorrect reason for authentication failure given

An issue exists with registration authentication via the Policy Validator. When using registration authentication via the Policy Validator, the Policy Validator does not always provide the correct reason for an authentication failure.

Policy Validator cannot start when policy signer certificate is chinese

An issue exists when you configure the Policy Validator to use certain certificates for policy signing. If the certificate you have specified to sign policy with contains chinese characters in its subject, the Policy Validator is unable to start.

You must choose a certificate without chinese characters.

Documented Policy Builder applet issues

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

Thresholds do not work for the Administrative Access Tree

When you set the threshold value for the Administrative Access tree in order to limit the number of entries that will be displayed, the setting is not immediately recognized by the Policy Builder; opening an item that contains more entries than the specified value will still return all the contained entries.

However, if you exit and then restart the Policy Builder applet, the threshold value you set in the previous session is recognized.

HP is aware of this issue and will correct it in a future release.

Problems when multiple instances of Rule Builder are open

Opening multiple instance of the Rule Builder utility from the Policy Builder applet may cause the Policy Builder freeze or behave unpredictably. You can open multiple instances of the Rule Builder if you access it directly from the Policy Builder's Policy Matrix while the one instance is already open (right-click, select **Create/Modify Conditional Rule** or **Create/Modify Workflow Rule**).

The Policy Builder was not intended to operate with multiple instances of the Rule Builder open. To avoid potential problems, ensure that you do not use the **Create/Modify Conditional Rule** or **Create/Modify Workflow Rule** menu items when the Rule Builder is already open, but rather create or modify the rules from the Rule Builder window directly.

Policy Builder not refreshing after Network Discovery

A Java error sometimes occurs in the Policy Builder after running Network Discovery, which results in the Resources tree not being properly refreshed. Clicking **Refresh** on the **View** menu will cause the correct information to appear under the resource tree.

Deleting the Delegated Administration Enforcer plugin

The Policy Builder erroneously allows users to delete the delegated administration enforcer from the **Component Configuration** window. This Enforcer plugin should never be deleted.

The **Component Configuration** window is only available to the Select Access super administrator running the Policy Builder full administration mode, or by those administrators who have been delegated access to this function. To ensure that this component is never deleted, HP recommends applying a workflow condition on the Component Configuration administrative function when delegating this privilege.

Naming rules and authentication methods

When naming new rules or authentication methods, the Policy Builder may allow you to enter invalid characters, such as commas. When you try to open the resource later, the resource will be invalid. When naming a rule or authentication server, you must use only the following alphanumeric characters: A-Z, 0-9, _ (underscore). All other characters are invalid and should not be used.

Cannot run both Policy Builder applets on the same machine

An issue exists which prevents users from running Policy Builder in both the full administration mode and delegated administration mode on the same machine.

You can work around this issue in one of the following ways:

- By opening each mode in a different browser (that is, one in Netscape, one in Internet Explorer).
- In Internet Explorer, by disabling the **Reuse windows for launching shortcuts** option.

  To disable this option:

  a. In Internet Explorer, select **Tools>Internet Options**.

  b. In the **Internet Options** dialog, select the **Advanced** tab.

  c. In the **Advanced** tab, under the Browsing category, locate the **Reuse windows for launching shortcuts** option and disable it.

X11 display error after rebooting in delegated mode on Solaris

A display issue exists with the Policy Builder in delegated mode on Solaris. When using the Policy Builder in delegated mode, rebooting your machine without closing down the Policy Builder can cause the following error the next time you try to start the Policy Builder:

```
Can't connect to X11 window server using ':0.0' as the
value of the DISPLAY variable.
```

The workaround for this issue involves exporting the display variable via a shell script, as follows:

```
DISPLAY=<host_name>:0.0; export DISPLAY
```

where *<host_name>* is the IP address of the machine.

Documented Enforcer plugin issues

HP has documented and is aware of the following issue with the following Enforcer plugin.

The servlet Enforcer plugin requires additional JAR files

In order to use the servlet Enforcer plugin, you must first download the JCE extension from Sun's Web site. Due to legal restrictions, HP cannot ship this extension with Select Access.

To download this extension, go to:

```
http://java.sun.com/products/jce/index-122.html.
```

After you unpack the zip file, you'll find jar files in the lib directory. You'll need to add `jce1_2_2.jar`, `US_export_policy.jar` and `local_policy.jar` to your `CLASSPATH`. You should then be able to run under the JRE1.3.

POSTing issue with international characters

When a Web browser POSTs data that includes non-ASCII characters, (for example, Chinese characters or letters with diacritical marks such as umlauts) and when SA triggers either POST-over-auth or POST-over-MDSSO in order to authenticate the user, the Enforcer plugin cannot restore the initial POST request so that the Web application can continue processing. The non-ASCII data becomes distorted.

To avoid this problem on the C++-based Enforcer plugins (Sun ONE, IIS, Apache, IBM HTTPD, Domino, Oracle), encode the following three forms in `<install_path>/content` directory to use the default character set used by the application rather than UTF-8:

- `Post_accepted.html`
- `Post_password_changed_form.html`
- `Post_redirect.html`

To make this change, locate the following entry:

```
<meta http-equiv="Content-Type" content="text/html;
charset=utf-8">
```

and change it to:

```
<meta http-equiv="Content-Type" content="text/html;
charset=<site_character_set>">
```

You do not need to make any code changes to these C++-based Enforcer plugins or to the Policy Validator.

Be aware that once the changes are made, the web server will only be able to handle characters of the specified character set. In order to support all languages, you MUST convert the entire Web site to UTF-8.

The processing of these characters remains a documented issue for the servlet Enforcer plugin. Therefore, HP recommends that you ensure that the user is authenticated before they POST data to avoid triggering these POST-over functions.

IIS Enforcer plugin cannot log to a file on Windows 2003

When running IIS6 with the IIS Enforcer plugin on Windows 2003, the Enforcer plugin is unable to log messages to a file unless the proper permissions have been assigned. In order to configure IIS6 to log to a file, the `NETWORK_SERVICE` account must have write permission to the log file.

In addition, if IIS6 is configured for Integrated Windows Authentication (IWA), then write permission must be given to all possible users. The reason for this is because IIS will impersonate the user and serve the request under that user account. Because the IIS Enforcer plugin code is not executed until after the impersonation

takes place, the user must have write permission to the log file in order for messages to be logged there.

Enforcer plugins cannot reliably access POST data

There is a known issue that exists with all Select Access Web server Enforcer plugins when reading POST data. These Enforcer plugins are not able to reliably read POST data unless that data comes from one of the forms shipped with Select Access. This is because POST data is not always made available to Select Access when and where it is expected.

For example, in IIS, POST data is fully available in ISAPI extensions, but might not be available in all ISAPI filters. Because the IIS Enforcer plugin is installed as an ISAPI filter, it can only read POST data when it is made available at the filter level.

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 does not 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.

  One exception exists: If you are using Registration Authentication via the Administration server to register new users and the Administration server and Web server are on different machines or domains, you will need to set certain SSO and/or MD-SSO parameters. For more information, see *Registration servers* on page 85 of the *HP OpenView Select Access 6.0 Policy Builder Guide*.
- C*ertificate 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 issue with the following Web server.

Cannot discover resources under Apache 2

An issue exists when trying to discover resources on Apache 2. The Network Discovery plugin is unable to locate existing resources on an Apache 2 web server.

The problem appears to be with an Apache 2 configuration parameter that is preventing the Network Discovery plugin from searching the server. To allow the Network Discovery plugin to run without incident, comment out the following parameter in the `httpd.conf` file of your server:

```
# AddDefaultCharSet ISO-8859-1
```

Apache hangs on HP–UX

Before configuring Select Access's Apache Enforcer plugin on HP-UX, 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 enhance security for Select Access's implementation of personalization, Enforcer plugins now export personalization attributes as variables that are prefixed with HTTP_SA instead of HTTP_ or HTTP_BSA as in previous releases. If you are upgrading to Select Access 6.0, you must modify your Web server scripts to use this new prefix or user our backwards compatibility flags, available through the **Custom Settings** setup wizard in the Setup Tool.

With this prefix modification, the Apache Enforcer plugin and Sun ONE (iPlanet) Enforcer plugins can now 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 now 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 6.0 Network Integration Guide*.

Enabling backwards compatibility when this prefix change is restrictive

If you have many Web server scripts that makes the implementation of this security enhancement restrictive, you can set the **USE_OLD_P13N** flag in the Custom settings of the Setup Tool. By enabling this mode, you configure Select Access to use the Select Access 5.0 implementation of personalization.

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 documentation issues

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

Upgrading from versions of Select Access previous to 5.0 not supported

The *HP OpenView Select Access 6.0 Installation Guide* erroneously includes information regarding upgrading from a version of Select Access previous to Select Access 5.0. In fact, upgrading from a version previous to 5.0 is not supported.

Incorrect value given for CA eTrust setting

In Chapter 5, *Preconfiguring a directory server* of the *HP OpenView Select Access 6.0 Network Integration Guide*, in the section entitled *To modify the maximum operation parameter* on page 62, the incorrect value is given for this parameter. To ensure that the correct number of search results can be returned, the `max-op-size` parameter should be configured with a value of 2000, not 1000 as stated in the guide.

Incorrect filename given

In Chapter 5, *Preconfiguring a directory server* of the *HP OpenView Select Access 6.0 Network Integration Guide*, in the section entitled *To upgrade Select Access schema files for CP Directory v4.1* on page 64, the incorrect filename is given. When upgrading CP Directory 4.1 for use with Select Access 6.0, you must upload the following file:

```
4.1_upgrade_schema_ext_for_SelectAccess_5.1_to_6.0.ldif.
```

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.