CA SiteMinder®

Policy Server Release Notes

r6.0 SP 5

Contact CA

Contact Technical Support

For your convenience, CA provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA products. At http://ca.com/support, you can access the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Provide Feedback

If you have comments or questions about CA product documentation, you can send a message to techpubs@ca.com.

If you would like to provide feedback about CA product documentation, complete our short customer survey, which is also available on the CA Support website, found at http://ca.com/docs.

Contents

Chapter 7: General Considerations 51

Chapter 1: Welcome

This document contains operating system support, installation considerations, known issues, fixes, and information about contacting CA Technical Support.

Chapter 2: New Features

This section contains the following topics:

Updated Instructions for using SiteMinder with Microsoft® SharePoint

Updated instructions for protecting resources on a Microsoft SharePoint server with SiteMinder are available from the CA Technical Support site in the following document:

- TEC484560

Kerberos Authentication

SiteMinder may be configured to use the Kerberos Authentication scheme to protect resources in a Kerberos domain.

Note: More information on using the Kerberos Authentication scheme exists in the *Policy Design Guide*.

Credentials Selector for Strong Authentication

The SiteMinder Credentials Selector lets you configure an authentication environment that presents an end user with a choice of credentials for logging in to a site to access a resource. The authorization decisions and user responses can be configured to depend on the end user's choice of authentication credentials.

For example, a user requests access to a protected application that provides him with a certain spending level for online purchases. A dialog box opens with a choice of basic authentication (Username and Password) or smart card authentication (SecureID or SafeWord).

If the user supplies only a valid Username and Password, the authentication level is 5 and his spending level is $1000. If the user supplies a valid Username and Password and checks the smart card authentication check box, he is prompted for his smart card PIN. Assuming that the PIN he provides is valid, the authentication level becomes 15, which allows the user a spending level of $5,000.

Note: For more information about the Credentials Selector, see the Credentials Selector technical note on the Technical Support site.

Solaris 10 Certification

The Policy Server and Web Agent are certified for global and non-global zones on systems running Solaris 10.

Note: For more information about Solaris 10 support, see the *Policy Server Installation Guide*.

Directory Mapping Configurations

Directory mapping now supports a configuration that lets SiteMinder authenticate users against one directory and validate users against another.

As a result, you can use the single sign-on (SSO) feature across multiple user directories in separate policy stores, even if the user directory name or user DN differs across individual user stores for the same user identity.

Note: For more information about configuring directory mappings, see the *Policy Design Guide*.

Oracle Support for iRecorder for SiteMinder

The CA Security Command Center (SCC) is now able to read security-related log data from the SiteMinder SQL Server and Oracle logs database.

Note: For more information about upgrading the 6.x audit log database schema to support the SiteMinder/CA SCC integration, see the *Upgrade Guide*. For more information about the iRecorder, see the *Audit iRecorder Reference Guide*.

Resetting Policy Server Statistics

There is a new debugging option to troubleshoot the Policy Server. To use debugging options, run the Policy Server process, smpolicysrv, interactively in a command window with debugging options turned on.

The following command lets you log Policy Server statistics to the Policy Server log file:

```
smpolicysrv -stats
```

However, resetting the statistics required you to restart the Policy Server.

The following command now lets you reset Policy Server statistics without restarting the Policy Server:

```
smpolicysrv -resetstats
```

The -resetstats switch resets the following counters:

- Max Threads is reset to the Current Threads value.
- Max Depth of the message queue is reset to the Current Depth of the message queue.
- Max Connections is reset to Current Connections.
- Msgs, Waits, Misses, and Exceeded limit are reset to zero.

The -resetstats switch does not reset the following counters:

- Thread pool limit
- Current Threads
- Current Depth of the message queue
- Current Connections
- Connections Limit

Note: For more information about troubleshooting the Policy Server, see the *Policy Server Management Guide*.

New smpolicysrv Command Line Options

You can use two smpolicysrv command line options, -dumprequests and –flushrequests, to troubleshoot and recover more quickly from an overfull Policy Server message queue. Only use these options in the following case:

1. Agent requests waiting in the Policy Server message queue time out.
2. One or more Agents resend the timed-out requests, overfilling the message queue.

Important! Do not use -dumprequests and -flushrequests in normal operating conditions.

Note: For more information, see the *Policy Server Management Guide*.

Chapter 3: Changes to Existing Features

This section contains the following topics:

ODBC SQL Query Schemes

ODBC user directory SQL Query Schemes previously could only be configured to use literal queries. ODBC SQL Query Schemes can now be configured to use literal and bind-based parameters.

Note: For more information on creating bind-based queries, see the *Policy Design Guide*.

Policy Server Profiler Performance Improvement

Trace messages can now be buffered when written to the trace logs, which results in improved Policy Server performance.

Note: For more information on enabling buffered tracing, see the *Policy Server Management Guide*.

Mixed Policy and Key Store Configurations

The Policy Server now supports mixed LDAP/ODBC policy and key stores. The policy store can exist in an ODBC database, and the key store can exist in an LDAP Directory Server, or vice versa.

Note: For more information on configuring policy and key stores, see the *Policy Server Management Guide*.

Key Store Management and Policy Server Behavior

The Policy Server now behaves in the following ways when a key store becomes unavailable:

- When a key store that has been configured separately from the policy store becomes unavailable, the Policy Server goes in to a suspended state and refuses any new requests on established connections until the key store comes back online.
- A Policy Server in a suspended state remains up for the length of time specified in SuspendTimeout, at which point the Policy Server shuts down gracefully. If SuspendTimeout is equal to zero, the Policy Server remains in the suspended state until the key store connection is reestablished.
- When the Policy Server is started and the key store is unavailable, the Policy Server shuts down gracefully.

Note: For more information on key store management, see the *Policy Server Management Guide*.

SiteMinder Policy Server Log File

The SiteMinder Policy Server log (smps.log) has been enhanced to detail the cr at which the Policy Server is operating.

Note: For more information on Policy Server logging, see the *Policy Server Management Guide*.

Policy Server Trace Filter Sub-Components

The Receive Request and Send Response sub-components may be selected from the following components when configuring a Policy Server trace filter:

- Login_Logout
- IsAuthorized

Note: For more information on configuring Policy Server tracing, see the *Policy Server Management Guide*. For more information on the tracing components and their sub-components, see the *Policy Server Management Console Help*.

Policy Server Threading Model

The Policy Server threading model has been enhanced. There are now two separate thread pools to handle messages to the Policy Server.

Note: For more information on how the Policy Server threading model works, see the *Policy Server Management Guide*.

Windows Authentication Scheme

The Policy Server has been enhanced to support a relative path for Windows authentication scheme targets.

Note: For more information on configuring a Windows authentication scheme, see the *Policy Design Guide*.

Persistent Session Validation Period

The Policy Server User Interface has been enhanced to let SiteMinder administrators specify a persistent session validation period in hours, minutes, and seconds.

Note: For more information on configuring persistent sessions in realms, see the *Policy Design Guide*.

Flushing the Policy Store Cache

The "flush all" command has been enhanced to flush the policy store cache. Prior to flushing the policy store cache, you must enable this feature by configuring the FlushObjCache registry key.

Note: For more information, see the *Policy Server Management Guide*.

Password Services Default Redirect URL

The default redirect URL for Password Services has changed from smpwservicescgi.exe to smpwservices.fcc.

Note: For more information, see the *Policy Design Guide*.

Chapter 4: Operating System Support

Before you install the Policy Server, ensure you are using a supported operating system and third-party software. For a list of supported operating systems, Web Servers, databases, Web browsers, LDAP directory servers, and servlet:

1. Log into the Technical Support site.
2. Search for the SiteMinder platform matrix for 6.x

Chapter 5: Software Requirements

This section contains the following topics:

Windows

The following requirements exist for Windows:

- 128 MB system RAM (minimum).
- 250 MB free hard disk space in the install location, and 180 MB of free space in the system's temporary file location.

  Note: These requirements are based on a medium size policy database, which is approximately 1,000 policies.
- Ensure that you have the required JRE version installed. For the required version, search for the SiteMinder Platform Matrix for r6.0 SP5 on the Technical Support site. You can download the latest JRE version at the Sun Developer Network (SDN).

Note: Additional non-system requirements exist in the *Policy Server Installation Guide*.

UNIX

The following requirements exist for UNIX:

- 128 MB RAM
- 300 MB free hard disk space, and 200 MB of free disk space in /tmp.

  Note: Typically, 10 MB or less free disk space in /tmp is required for the daily operation of the Policy Server. The Policy Server creates files and named pipes under /tmp. The path to which these files and pipes are created cannot be changed.
- Ensure that you have the required JRE version installed. For the required version, search for the SiteMinder Platform Matrix for r6.0 SP5 on the Technical Support site. You can download the latest JRE version which at the Sun Developer Network (SDN).

Note: Additional non-system requirements exist in the *Policy Server Installation Guide*.

JDK/JRE Considerations

Consider the following when using a supported JDK/JRE:

- JDK 1.5.0_06 through JDK 1.5.0_09 leaks handles on Windows and Solaris platforms.

  This issue is a result of a Sun Microsystems bug. Refer to Sun bug number 6399321.

- JDK 1.5.0_05 through JDK 1.5.0_09 causes ServletExec to crash on dual processor machines.

Note: For a list of supported CA and third-party components, refer to the SiteMinder r6.0 SP5 Platform Support Matrix on the Technical Support site.

To locate the support matrix from the Support site

1. Click Technical Support.
2. Click Support By Product or Solution.
3. Select CA SiteMinder Web Access Manager from the Select a Product or Solution Page list.
4. Click Platform Support Matrices in the Product Status group box.

You can download the latest JDK and JRE versions at the Sun Developer Network.

Chapter 6: Installation and Upgrade Considerations

This section contains the following topics:

Upgrading the Policy Server from 4.61 SP5J or 6.0 SP1J

Upgrading a Japanese Policy Server to 6.0 SP5 overwrites the localized version. The Japanese Policy Server is not being localized for 6.0 SP5.

Upgrades and Federation Security Services

If you are upgrading from r6.0 SP5 cr04 or earlier and plan on installing the Policy Server Option Pack for Federation Security Services, re-import the SiteMinder policy store schema file (smpolicy.smdif) into your policy stores. A new property has been added to support the use of redirect URLs for SAML 1.x single sign-on. The redirect URLs, which are optional and configured in the SAML 1.x authentication scheme, let you redirect users to another location when authentication problems occur.

For example, if a user cannot federate, you can redirect the user to a registration page.

Note: For new installations, the latest version of the policy store schema file has the necessary entries for redirect URLs. There is no additional setup required.

To define the redirect URL property collection in the policy store:

1. Run the Policy Server installation.
2. Run the following command:

   smobjimport -i*policy_store_schema* -d*sm_admin_user* -w*sm_admin_password* -v

   policy_store_schema

   Specifies the location of the SiteMinder policy store scheme file.

   sm_admin_user

   Specifies the name of the SiteMinder Super User account.

   sm_admin_password

   Specifies the password for the SiteMinder Super User account.

   Important! Do not use the force (-f) flag when re-importing the the policy store schema. The force flag overwrites existing policy store data.

Upgrades and Identity Manager

If you are upgrading from cr15 or earlier and are using ODBC user stores, complete the following procedure for every environment related with an ODBC user store before using Identity Manager:

1. Open the SiteMinder Policy Server User Interface.
2. Open the anonymous authentication scheme related with the environment using the ODBC user store.
3. Click the Schema Setup tab and replace the User DN with User ID.
4. Save the changes.

DN refers to the tblUsers.id field in the ?tblUsers? table of the ODBC user store. The UID is stored in the tblUsers.loginid field.

Example

User ?selfreguser? was chosen as a user for public tasks.

This user has UID = ?selfreguser? (tblUsers.loginid = ?selfreguser?) and DN = ?2? (tblUsers.id = ?2?).

The User DN in the anonymous authentication scheme should be changed from ?2? to ?selfreguser?

Note: If you create a new environment associated with an ODBC user store, ensure this procedure is completed after creating the environment.

MDAC Versions

It is required that the MDAC versions installed on the client and server sides are compatible.

Note: More information exists in the Microsoft MDAC documentation.

Multi-Mastered LDAP Policy Stores

LDAP directories using multi-master technology may be used as SiteMinder policy stores. The following configuration is recommended when configuring an LDAP policy store in multi-master mode:

- A single master should be used for all administration.
- A single master should be used for key storage.

  This master does not need to be the same as the master used for Administration. However, we recommend that you use the same master store for both keys and administration. In this configuration, all key store nodes should point to the master rather than a replica.

  Note: that If you use a master for key storage other than the master for administration, then all key stores must use the same key store value. No key store should be configured to function as both a policy store and a key store.
- All other policy store other masters should be set for failover mode.

Due to possible synchronization issues, other configurations may cause inconsistent results, such as policy store corruption or Agent keys that are out of sync.

Contact SiteMinder Support for assistance with other configurations.

Multi-mastered LDAP User Store Support Limitations (53677)

The multi-mastered LDAP enhancement has the following limitations:

- The Policy Server only supports multi-mastered user stores in a backup capacity. Since Password Services makes frequent writes to the user store, you cannot simultaneously update user information in multiple master instances. In addition, the LDAP implementation could produce out-of-date information or data loss due to delayed replication.
- Multi-mastered support does not extend to custom code such as custom authentication schemes.

Compatibility with Other Products

To ensure interoperability if you use multiple products, such as IdentityMinder, Identity Manager, TransactionMinder, and eProvision, check the Platform Support Matrices for the required releases of each product. The platform matrices exist on the Technical Support site.

IdentityMinder and Policy Server Upgrades

(Valid for SiteMinder environments in which the Policy Servers are being upgrading from cr15 or below and SiteMinder ODBC user store connections are configured)

After upgrading the Policy Server, the following procedure should be completed for every environment associated with an ODBC user store connection before using IdentityMinder:

Updated snmptrap File

This service pack includes an updated snmptrap.conf file. Before installation, back up and save the original snmptrap.conf file, located in *siteminder_installation*\config.

Operational Changes from 5.x

The following features behave differently in version r6.0 SP5.

Failed Password Change Requests

In a 5.5 environment, when a user submits a password change request that contains an invalid current password, the Password Change Information screen appears with a message stating that the old password is incorrect. The user can provide the correct credential and change the password. In r6.0 SP5, the Policy Server redirects the user to the login screen without the message.

Enabling the DisallowForceLogin registry key allows the 5.5 behavior in an r6.0 SP5 environment. The registry key is located at:

HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\PolicyServer

The KeyType must be configured as REG_DWORD and the Value must be 0 (disabled) or 1 (enabled). The registry key is disabled by default.

If a value other than 0x1 is configured, the feature is disabled. If the registry key is disabled, the r6.0 SP5 behavior is in effect.

Effect of Single Policy Server Process on Audit Logging to Text Files (19630)

Prior to SiteMinder 6.0, when the audit logging was configured to write to text files, each Policy Server process added to the configured base filename. The addition included a distinguishing string ("_Acct", "_Adm", "_Auth" or "_Az") and a current date-time string. The r6.0 SP5 single-process Policy Server does not add distinguishing characters to the configured file name (other than appending .<number> when rolling over the log files).

Regarding the effect of new policy stores on audit logging, see Audit Logs (24116).

iPlanet Web Server Startup (24343)

An iPlanet Web server no longer starts automatically after configuration. This applies to all supported platforms.

Policy Server User Interface Requires Sun Java Plug-in

Viewing the Policy Server User Interface on supported versions of Microsoft Internet Explorer requires the Sun Java Plug-in.

To verify that the proper Java Plug-in is installed and enabled

Windows:

1. From the Control Panel, select Java Plug-In.
2. On the Browser tab, make sure that Microsoft Internet Explorer is checked and click Apply.

UNIX:

Follow the instructions for starting the Java Control Panel in the Java Plug-in Developer Guide for JSE 1.4.2.

If the plug-in is not set, the Policy Server User Interface stalls indefinitely at the Downloading Administration dialog box.

If you are still having difficulty getting the Policy Server User Interface to display, run the Policy Server User Interface Browser Compatibility Test. If the panel is a solid box, click Details for troubleshooting information.

Report Files

The Crystal Reports server is not distributed with Policy Server v6.0, as it was with previous releases. Policy Server v6.0 provides sample reports files (.rpt) that are compatible with Crystal Reports 9.0. These files are provided for customer convenience. CA does not provide support for using the sample files.

No Default Policy Store

The r6.0 SP5 Policy Server does not have a default policy store. In addition, Microsoft Access is no longer supported as a policy store. You can find a list of supported databases at the SiteMinder Platform Matrix for r6.0 SP5 on the Technical Support site.

Remote Services Variables Superseded

Remote Services variables are superseded by Web Services variables.

Cache Settings Simplified

The Cache settings in the Policy Server Management Console have been simplified to a single setting.

Changes to the Cache Model

The cache model for SiteMinder r6.0 SP5 differs from the model for 5.x:

- The Policy Store cache is no longer configurable.
- The L2 cache is replaced by self-tuning per-object-class caches.
- The User Authorization (AZ) cache size is configurable using the Policy Server Management Console. The cache can be tuned using the new counters available in the SiteMinder OneView Monitor.

Supported Security Bridge (27028)

The r6.0 SP5 Policy Server supports the 3.1 Security Bridge. Older Security Bridge versions are not compatible with this Policy Server.

Windows Considerations

The following considerations apply to Windows.

Upgrading the Policy Server from cr10 or Later

(Valid for 5.1 Sun ONE directory servers and Windows 2003)

If a 5.1 Sun ONE directory server and the Policy Server are installed on the same Windows 2003 system, upgrade the LDAP SDK to 5.0.8 dated July 17, 2002 or later. Failing to upgrade the LDAP SDK results in Policy Server instability.

Note: Upgrade the LDAP SDK, regardless of the use of the Sun ONE directory server.

Solaris Considerations

The following considerations apply to Solaris.

Solaris 10 Support

The Policy Server and Web Agent are certified for global and non-global zones.

Note: More information on Solaris 10 support exists in the *Policy Server Installation Guide*.

Required Operating System Patches on Solaris (24317, 28691)

The following table lists required and recommended patches by version:

	Required	
Solaris 8	■ 108827-36 or any superseding patch ■ 108434-09 or any superseding patch (C++ compiler patch from 108434-13) ■ 10843421 ■ 112438-01 (to install the /dev/random interface) ■ 111721-04	The latest recommended patch cluster
Solaris 9	■ 111722-04 or any superseding patch ■ 111711-15 or any superseding patch	none

You can find patches and their respective installation instructions at SunSolve (http://sunsolve.sun.com).

Errors in the SMPS Log due to a gethostbyname() Error (54190)

Network connectivity errors appear in the smps log when gethostbyname() is called. These errors appear even though the directories are available on the network. This was a Solaris issue, which according to Sun bug ID 4353836, has been resolved. Sun lists the following patches for Solaris 8 and 9:

Solaris 8

- 108993-27 libc, libthread and libnsl, ldap patch. This patch has a dependency on KU 108528-24)
- 108820-02 nss_compat.so.1 patch
- 115583-01 /usr/lib/nss_user.so.1 patch

- 109326-11 libresolv.so.2 and in.named patch
- 113648-02 /usr/sbin/mount patch
- 115827-01 /sbin/sulogin and /sbin/netstrategy patch

Solaris 9

- 112874-16 (libc)
- 113319-12 (libnsl)
- 112970-05 (libresolv)
- 115545-01 (nss_files)
- 115542-01 (nss_user)
- 115544-01 (nss_compat)

Policy Server Fails to Connect to LDAP User Stores (82268, 67022)

The Policy Server fails to connect to LDAP user stores that use SSL certificates with AKI extensions.

Solution

This is a known issue with the Solaris SSL driver that occurs when it communicates with a Windows 2003 server. To solve this problem, replace the following five libraries with newer versions by installing the patch that corresponds to your version of Solaris:

- libplc4.so
- libnspr4.so
- libplds4.so
- libssl3.so
- libnss3.so

The Solaris patches are:

Solaris 8: 119209-12

Solaris 9: 119211-12

Solaris 10: 119213-12

The libraries are installed in the following locations:

- The Solaris 8 and 9 patches install the libraries in the following directory: /usr/lib/mps/secv1.
- The Solaris 10 patch installs the libraries in the following directory: /usr/lib/mps.

Verify that the NSS libraries are version 3.9.3 or greater and that the NSPR libraries are version 4.5 or greater.

Note: For Solaris 10, the newer libraries may already be in place, and the patch may not be needed.

Red Hat Enterprise Linux AS and ES Considerations

The following considerations apply to Red Hat Enterprise Linux AS and ES.

Policy Server and Red Hat Enterprise Linux AS

The Policy Server was built using gcc 3.2.3 on Red Hat AS 3.0.

Updated Database Drivers for Red Hat Enterprise Linux AS 3.0 to 5.1 (42834, 47304)

If you are upgrading from 6.0 SP3 or earlier, the ODBC database drivers for Red Hat Enterprise Linux AS have been updated with new drivers. As a result, if your Linux Policy Server is using these drivers to connect to an ODBC policy store, you must update the DSN connection information in the system_odbc.ini file with the new driver settings.

SiteMinder SDK and Red Hat Enterprise Linux AS (28203, 28268)

The SiteMinder SDK was built using gcc 3.2.3 for Red Hat AS 3.0.

Red Hat Enterprise Linux AS Requires Korn Shell (28782)

A Policy Server installed on Red Hat AS requires the Korn shell. If you do not install a Korn shell on Red Hat AS, you cannot execute the commands that control the Policy Server from a command line, such as start-all and stop-all.

Excluded Features on Red Hat Enterprise Linux AS

The following features are not supported by the Policy Server on Red Hat AS:

- Cryptocard authentication scheme
- OCSP
- Safeword authentication scheme
- SiteMinder Test Tool
- Teleid authentication scheme

Apache 2.0 Web Server and ServletExec 5.0 on Red Hat Enterprise Linux AS (28447, 29518)

To use Apache 2.0 Web Server and ServletExec 5.0 on Red Hat AS

1. Run the ServletExec 5.0 AS installer against Apache 1.3.x.

   The ServletExec AS Java instance is created.

2. Run ServletExec and Apache 1.3.x, and make sure you can run /servlet/TestServlet.

3. Shutdown Apache 1.3.x, but leave ServletExec running.

4. Using anonymous FTP, access ftp://ftp.newatlanta.com/public/servletexec/4_2/patches and download the latest zip.

5. Extract the following from the zip:

   mod_servletexec2.c

6. Edit the httpd.conf file of your HP-Apache 2.x so that it contains the necessary ServletExec-specific directives.

   Note: The directives are also present in the httpd.conf file of your Apache 1.3.x if you allowed the ServletExec installer to update the httpd.conf during installation. For more information on editing the httpd.conf file, refer to the New Atlanta Communication ServletExec documentation.

7. Start Apache 2.x.

8. Test the Web Server with ServletExec by accessing:

   /servlet/TestServlet

HP-UX Considerations

The following considerations apply to HP-UX.

Required Operating System Patches on HP-UX

The following table lists required and recommended patches by version:

Version	Required	Recommended
HP-UX 11i	KRNG11i, PHSS_26263, PHCO_29029	none

Note: You may replace the above patches with the latest ld and linker tools cumulative patch.

It is recommended that you install the June 2003 or the latest available patch bundle for HP 11.x Operating system.

HP maintains a list of the recommended patches for using Java1.4.1. at: http://h18012.www1.hp.com/java/patches/index.html

Kernel Parameters

HP provides a tool called HPjconfig, which gives the list of recommended Kernel parameters for executing Java on HP-UX systems. Because the Policy Server uses Java, this tool should be used to determine the recommended Kernel Parameters. You can search for this tool at the HP Web site: http://www.hp.com.

Excluded Features on HP-UX

The following features are not supported by the Policy Server on HP-UX

- Cryptocard authentication scheme
- Safeword authentication scheme
- Teleid authentication scheme
- SiteMinder Test Tool
- FIPS or Ipv6

Apache 1.3.28 Web Server Installation Fails on HP-UX 11i (28327) (28302)

When you install the Apache 1.3.28 Web Server on HP-UX 11i, the installation program fails and issues a parsing error in the socket.h file during gmake. You can resolve this issue doing one of the following:

- Rename the types.h header file
- Compile Apache using the native HP compiler

To rename the types.h header file

1. Rename the types.h header file that comes with the gcc installation to types.old.

   Note: The file is located in usr/local/lib/gcc-lib/hppa2.0n-hp-hpux11.00/3.2/include/sys

2. Move the types.h system header file from /usr/include/sys to the latter directory.

To compile Apache using the native HP compiler

1. Export and set the variable CC to the following: cc -Ae +02
2. Run the Apache configuration script.
3. Run gmake.

Apache 2.0 Web Server and ServletExec 5.0 on HP-UX 11i (29517, 28446)

To use Apache 2.0 Web Server and ServletExec 5.0 on HP-UX 11i

1. Install Apache v1.3.x.
2. Run ServletExec 5.0 AS installer against Apache 1.3.x.

   The ServletExec AS Java instance is created.

3. Run ServletExec and Apache 1.3.x, and make sure you can run /servlet/TestServlet.
4. Shutdown Apache 1.3.x, but leave ServletExec running.
5. Install HP-Apache v2.x from the .depot file.

   Note: By default, this file is installed in /opt/hpws/apache directory.

6. Modify the apxs script by changing:

   $opt .= " -module -avoid-version $apr_ldflags

   to

   $opt .= " -rpath $CFG_LIBEXECDIR -module -avoid-version $apr_ldflags

   The extra parameter indicates that the created library will be installed in $CFG_LIBEXECDIR

   Note: This script is located in the /opt/hpws/apache/bin directory.

7. Using anonymous FTP, access ftp://ftp.newatlanta.com/public/servletexec/4_2/patches/ and download the latest zip file.

8. Extract the following file from the zip:

   mod_servletexec2.c

9. Execute the following command:

   apxs -n servletexec -i -a -c -D XP_UNIX -D APR_WANT_BYTEFUNC mod_servletexec2.c

10. Edit the httpd.conf file of your HP-Apache 2.x to contain the necessary ServletExec-specific directives.

    Note: The directives are also present in the httpd.conf of your Apache 1.3.x if you let the ServletExec installer update the httpd.conf during installation. For more information on editing the httpd.conf file, refer to the New Atlanta Communication ServletExec documentation.

11. Start HP-Apache 2.x.

12. Test the Web Server with ServletExec by accessing the following:

    /servlet/TestServlet

More Secure smpolicy.smdif File (70643, 69813)

When manually configuring a policy store on Windows, you can choose one of two .smdif files:

- smpolicy.smdif
- smpolicy-secure.smdif

The file smpolicy-secure.smdif provides additional security through enhanced default Web Agent configuration parameters. For more information, see the *Policy Server Installation Guide*.

Chapter 7: General Considerations

This section contains the following topics:

IdentityMinder Object Support in Policy Stores (29351)

Policy Servers that have not been enabled for IdentityMinder cannot be connected to policy stores that contain IdentityMinder objects. Policy Servers that have been enabled for IdentityMinder 5.6 SP2 can be connected to r6.0 SP5 policy stores that contain IdentityMinder objects.

Note: For more information about configuring and deploying IdentityMinder, see the *IdentityMinder Web Edition Installation Guide*.

NTLM Authentication Scheme Replaced by Windows Authentication Scheme

This service pack does not include an NTLM authentication scheme template. This authentication scheme type has been replaced by the Windows Authentication template. Support for NTLM authentication is now provided through the new authentication scheme template.

Unsupported Features

The following features are not supported by SiteMinder:

- Identity Manager roles
- Cryptocard authentication scheme on Red Hat AS and HP-UX
- SafeWord authentication scheme on Red Hat AS and HP-UX

- TeleID authentication scheme on Red Hat AS and HP-UX
- DMS on Red Hat AS and HP-UX
- SiteMinder Test Tool on Red Hat AS and HP-UX
- OCSP on Red Hat AS
- Password services with Microsoft Active Directory Global Catalog
- Enhanced LDAP referrals with Microsoft Active Directory Application Mode (ADAM)
- Enhanced LDAP referrals with Novell eDirectory
- Enhanced LDAP referrals with Oracle OID 9.0.4 (Oracle bug 3512354)
- Enhanced LDAP referrals with Siemens DirX is only supported for searches and writes. That is, password services write referrals is supported. However, enhanced referrals for binds and thus authentication is not supported.
- FIPS and IPV6 on HPUX Policy Server

System Management Limitations

The following system management limitations exist:

OneView Monitor GUI Alert Issue in Netscape 6.2.3 Browser (23634) (23128)

Alerts do not work in a OneView Monitor GUI window running in a Solaris Netscape 6.2.3 browser.

OneView Monitor GUI alerts do work in IE and higher versions of Netscape.

Pop-up Blockers May Interfere with Help

Certain pop-up blockers prevent the Policy Server User Interface help window from opening. Many pop-up blockers allow the pop-up if you press CTRL while you click the link.

Registry Setting No Longer Required for Setting the Maximum Number of Connections (27442)

In previous versions of the Policy Server, two ODBC connections were created for each Policy Server service. The following registry setting overrode the default value and indicated the maximum total number of ODBC connections created by the Policy Server for all services:

Netegrity\SiteMinder\CurrentVersion\Database\UserDirectoryConnections

For r6.0 SP5 Policy Servers, the maximum number of connections is determined dynamically, based on five times the maximum number of threads specified in the Policy Server Management Console. (See the Performance group box of the Settings tab in the Management Console.)

If you are upgrading to the r6.0 SP5 Policy Server from a 5.x Policy Server, remove the UserDirectoryConnections registry setting. If you do not, and the value specified by the setting is less than the maximum number of threads calculated by the Policy Server, your Policy Server logs will contain many error messages. These messages will indicate that the value of the registry setting overrides the maximum number of connections calculated by the Policy Server.

Policy Server Limitations

The following Policy Server limitations exist:

Text Truncated When Installing Policy Server Using Exceed (25757)

Running the Policy Server installer (nete-ps-6.0-sol.bin) or Policy Server Configuration Wizard (nete-ps-config.bin) using Exceed can cause text in the dialog box to truncate due to unavailable fonts on the Exceed server. This limitation has no affect on the Policy Server installation or configuration.

Error Changing Long Password When Password Services is Enabled (26942)

If the Policy Server has Password Services enabled, changing the password may fail if the old password length exceeds 160 UTF8 octets and the new password length exceed 160 UTF8 octets.

Leading Spaces in User Password May Not Be Accepted (27619)

A user whose password includes leading spaces may not be able to authenticate under the following combination of circumstances:

- The Policy Server is running on Solaris.
- The password with leading spaces is stored in an LDAP User Store.

Note: A password policy may or may not be enabled.

A related limitation has also been observed:

When an administrator attempts to set a user's password with leading spaces using the Netscape LDAP Console, the console removes the spaces before storing the password (if the Policy Server Admin UI is used to set the password, the spaces are left intact).

DMS Configuration Wizard Next Button Disabled in Netscape 6.2.3 Browser (27208)

On Solaris 2.8 or 2.9, if you are running the Policy Server User Interface using a Netscape 6.2.3 Web browser, the Next button on the Delegated Management Services Configuration Wizard is disabled, which keeps you from being able to run the wizard. To fix this problem, run the Policy Server UI through a Netscape 7.0 browser. You can access this wizard by selecting Tools > DMS Config Wizard.

Netscape 6.2.3 Browser Causes Missing Attribute Types in Response Attribute Editor (27214)

On Solaris 2.8 or 2.9, if you are running the Policy Server UI using a Netscape 6.2.3 Web browser, the Attribute drop-down menu in the SiteMinder Response Attribute Editor dialog box only lists the WebAgent-HTTP-Header-Variable response attribute type, which is incorrect since there should be several choices. This problem is caused by running the Policy Server UI using a Netscape 6.2.3 browser. To fix this problem, run the Policy Server UI with a Netscape 7.0 browser.

To access this dialog box

1. Select Edit > Create Response on the Domains tab.
2. Click Create.

Netscape 6.2.3 Browser Causes Unreadable Date in Time Dialog (27199)

On Solaris 2.8 or 2.9, if you are running the Policy Server UI using a Netscape 6.2.3 Web browser, there is an unreadable date in the Effective Starting Date or Expiration Date fields in the Time Dialog. This problem is caused by running the Policy Server UI using a Netscape 6.2.3 browser. To fix this problem, run the Policy Server UI with a Netscape 7.0 browser. To access this dialog box, select the Set button from the SiteMinder Policy dialog.

Netscape Browser Causes Missing Attributes in SiteMinder Response Dialog (44668, 44675)

On Red Hat Linux AS 3.0 and HP-UX 11i, if you are running the Policy Server User Interface using a Netscape 6 or 7 Web browser, attributes that you create do not appear in Attribute List on the SiteMinder Response Dialog. This problem is caused by running the Policy Server UI using a Netscape 6 or 7 browser. To fix this problem, run the Policy Server UI with a Microsoft Internet Explorer browser.

To access the SiteMinder Response Dialog, create a response under a domain.

Certificate Mappings Issue with certain Policy Stores (27027, 30824, 29487)

Certificate mappings do not work when the IssuerDN field is longer than 57 characters for policy stores installed on the following directories:

- Novell eDirectory
- Active Directory
- Critical Path

Handshake Errors with Shared Secret Rollover Enabled (27406)

In the Policy Server error log, you may see an occasional handshake error related to the shared secret, followed by a successful connection. This may occur if the shared secret rollover feature was enabled for the Web Agent communicating with the Policy Server. This behavior is expected as part of a normal shared secret rollover. You can ignore these errors.

Policy Servers Sharing Policy Store Not Updated Consistently (39844) (39837)

If you have a frequently updated policy store shared by multiple Policy Servers, not all of the Policy Servers are updated consistently. This is caused by ServerCommand getting deleted before the Policy Servers had a chance to update their cache.

To fix this problem, increase the following DWORD registry setting:

SiteMinder\CurrentVersion\ObjectStore
Key: ServerCommandTimeDelay

Change value to 10.

Internal Server Error When Using SecureID Forms Authentication Scheme (39664)

When using the SecureID forms authentication scheme, if users do not enter their passwords correctly during their initial login, they are not granted access to resources despite providing correct credentials in subsequent tries. The Policy Server presents users with an internal server error and these users must restart the Web browser to continue.

X.509 Client Certificate or Form Authentication Scheme Issue (39669)

The Policy Server's X.509 Client Certificate or Form authentication scheme is not working properly when using an alternate FCC location.

Certain User Name Characters Cause Authenticating or Authorizing Problems (39832)

When the Policy Server is using an LDAP user store, users with characters such as &, * , \, and \\ in their user names are not getting authenticated and authorized properly. For example, the Policy Server does not authenticate or authorize these sample users:

- use&r1
- use*r2
- use\r3
- use\\r4

RBAC: Policy Server and IdentityMinder Application Name Issue (39777)

When the Policy Server is configured to work with IdentityMinder 6.0, the name of the IdentityMinder application for the role/task assigned to the user are not appearing in the Policy Server response or in the Policy Server log files.

RBAC: Policy Server and IdentityMinder Environment Roles/Tasks Issue (39776)

When the Policy Server is configured to work with IdentityMinder 6.0, the roles and tasks associated with an authorized user's IdentityMinder environment do not appear in the Policy Server response sent out by the IdentityMinder application or in the Policy Server log files.

DEBUG Logging With SafeWord Authentication Causes Policy Server to Fail (42222, 43051)

On Solaris, when resources are protected by SafeWord authentication schemes, if you enable DEBUG or ALL logging in the SmSWEC.cfg SafeWord configuration file, the Policy Server fails. As a result, do not enable DEBUG or ALL logging for SafeWord authentication schemes. The SafeWord server is PremierAccess server, using protocol 200 or 201.

Active Directory Integration Enhancement For LDAP Namespace (43264, 42601)

This limitation is related to this new AD feature from 6.0 SP 2:

"Enhanced User Account Management and Password Services Integration with Active Directory (SM5504) (28460) (23347) (24047) (25816)"

When following the instructions in section "Enabling Active Directory Integration Enhancement", be aware that this feature is only supported for the LDAP and not the AD namespace.

Policy Server Does Not Support Roll Over of Radius Log (44398) (43729) (42348)

The Policy Server does not have the capability to roll over the radius log. Prior to the 6.0 release, you could roll over the radius log by running the smservauth -startlog command.

smnssetup Tool Deprecated (44964) (45908) (46489)

The smnssetup tool was removed from distribution in 6.0 SP 4. You should use the Policy Server Configuration Wizard (nete-ps-config) to configure:

- the OneView Monitor GUI
- the Policy Server User Interface
- the documentation virtual directory
- SNMP support
- Hardware Key Storage
- a policy store

The wizards gives you the option of using either a GUI or a console window. For more information, see the *Policy Server Installation Guide*.

Policy Server Fails to Initialize Java Virtual Machine on Red Hat AS 3.0 (44649) (44971)

On Red Hat Linux Enterprise AS 3.0 with Update 5, the Policy Server may fail to initialize the Java Virtual Machine when running on a multi-processor machine. As a result, the following SiteMinder functionality does not work:

- Java authentication schemes
- Java active rules, policies, and responses
- SAML federation

This problem is caused by an incompatibility between the Sun JDK on Linux and Red Hat's ExecShield, a kernel-based security feature. A work-around is to disable the ExecShield in the Linux SMP kernel only.

To decide if you want to disable the ExecShield, see Red Hat's "New Security Enhancements in Red Hat Enterprise Linux v.3, update 3" at http://www.redhat.com/f/pdf/rhel/WHP0006US_Execshield.pdf.

To disable ExecShield in the Linux SMP kernel only

1. In the /etc/grub.conf file, set the noexec=off kernel parameter in the SMP kernel only, as noted in the following example:

   title Red Hat Enterprise Linux AS (2.4.21-32.ELsmp)

   root (hd0,0)

   kernel /vmlinuz-2.4.21-32.ELsmp ro root=LABEL=/noexec=off

   initrd /initrd-2.4.21-32.ELsmp.img

2. Reboot the machine.

User Directory Limitations

The following user directory limitation exists:

ODBC User Store Failover

Given

A Policy Server is configured on Solaris to use two Oracle-based user stores: one is the primary user store and the other is the secondary user store.

Result

The time for the Policy Server to failover from the primary to the secondary, in the event of a network failure, may be as long as 8 minutes.

Solution

This time can be reduced by setting the TCP/IP setting, tcp_ip_abort_interval, to the desired time.

Perl Scripting Interface Limitations

The following Perl scripting interface limitations exist:

Perl use Statement for PolicyMgtAPI Must Come Before Use Statement for AgentAPI (24755)

On Solaris, a core dump results if you call use for AgentAPI before you call use for PolicyMgtAPI. If you are calling use for both modules, do so in the following order:

- use Netegrity::PolicyMgtAPI;
- use Netegrity::AgentAPI;

Methods that Return Arrays May Return undef in a One-Element Array (28499)

With methods that return an array, undef should be returned if an error occurs or there is nothing to return. However, these methods may incorrectly return a one-element array with the first element set to undef.

Perl Scripting Interface and Multi-valued Agent Configuration Parameters (37850)

The Perl Scripting Interface does not support setting multi-valued Agent configuration parameters.

Compatibility Limitations

The following compatibility limitation exists:

Oracle Parallel Server and Oracle Real Application Clusters Not Supported (27510)

The r6.0 SP5 Policy Server's Oracle wire protocol drivers do not support the Oracle Parallel Server or Oracle Real Application Clusters.

Japanese Policy Server Limitations

The following Japanese Policy Server limitation exists:

Agent Shared Secrets are Limited to 175 Characters (30967, 28882)

A Shared Secret for a SiteMinder Agent in a Japanese operating system environment may have no more than 175 characters.

Chapter 8: Known Issues

This section contains the following topics:

Web Services Variables Do Not Appear after Upgrade (46882)

Symptom:

After upgrading a policy store, I try to view Web Service Variables from the Policy Server User Interface. I receive a SiteMinder Administration error message and cannot view them.

Solution:

1. Create a new policy store instance.
2. Export your existing policy store.
3. Import the policy store into the new policy store instance.

   Note: More information on creating a new policy store instance exists in Create a New Policy Store in an LDAP Directory and Relational Databases as a Policy or Key Store in the *Policy Server Installation Guide*. More information on exporting your existing policy store into the new policy stores exists in Migrate an Existing Policy Store into an LDAP Directory and Migrate an Existing Policy Store into a Relational Database in the *Policy Server Installation Guide*.

Searching CertSerialNumbers in a Custom Certificate Mapping Fails (59352)

Symptom:

(LDAP) The default Policy Server behavior is to treat a CertSerialNumber as a broken string of numbers. This behavior causes a custom certificate mapping to fail if the user directory stores the CertSerialNumber as an unbroken string of numbers. The Policy Server fails to lookup the user because the default LDAP search contains spaces.

Solution:

Enable the NoSpacesinCertNumbers registry setting. Enabling the registry setting causes the Policy Server to treat certificate serial numbers as an unbroken string of numbers for all serial number comparisons.

Location:
HKEY_LOCAL_MACHINE/SOFTWARE/Netegrity/Siteminder/CurrentVersion/PolicyServer/NoSpacesInCertSerialNumbers

Values: 0 (disabled) 1 (enabled)

Default Value: 0

Upgrading a Solaris Policy Server (57935)

Symptom:

If your license file is older than January 2005, the Policy Server may experience problems reading the license file after an upgrade. You may receive a message stating that a valid end-user license cannot be found.

Solution:

Contact Technical Support, and request a new license file.

Linux Policy Server Does Not Delete Oracle Session Store Sessions (39143)

Symptom:

A Linux Policy Server may not immediately delete sessions from an Oracle session store when the idle timeout setting for the realm is reached.

Solution:

The Policy Server does begin to delete sessions shortly after the idle timeout setting is reached. For example, if the idle timeout setting is 30 minutes, the Policy Server may begin deleting sessions at 45 minutes.

Password Screen does not Prompt for Multiple SafeWord Authenticators (56766)

(**Solaris 9**) Users are unable to access protected resources when a SafeWord authentication scheme requires both fixed and token-based authenticators. The password screen only prompts users for one authenticator. Therefore, the user is unable to provide both types of credentials and cannot access the protected resource.

Users are Incorrectly Redirected after Receiving a New SecureID PIN (56738)

(**Windows 2003**) After users have received a new PIN, they are incorrectly redirected to a Diagnostic Information page that displays the following message: "Security Protection Fault: Unknown AuthReason." The latter occurs for both user and system-generated PINs.

Policy Server May Fail to Start due to a Dynamically Updated system_odbc.ini File (55265)

Symptom:

(HP-UX and Linux only) The Policy Server may fail to start because the system_odbc.ini file is dynamically updated.

Solution:

After the Policy Server installation, save the file as Read-Only.

Policy Server Installer Lists an Unsupported Operating System (55924)

The Policy Server installer lists Linux Advanced Server 2.1 as a supported operating system. Linux Advanced Server 2.1 is not supported.

Mixed Certificate-Based Authentication Schemes (27997)

The following authentication schemes are affected by the value of the Web Agent parameter for FCC Compatibility Mode (FCCCompatMode):

- Certificate or HTML Forms
- Certificate and HTML Forms

Note: Refer to the "Configure Web Agents" chapter of the *Web Agent Guide*. The section titled "Configure Credential Collectors in a Mixed Environment" discusses the impact of FccCompatMode and several other Web Agent parameters as they relate to the authentication schemes noted above.

Password Change Fails if UserDN Equal to or Greater than 1024 Characters (52424)

A password change fails and the user receives an error message prompting them to contact the Security Administrator or Help Desk if the combination of the new password; old password; and user identity, which is comprised of the userID, Client IP and time stamp is equal to or exceeds 1024 characters.

Policy Server Audit Logging Text File does not Audit Impersonator Events (52235)

You can audit impersonator events in either an Oracle or SQL server database by creating the SiteMinder schema for audit logs and using the database for audit logging. For more information on creating the audit log schema and configuring the Policy Server Management Console for audit logging using an Oracle or SQL server database, see the *Policy Server Installation Guide*.

Passwords for User Accounts Stored in Active Directory cannot be Locked (48125)

SiteMinder continues to let users change their passwords when the "User cannot change password" feature is enabled for the accounts.

Affiliate Domain Limitation When Upgrading 6.0 Policy Server on Japanese System (46338) (45693)

If you upgrade a 6.0 SP 1 or earlier Japanese Policy Server to r6.0 SP5, the contents of any previous affiliate domain are not displayed in Policy Server User Interface.

Configuring Registration Services for 6.0 SP1J (29659, 29660)

When configuring User Self Registration using the SiteMinder 6.0 SP1J you must set the HttpheaderEncodingSpec parameter in the agent configuration object to UTF-8,RFC-2047.

If you do not, several of the registration forms function incorrectly for Japanese characters. For example:

- The welcome JSP page (Welcome.jsp) shows bad characters for Japanese usernames and user directory names.
- The link for 'Modify self profile' is missing on the launch.jsp page.
- Users cannot modify their profiles after logging in to the Welcome.jsp.

Creating a SiteMinder Administrator in CriticalPath IDS 4.2.5 Fails (84995)

Symptom:

Sun Microsystems' Logical Domains (LDOMS) 1.1 returns a host ID value of 00000000 to SiteMinder. SiteMinder uses this value to create the IDs of policy server objects. When SiteMinder uses the value of 00000000 to create the object ID of the administrator, the resulting object ID is invalid, and the newly-created administrator fails to log in to the server.

Solution:

Contact Sun Microsystems for a patch that corrects the host ID value returned to SiteMinder.

STAR Issue: 17982871-1

Testing SunOne Directory Server Connections on Windows

Symptom:

You may experience problems testing a SunOne directory server connection from the Policy Server Management Console if:

- The machine that is hosting the Policy Server is also hosting the SunOne LDAP store.
- You are starting the Policy Server Management Console from a location other than *policy_server_home*\bin.

  policy server home

  Specifies the Policy Server installation path.

This problem occurs because multiple versions of the same LDAP SDK library, nsldap32v50.dll, exist on the machine:

- The Policy Server installer installs one version of the DLL to *policy_server_home*\bin. This version of the DLL does not cause problems when you attempt to test the connection.
- SunOne installs another version of the DLL to the system directory, for example C:\WinNT\system32. This version of the DLL may cause problems when you attempt to test the connection.

Note: This DLL conflict does not affect Policy Server processes or any of the SiteMinder command-line tools.

On Windows, when any process calls the operating system (OS) library loader, the loader looks to specific locations, in the following order, to load the DLL:

1. The directory from which the process was launched
2. The current directory
3. The system directory, for example C:\WinNT\system32
4. The Windows directory, for example C:\WinNT\system
5. The directories that are listed in the PATH environment variable

Therefore, if you start the Policy Server Management Console from a location other than *policy_server_home*\bin, the OS library loader loads the DLL from the system directory, for example C:\WinNT\system32, which may cause problems when you test the connection.

Solution:

Start the Policy Server Management Console from the *policy_server_home*\bin location.

Integrated Security Services and z/OS User Stores

(Valid for z/OS 1.7)

The Policy Server only supports SiteMinder password policies on ISS LDAP server user stores when "native authentication" is disabled.

The Policy Server supports integrated security services (ISS) LDAP server "native authentication" with z/OS. When "native authentication" is enabled on the ISS LDAP Server, users with native RACF profiles are supported and RACF password policies are enforced.

SiteMinder password policies should be disabled when running in ?native authentication? mode. Simultaneously applying LDAP password polices and SiteMinder password policies may result in unexpected behavior.

Policy Server Does Not Connect to LDAP Stores Using SSL with AKI (80655, 78751)

Platform: Solaris only

Symptom:

The Policy Server does not connect to LDAP stores that use SSL certificates with the AKI extension.

Solution:

To solve this problem, install the patch that corresponds to your version of Solaris:

- Solaris 8: 119209-12
- Solaris 9: 119211-12
- Solaris 10: 119213-12

For more information on how to install the patch corresponding to your version of Solaris, see the Troubleshooting chapter at the end of the *Policy Design Guide*.

STAR Issue: 17628120-1

ResponseTime Data Field Cannot Be Enabled

Symptom:

The ResponseTime data field cannot be enabled through the Policy Server Management Console.

Solution:

To output the ResponseTime to a trace log, edit the Web Agent Trace Configuration file, WebAgentTrace.conf, or other file specified in the Policy Server Configuration Object (ACO) and restart the Policy Server. For more information, see the *Web Agent Guide*.

STAR Issue: 18121336

Chapter 9: Defects Fixed in SiteMinder Releases

This section contains the following topics:

Defects Fixed for 6.0 SP5

Release 6.0 SP5 contains the following fixes:

Memory Leak in IIS NTLM Authentication Scheme Causes Failure (59283, 81045)

Symptom:

A small memory leak in the IIS NTLM authentication scheme can cause the Policy Server to fail.

Solution:

This is no longer an issue.

User Must Change Password When Password Policies Disabled (68697)

Symptom:

When the User must change password at next login checkbox is selected on the User Management dialog and the Password Policies Enabled for this Authentication Scheme checkbox is not selected on the Authentication Scheme Properties dialog, the user is redirected to the Password Change Request Page instead of authenticating.

Solution:

When the User must change password at next login checkbox is selected on the User Management dialog and the Password Policies Enabled for this Authentication Scheme checkbox is not selected on the Authentication Scheme Properties dialog, the user is no longer redirected to the Password Change Request page and can authenticate successfully.

STAR Issue: 16823492-1

Policy Server Continuously Flushes Policy Store and User Directory Caches (86158)

Symptom:

The Policy Server continuously flushes the policy store and user directory caches.

Solution:

This is no longer an issue.

STAR Issue: 18122810;01

AuthValidate Directory Mapping Fails with Single Policy Store (86696)

Symptom:

AuthValidate Directory Mapping fails when the authentication and validation user directories are associated with the same policy store.

Solution:

AuthValidate Directory Mapping is designed to work when the authentication and validation user directories are each associated with a different policy store. When the two user directories are associated with the same policy store, AuthValidate mapping fails.

STAR Issue: 18106843;01

Policy Evaluation Is Incorrect (85346, 87104)

Symptom:

Policy evaluation is incorrect.

Solution:

Flush the Policy Server cache using the new command line option –flushcache with the command smpolicysrv at runtime. This option causes the Policy Server to rebuild the cache with up-to-date data from the policy store.

STAR Issue: 18075700-01

Policy Server Management Console Profiler Output Is Excessive (80574, 88689)

Symptom:

When upgrading to SiteMinder 6.0 or greater from SiteMinder 5.5, customers find that the trace output, which is configured on the Policy Server Management Console Profiler tab, is excessive.

Solution:

To help you manage trace output, two new features have been added to the Policy Server Management Console. They have been added to the Components and Filters tabs, respectively, on the pane that opens when you click Configure Settings on the Profiler tab.

On the Components tab, you can now independently select and deselect the following two new subcomponents when the components Login_Logout/Authorization and isAuthorized are selected:

- Receive_Request
- Send_Response

On the Filters tab, you can now choose among four filters, two of them new. To the existing filters, equal and not equal, have been added the following new filters:

- contains
- does not contain

By deselecting the new subcomponents or using the new filters, you can reduce the trace output.

STAR Issue: 17523948-2

Multiple Policy Servers Share Policy Store

Symptom:

When multiple Policy Servers share one policy store or two replicated policy stores, they do not behave as expected.

Solution:

Add a DWORD registry key named FlushObjCache at the following location:

HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion
\ObjectStore

When this key value is set to one and the Flush All command is executed, both the primary and secondary Policy Server caches are flushed and rebuilt from the policy store. The primary cache is the object cache. For more information, see the Policy Server Management Guide.

STAR Issue: 16957333

Resource Leak in Idle Connections (75932)

Symptom:

Idle LDAP connections resulted in a resource leak.

Solution:

This is no longer an issue.

STAR Issue: 17188516

Resource Leak in TLI Buffering (82478)

Symptom:

A resource leak occasionally occurred in the TLI buffering.

Solution:

This is no longer an issue.

STAR Issue: 17908988

SNMPGETNEXT and Non-Existing Table Entries (85555)

Symptom:

Agents making an SNMPGETNEXT on a non-existing entry in a table were returning the first entry in the next column, not the first OID in the same column.

Solution:

This is no longer an issue.

STAR Issue: 17870806-1

Active Directory User Stores and Change Password State (82112)

(Valid for Active Directory over the AD namespace)

Symptom:

When a user was prompted to enter a new password before being authorized for a protected resource, submitting an incorrect old password with the new password resulted in:

- A successful password change
- Access to the protected resource

Solution:

This is no longer an issue.

STAR Issue: 17779807-01

Disabled Users can be Managed in the Policy Server User Interface (83289)

Symptom:

The Enable/Disable button, which is located on the User Management dialog and lets SiteMinder administrators modify the state of user accounts, remained active even though the user is disabled in the user store.

Solution:

This is no longer an issue.

STAR Issue: 17738132-01

Policy Server Management Console Changes cannot be Saved after Upgrade (86081)

(Valid for Policy Server upgrades from cr15 to cr27 on Solaris)

Symptom:

After upgrading the Policy Server, applying changes to the Settings tab resulted in an error message stating that the logging parameters were incorrect.

Solution:

This is no longer an issue.

STAR Issue: 18087243

ServerCommandTimeDelay Registry Key Results in Degraded Performance (86158)

Symptom:

Configuring the ServerCommandTimeDelay registry key to a value greater than one minute resulted in degraded performance due to the continuous flushing of the policy and user directory caches.

Solution:

This is no longer an issue.

STAR Issue: 18122810-01

Policy Server User Interface allows Realms with the Same Resources to be Created (82347)

Symptom:

The Policy Server User Interface did not prevent an administrator from creating a realm with the same resources (Agent and resource filter) as an existing realm. Rather, the realm was created and an error stating that the same resource filter was in used by another cached realm was output to the SiteMinder Policy Server log (smps.log)

Solution:

This is no longer an issue.

STAR Issue: 17889851;1

Policy Server Fails on Solaris (82710)

Symptom:

The Policy Server was failing on Solaris.

Solution:

This is no longer an issue.

STAR Issue: 17870535-01

Server Command Processed Repeatedly (83213)

Symptom:

After a trusted host was modified, the Policy Server was repeatedly processing the associated server command message.

Solution:

This is no longer an issue.

STAR Issue: 17893309

Policy Server Log does not Log Daylight Savings Time Offset (76949))

Symptom:

The timezone offset update was not properly displayed in the SiteMinder Policy Server log (smps.log)

Solution:

This is no longer an issue. A Daylight Savings flag has been added to the log. A value of one (1) specifies daylight savings. A value of zero (0) specifies standard time.

STAR issue: 15726130;02

XPSDDInstall Fails against an LDAP Policy Store (79551)

Symptom:

When a Policy Server and an LDAP policy store were both configured on Solaris 10 systems, using the XPSDDInstall utility to import the policy store data definitions resulted in a failure.

Solution:

This is no longer an issue.

STAR Issue: 17656481;01

Policy Server Fails due to Buffer Overrun (81230)

Solution:

Long user DNs resulted in exceptionally long audit messages after a failed authentication. The Policy Server failed due to these messages.

Symptom:

This is no longer an issue.

STAR Issue: 17800619-1

Disabled LDAP Users able to Change Account State

Symptom:

When disabled users attempted to login, they received a message stating that account could not be accessed and to contact the Security Administrator or Help Desk for assistance. This was expected behavior.

However, if the disabled users attempted to login using incorrect credentials, and exceeded maximum attempts allowed by the password policy, the disabled flag was set to locked.

Solution:

This is no longer an issue.

STAR Issue: 17738132-1

Policy Server Fails during New Pin Mode Request (82097)

Symptom:

Policy Servers may have crashed when an ACE authentication scheme was performing a new pin mode request.

Solution:

This is no longer an issue.

Policy Server Fails to Respond when Failing Over Idle Connections (82219)

Symptom:

The Policy Server was failing to respond when failing over idle connections.

Solution:

This is no longer an issue.

STAR Issues: 17708176;1,17809840,17855066-1.17809840-1

ACE Authentication Results in Policy Server Failure on Linux (76937)

Symptom:

Linux Policy Servers were unexpectedly failing when the ACE Authentication scheme was being used.

Solution:

This is no longer an issue.

STAR Issue: 17344233;01

Users not Forced to Change Password after Failed Attempt (79852)

Symptom:

When users were prompted to change their password at login, Active Directory would reject the change request if the password failed to meet the complexity requirements. This was expected behavior.

However, upon next login, users were not prompted to change their password and were authenticated using the old password.

Solution:

This is no longer an issue.

STAR Issue: 17651196-1

Access Log Concatenates Log Entries (80474)

Symptom:

Log entries in the SiteMinder access log (smaccess.log) with more than 1024 were concatenated with the next line.

Solution:

This is no longer an issue.

STAR Issue: 17602184

SM_USERGROUPS Well-Known Attribute Returns No Groups (77151)

Symptom:

A response returning the SM_USERGROUPS well-known attribute incorrectly returned no groups.

Solution:

This is no longer an issue.

STAR Issues: 17515653-1 and 16652769-1

Authentication Process Stops When a Disabled User is Found (77175)

Symptom:

A user could be found in more than one user directory or database associated with a policy domain. This user has the same password in each store, but is only disabled in one of the stores. During authentication, if the Policy Server found the disabled account first, the authentication process stopped. The Policy Server did not process the authentication request against the subsequent user stores.

Solution:

This is no longer an issue.

STAR Issue: 17405689;01

Session Key Rollover Results in Shared Secret Rollover (78685)

Symptom:

Rolling the session ticket key also caused the Policy Server to roll the trusted host shared secret.

Solution:

This is no longer an issue.

STAR Issue: 17642192;01

Unauthenticated Users and Active Expression Evaluation (79489)

Symptom:

The Policy Server was failing when an active expression returned a user context value for a user that did not provide valid credentials.

Solution:

This is no longer an issue.

STAR Issue: 17687684-01

Upgrades do not Preserve OneView Monitor Settings (70456)

Symptom:

The SiteMinder OneView Monitor configuration settings are not preserved when the Policy Server is upgraded.

Solution:

This is no longer an issue.

STAR Issue: 17074840;01

Policy Server Fails on Large Multiple CPU Platforms (73718)

Symptom:

Policy Servers were unexpectedly failing on large, multiple CPU hardware platforms.

Solution:

This is no longer an issue.

STAR Issue: 17237873-01

Policy Server Fails on Shutdown (77780)

Symptom:

Policy Servers were unexpectedly failing during shutdown if text-based audit logging was enabled.

Solution:

This is no longer an issue.

Policy Server Responds with Policy Not Applicable Error (72434)

Symptom:

In some cases, the Policy Server would return an error message stating that a valid policy was not applicable.

Solution:

This is no longer an issue.

STAR Issue: 17166455-1

Error Message Causes the Policy Server to Hang (73454)

Symptom:

An error message stating that a loadlibrary error occurred caused Policy Servers to hang.

Solution:

This is no longer an issue.

STAR Issue: 17097843;01

CA SSO Integration Rejects Cookies (74765)

Symptom:

The CA SSO authentication scheme was rejecting cookies if they did not match the case of the SiteMinder cookies. As a result, the Policy Server was prompting users for credentials, even though they had successfully logged into SSO.

Solution:

This is no longer an issue.

STAR Issue: 17367123-2

Policy Server Process Creates File with Incorrect Permissions (76159)

Symptom:

The Policy Server process, smpolicysrv, was creating the smpublish.xml file with incorrect permissions.

Solution:

This is no longer an issue.

STAR Issue: 17505881-1

Policy Server OCSP Responder Certification Validation (76212)

Symptom:

The Policy Server OCSP responder certification validation was not checking that the cacertificate attribute contained the DER binary certificate data from the correct certificate authority.

Solution:

This is no longer an issue.

STAR Issue: 17461668;01

Client Certificates with OIDs are not Parsed Properly (76629)

Symptom:

x.509 Client Certificates with OIDs in the SubjectDN were not being parsed properly.

Solution:

This is no longer an issue.

STAR Issue: 17515216;01 and 17490798;01

Policy Server not Closing User Directory Connections (65757,71075)

Symptom:

In certain cases, Policy Servers installed to Solaris or Red Hat Linux systems were not properly closing user directory connections marked CLOSE_WAIT.

Solution:

This is no longer an issue.

STAR Issue: 15922351-1

ACE Authentication Results in Policy Server Failure (73519)

Symptom:

If the Policy Server was installed on Linux, using the ACE authentication scheme caused the Policy Server to fail.

Solution:

This is no longer an issue.

STAR Issue: 17344233;01

Authentication Process Stops When a Disabled User is Found (73873)

Symptom:

A user could be found in more than one Active Directory user store over the AD namespace. This user is only disabled in one of the stores. During authentication, if the Policy Server found the disabled account first, the authentication process stopped. The Policy Server did not process the authentication request against the subsequent user stores.

Solution:

This is no longer an issue.

STAR Issue: 1740589;01

Authentication Validation Mapping and Mixed User Stores (70551,74371)

Symptom:

In certain cases where authentication validation directory mapping was configured using mixed user stores, users were not being mapped properly. As a result, authentication failed, and users were re-prompted for credentials when requesting resources across multiple Policy Servers.

Solution:

This is no longer an issue.

STAR Issue: 17397458;01, 17055724;1 and 17083786;1

Agent Type Changes do not take affect in the Consumer Site (71600)

Symptom:

In environments where master-consumer policy store replication was configured, changes made to an existing agent type did not appear in the Policy Server User Interface at the consumer site.

Solution:

This is no longer an issue.

Active Directory Password Changes Expire (72197)

Symptom:

After upgrading Policy Servers, users could change their password using Active Directory password services, but the changed password failed.

Solution:

This is no longer an issue.

STAR Issue: 17280254;1

Policy Server Fails when Authentication Scheme Changes (70874)

Symptom:

Changing the authentication scheme type in an existing realm from Basic over SSL to HTML Forms resulted in Policy Server failure if the Policy Server was not restarted.

Solution:

This is no longer an issue.

STAR Issue: 17175375;01

Policy Server Incorrectly Reports Mixed Mode Status (70890)

Symptom:

In certain cases, rather than reporting that initialization had failed when the policy store was not available, Policy Servers reported that they had started in mixed mode.

Solution:

This is no longer an issue.

STAR Issue: 17064524

LDAPS User Store Failure Results in Policy Server Failure (70912)

Symptom:

Policy Servers failed to respond if one or more LDAPS user store instances became unresponsive.

Solution:

This is no longer an issue.

STAR Issue: 16707446-1

Alternative Directory Path Causes Smexec to Fail (68852,70956)

Symptom:

Specifying a directory path other than root caused the smexec service to fail.

Solution:

This is no longer an issue.

Onyx Issue: 12625

Users Incorrectly Authorized with Mixed User Store Directory Mapping (71230)

Symptom:

In certain cases, the Policy Server was authorizing users which were included in the LDAP authentication directory, but not part of the ODBC authorization directory.

Solution:

This is no longer an issue.

STAR Issue: 17154679;01

Recalculating Response Attributes Fails with Multiple User Attributes (71427)

Symptom:

The attribute caching feature that periodically recalculates response attributes was not working when multiple user attributes were being fetched using the WebAgent-HTTP-Header-Variable.

Solution:

This is no longer an issue.

STAR Issue: 17229882;01

Policy Server uses Incorrect LDAP Connection for Searches (71624)

Symptom:

In certain cases, Policy Servers were using the incorrect LDAP connection to perform user store searches.

Solution:

This is no longer an issue.

STAR Issue: 17197996-1

Library Configuration on HPUX may Lead to Policy Server Failure (68907)

(Valid for HPUX Policy Servers)

Symptom:

During multi-threaded operations, a certain library configuration was resulting in HPUX Policy Server.

Solution:

This is no longer an issue.

Onyx Issue: 12168

Password Policies Custom Dictionaries not Loading (69746)

Symptom:

If the file descriptor returned by the Solaris was greater than 255, custom password dictionaries were not loaded.

Solution:

This is no longer an issue.

STAR Issue: 17061719-1

SecureID with HTML Forms Redirects Users to Wrong Page (69825)

Symptom:

If the SiteMinder password services file (smpwservices.fcc) was being used with the SecureID with HTML Forms authentication scheme, users were being prompted to re-enter credentials, rather than being redirected to the Next Token page.

Solution:

This is no longer an issue.

STAR Issue: 17117269-1 and 17114758-1

Basic Over SSL Authentication Accepts Blank Password (70740)

Symptom:

The Basic Over SSL authentication scheme granted access to protected resources when users provided a valid user name, but did not provide a password.

Solution:

This is no longer an issue.

STAR Issue: 17182087;01

Enhanced LDAP Referrals do not Work a in Multi-Master LDAP Environment (68780)

Symptom:

Enhanced LDAP referrals were not working in a consumer/Master LDAP environment. After the directory server's idle timeout setting expired, the Policy Server failed to modify the user attribute over the SSL connection. Rather, the transmission appeared in clear text.

Solution:

This is no longer an issue.

Wild Cards Cause Validate DN Operation to Fail (69008)

Symptom:

User attributes containing a parenthesis and a wild card character, for example (samaccountname=*) caused the Validate DN operation to fail.

Solution:

This is no longer an issue.

STAR Issue: 16398063;01

Policy Store Object Cache Returns Duplicate Entries (66270)

Symptom:

The Policy Store object cache was returning duplicate entries when under heavy load.

Solution:

This is no longer an issue.

Onyx Issue: 11619

SiteMinder Wire Protocol Help Files not Found (66280)

Solution:

The SiteMinder Wire Protocol help files were not shipped with the Policy Server.

Symptom:

This is no longer an issue.

Onyx Issue: 12387

Policy Store Object Cache Returns Corrupted Entries (66341)

Symptom:

The policy store object caches was returning corrupted entries under heavy load.

Solution:

This is no longer an issue.

Onyx Issue: 11974

Adding/Removing Password Policy Expressions Results in an Error (66609)

Symptom:

Modifying a policy password by removing and adding regular expressions resulted in an error message in the SiteMinder policy server log (smps.log). The error message stated that the modified password policy object failed to save.

Solution:

This is no longer an issue.

Incorrect CRL Message in the SiteMinder Policy Server Log (66792)

Symptom:

The SiteMinder Policy Server log (smps.log) stated the that CRL was being retrieved from the Directory, even though the CRL was found in the cache.

Solution:

This is no longer an issue.

Onyx Issue: 12340

Basic Over SSL Authentication Accepts Certificates (67500)

Symptom:

If they presented a valid certificate, but no credentials, users were denied access to resources protected by the X.509 Client Certificate and Basic authentication scheme. This is expected behavior.

However, within the same browser session, the same users were granted access to resources protected by the Basic Over SSL authentication scheme without providing credentials. Rather, the Basic Over SSL authentication scheme accepted the certificate presented earlier in the session and authenticated the user.

Note: This issue only occurred with Mozilla™ Firefox™.

Solution:

This is no longer an issue.

STAR Issue: 16943710;01

Evaluating Identity Manager Roles Causes Memory Leaks (66776)

Symptom:

Memory leaks occurred when evaluating Identity Manager (IM) roles if the following IM generated responses were used:

- SM_USER_APPLICATION_ROLES
- SM_USER_APPLICATION_TASKS

Solution:

This is no longer an issue.

Onyx Issue: 11952

Documentation Link in the Policy Server User Interface does not Work (66185)

(Valid for Solaris)

Symptom:

If the SiteMinder documentation was installed prior to the Policy Server, the Online Documentation link in the Policy Server User Interface did not open the documentation.

Solution:

This is no longer an issue.

Onyx Issue: 12258

Password Change Requests Apply to All Authentication Schemes (66216)

Symptom:

When user accounts were set to "change password at next login", users were being prompted to change their passwords, even if the authentication scheme did not require a password.

Solution:

This is no longer an issue.

To revert to the previous behavior of processing password change requests, regardless of the authentication scheme type, enable the AlwaysProcessNonRelevantAuthRequest registry key.

To enable the key

1. Run regedit
2. Navigate to \\HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\PolicyServer
3. Create the AlwaysProcessNonRelevantAuthRequest key with the following settings:

   Type: DWORD

   Value: 1 or 0

   1

   Enables the key. When a user account is set to "change password at next login", the user will be prompted to change the password, regardless of the authentication scheme type.

0

Disables the key. When a user account is set to "change password at next login", the user will only be prompted to change the password if the authentication scheme uses passwords.

Note: A value other than 1 or 0 disables the key.

Onyx Issue: 263569

SiteMinder Object Import Utility Causes Fault on Policy Server (66477)

Symptom:

In certain cases, the SiteMinder object import utility (smobjimport) was causing a segmentation fault on the Policy Server when importing a policy store objects.

Solution:

This is no longer an issue.

Onyx Issue: 12418

Incorrect Password Accepted for Password Change Request (65110,66730)

Symptom:

When Active Directory user accounts were set to the "change password at next login" state, incorrect passwords were accepted during authentication and the users were redirected to change their password. The same incorrect password could be used for the password change request. As a result, the password was changed and access to the protected resources was granted.

Solution:

This is no longer an issue.

Onyx Issue: 12141

Policy Server Reports "Policy Is Not Applicable" Error (72434, 80261)

Symptom:

The Policy Server intermittently reports a "policy is not applicable" error, when in fact, the policy does apply.

Solution:

The Policy Server now reports a message that describes the actual error. For example, if the Policy Server cannot contact an authorization directory, it reports the following message: Authorization directory could not be contacted.

STAR Issue:17166455-1

Admin UI Login Error Causes Policy Server to Hang (73454, 80263)

Symptom:

The Admin UI Login error "xerces-c_1_5_1.dll was not found. Re-installing the application may fix this Symptom:." causes the Policy Server to hang.

Solution:

This error is no longer displayed, and the Policy Server no longer hangs.

STAR Issue: 17097843;01

Policy Server Crashes on Startup (73718, 80153)

Symptom:

Policy Server crashes on startup.

Solution:

This behavior was seen on multiple large hardware platforms and is no longer an issue.

STAR Issue: 17237873-01

Error Causes SSO Failure (74765, 80265)

Symptom:

Error "cookie name does not match" causes SSO to fail.

Solution:

This error occurred when the user's DN and the cookie DN matched, but their cases did not match. To fix this issue, both DNs are converted to lowercase and then compared.

STAR Issue: 17367123-2

Certificate-Only Authentication Schemes Fail with Custom Certificate Mapping (75552, 80266)

Symptom:

When you create a custom certificate mapping for an LDAP user directory, the resulting search query string includes the LDAP User DN Lookup Start and End strings in addition to the Mapping Expression that you specify on the Create Certificate Mapping pane. The resulting query is invalid and the search fails.

Solution:

You can exclude the DN Lookup Start and End strings from the search query string by setting the

\Netegrity\SiteMinder\CurrentVersion\PolicyServer\EnableCustomExprOnly

registry key as follows:

- value = 1

  Excludes the DN Lookup Start and End strings from the search query string.

- value /= 1 (default)

  Includes the DN Lookup Start and End strings in the search query string.

STAR Issue: 17360040-01

Policy Server Does Not Check OCSP Responder Certificate Validation (76212, 80203)

Symptom:

The Policy Server does not check the OCSP responder certificate validation to verify that the DER-encoded binary certificate is issued by the Certificate Authority (CA) specified in the user directory.

Solution:

This is no longer an issue.

STAR Issue: 17461668;01

Encoded OID Value Causes Certificate Authentication to Fail (76629, 80264)

Symptom:

When the Policy Server extracts an X.509 Client Certificate Subject DN's OID value for certificate authentication, the OID value is in an encoded form instead of in the form of a string as expected. This causes authentication to fail.

Solution:

This problem is no longer an issue.

STAR Issues: 17515216;01+17490798;01

Windows Authentication Scheme Does Not Support Relative Target (76980, 81280)

Symptom:

When creating a Windows authentication scheme, you cannot specify a relative path name for the Target or resource that the authentication scheme protects.

Solution:

When creating a Windows authentication scheme, you can now select the Use Relative Target checkbox to specify a relative path name for the Target or resource that the authentication scheme protects. When this checkbox is selected, the Server Name field is dimmed.

STAR Issue: 16829145-01

Response Does Not Return User Groups (77151, 80571)

Symptom:

When invoked, the response does not return the user groups to which the user belongs.

Solution:

This problem is no longer an issue.

STAR Issues: 17515653-1;+16652769-1

Policy Server Stops When User Disabled in First Directory (77175, 80272)

Symptom:

Use Case: One user exists in two user directories and has the same password in both directories. In the first of the two directories, the user is disabled. The two user directories are bound to an authentication policy.

Expected Behavior: Even though the user is disabled in the first user directory, the Policy Server can authenticate the user against the second user directory.

Problem Behavior: When the user tries to authenticate, the Policy Server returns a "user disabled" error and stops processing.

Solution:

This is no longer an issue.

STAR Issue: 17405689;01

Policy Server Fails During Shutdown (77780, 80154)

Symptom:

The Policy Server fails when accessing the audit log file during shutdown.

Solution:

This is no longer an issue.

Shared Secret Rolls Over with Session Key (78685, 80156)

Symptom:

When the session key rolls over, the shared secret rolls over also.

Solution:

This is no longer an issue.

STAR Issue: 17642192;01

Policy Server Hangs When Stopped and Audit Logging Enabled (78833, 80155)

Symptom:

The Policy Server hangs when stopped and audit logging is enabled for all policy store objects.

Solution:

This problem is no longer an issue.

Policy Server Fails When Authentication Attempted with Invalid ID (79489, 80269)

Symptom:

Policy Server fails when authentication is attempted with an invalid user ID.

Solution:

This is no longer an issue.

STAR Issue: 17687684-01

Password Change Flag Reset When Password Change Fails with AD (79852, 81042)

Symptom:

The password change flag is reset when the password change fails with Active Directory (AD), allowing the user to authenticate with the old password when a new password is required.

Solution:

This problem is no longer an issue.

STAR Issue: 17651196-1

Policy Server Logs Not Rolled Over (80385, 82497)

Symptom:

Policy Server logs are not rolled over when the rollover interval is time-based.

Solution:

This problem is no longer an issue.

STAR Issue: 17730333-1

User Disabled in Authorization Directory Is Authorized (80437, 82501)

Symptom:

When directory mapping is configured, a user who is disabled in the authorization directory is authorized.

Solution:

This problem is no longer an issue.

Log Entries Longer than 1024 Characters Are Concatenated (80474, 82503)

Symptom:

Log entries longer than 1024 characters are concatenated with the next line in the log file.

Symptom:

The buffer size has been increased to hold 4096 characters, and this problem is no longer an issue.

STAR Issue: 17602184

Disabled User Exceeds Maximum Login Times and Is Enabled (81291, 82101)

Symptom:

A disabled user who tries and fails to log in more than the maximum number of times permitted by the password policy and then waits for the time interval required by the password policy is enabled.

Solution:

This problem is no longer an issue.

STAR Issue: 17738132-1

Policy Server Fails When Authorization Directory Stopped (81791, 82508)

Symptom:

The Policy Server fails and restarts or stops when the user tries to access a protected resource in the following case: Directory mapping is being configured, and the authorization directory is stopped.

Solution:

This problem is no longer an issue.

Policy Server Trace Log Does Not Roll Over at Expected Times (81978, 82573)

Symptom:

When the Policy Server trace log rollover time is set to 00:00, the log does not roll over at the expected times.

Solution:

This problem is no longer an issue.

The Policy Server Sends Null Value Active Responses to Custom Agents (67558, 70010)

The Policy Server no longer sends null value active responses to custom agents. You can override this default behavior by modifying the DWORD registry key named Enable Null Value Response at the following location:

HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion

\PolicyServer

For more information, see the Responses and Response Groups chapter in the *Policy Design Guide*.

Policy Server Does Not Start after Installation (57877)

A Policy Server installed with an LDAP policy store may not have started after installation. This occurred because the Policy Server installer did not configure the policy store and the key store settings to use the same directory type.

This is no longer an issue.

Users Stored in Active Directory are not Authenticated over SSL (53615)

Users in an Active Directory namespace were not authenticated over SSL when the accounts were to force a password change on the next logon and the SaslBindEnabled registry key was enabled. This is no longer an issue.

CoreStreet OCSP Responder may cause Status Code 33 on Validation (54846)

This is no longer an issue.

Administratively Reset Accounts are Disabled on User Log in (55502)

SiteMinder accounts, which had exceeded the specified inactivity period but had yet to be disabled, were being administratively reset in Identity Manager. When a user attempted to log in, the SiteMinder password policy disabled the account due to inactivity, even though an administrator had enabled the account and reset the password. This is no longer an issue.

Activity by Administrator Report Incorrectly Lists Deleted Administrator Accounts (55601, 55257)

Administrator accounts that had been deleted prior to a password services request were incorrectly appearing in the Activity by Administrator report. The deleted accounts were listed as submitting the password services request, instead of the account that actually made the request. This is no longer an issue.

Authentication Schemes Clear Redirect URLs when Returning Failure (55773)

This is no longer an issue.

New Multi-Value Parameters are not Saved (55784)

Adding a new multi-value parameter to an agent configuration object did not work correctly. New multi-value parameters failed to save and did not appear in the parameters list. Multi-value parameters had to be saved as a single-value parameter prior to being saved as a multi-value parameter. This is no longer an issue.

Policy Server Installer Removes the Windows Services Configuration when Upgrading from Identity Manager 8.1 (55785)

This is no longer an issue.

Unprotected Realm is Incorrectly Protected (55890)

When an unprotected realm contained a disabled rule that was referenced by two or more policies, the resource in the unprotected realm was incorrectly considered protected. This is no longer an issue.

Pure Java AgentAPI.isProtected Sets Realmdef Members to Null for Unprotected Resources (55246)

This is no longer an issue.

Pure Java AgentAPI.login does not accept Null or Blank ClientIP (55247)

When the AgentAPI.login function was called with a null or blank IP, the function raised an exception. This is no longer an issue.

Policy Server Installation May Fail with Kernel Versions Lower than 2.4.21-27.EL (54534)

The Policy Server installation may have failed for Linux users using the JRockit JVM and Linux kernel versions lower than 2.4.21-27.EL. This problem was resolved in the RHEL3 U4 kernel in kernel version 2.4.21-27.EL.

System Generated PIN's are not displayed when SecureID Authentication is used (54105)

System generated PIN'S were not being displayed properly to the end user when SecureID authentication was used with Policy Server on Solaris. If system generated PINs were being used as part of SecurId authorization, the PIN was properly generated and set as the user's new PIN. However, the user received a 500 error instead of a screen showing the new PIN. The PIN value had to be read from the Policy Server log.This is no longer an issue.

Policy Server on Solaris has been modified so that authorization through SecureID will not fail if a system generated pin is requested.

User Authentication Fails using authenticateUser() Function (52937)

When using authenticateUser() from Java Policy Management API to authenticate users, the status was improperly returned and the user was not authenticated. This is no longer an issue.

Identity Minder Fails to Retrieve User with DN (53908)

This is no longer an issue. Policy Server has been modified to add support for the "DIRECTORY_SERVER_STICKINESS" property in Identity Minder. This option ensures that the same directory is used for validation on create object actions from within the Identity Minder interface, allowing the action to succeed without having to wait for the object to propagate to other LDAP servers.

Importing a Policy Store Fails on Solaris (54708)

When using a policy store exported from a 5.5 Policy Server with Policy Server Option Pack installed on Solaris to import to 6.0 Policy Server, the import was terminated abnormally. This is no longer an issue. The 5x policy store with option pack can now be successfully imported in to a new 6x policy store with option pack, without generating any segmentation fault error and core dumps on Solaris computers.

Improper Return of Policy Server Connection Status (54815)

When connection to Policy Server was not successful the API method Connect() returned a blank status. This is no longer an issue. The agent API method Connect() will return the correct status (SM_AGENTAPI_FAILURE) when connection to policy server is not successful.

Cannot Read License File After an Upgrade to PS6SP4CR06 on Solaris (54833)

IVNS.LIC cannot be read because it was installed as ivns.lic using a file name in lower case after an upgrade to PS6SP4CR06 on Solaris. This is no longer an issue. The user should rename ivns.lic to IVNS.LIC on Solaris to prevent problems with the DataDirect ODBC drivers.

Null Pointer Exception not Handled Properly for Java Policy Management API Functions (54842)

This is no longer an issue. Null pointer exceptions are properly handled for TrustedHost objects in SiteMinder SDK.

Upgrading From 6.0 SP4 CR2 to 6.0 SP4 CR6 Deletes the Admin Directory (54906)

Upgrading the Policy Server from 6.0 SP4 CR2 to 6.0 SP4 CR6 on Windows 2000 with the IIS Web Server running resulted in the admin directory being deleted. This is no longer an issue. The admin directory is not deleted when IIS Web Server is running.

Note: IIS Web Server should be stopped before the upgrade.

Radius Authentication Fails for More Than 1024 Radius Connections (54933)

This is no longer an issue. The radius authentication was upgraded to properly handle more than 1024 connections.

Incorrect Certificate Validation Error Message Referring Vtk_ValidateAddCertNew (55379)

This is no longer an issue. The incorrect certificate validation error message referring Vtk_ValidateAddCertNew has been changed to refer the proper method Vtk_ValidateAddCertRaw.

Console Policy Server Installer does not Mask Passwords (51919)

The 6.0 Policy Server console installer now masks passwords. Password-masking is available when the installer requests the following:

- The Policy Store encryption key. The installer prompts the user to enter and confirm the encryption key. The installer checks for the minimum (6) and maximum (25) character length.
- The Admin information for the policy store
- The Super User account information for the policy store
- The root password to configure SNMP
- PKCS information for hardware key storage
- The different user account failure information for the policy store

LDAP does not Connect Over SSL When the LDAP Host Name Resolves to more than 50 IP Addresses (53657)

This is no longer an issue, and LDAP uses the first IP address in the resolution list.

User is not Authenticated When the LDAP User DN Lookup End field Contains Double Byte Characters (54362)

User was not authenticated if the LDAP User DN Lookup End field contained Japanese double byte characters, unless the Japanese double byte characters were followed by an extra double byte space character. This is no longer an issue. The extra double byte space character is not required.

Authorization Scheme Messages are Lost When Multiple User Directories are Configured in the Same Domain (54385)

This is no longer an issue. User, error, and redirect messages are properly returned from authentication attempts in a domain for which multiple user directories are configured.

Domain Scope User is Unable to Call Function GetRealm( ) in the Perl SDK (54465)

This is no longer an issue. The Domain Scope user is able to call function GetRealm( ) in the Perl SDK. This behavior is in sync with that of the SiteMinder Administrator user interface.

Temporary Passwords do not Adhere to Password Policy Restrictions (54519)

When the Forgotten Password feature was used, the Policy Server created random temporary passwords that did not adhere to the password policy restrictions. This is no longer an issue, and temporary passwords now adhere to the password restrictions specified by the password policy. Supported restrictions include:

- minimum length
- maximum length
- minimum upper case characters
- minimum lower case characters
- minimum digits

In the event that password policies are not applied to the user directory, the temporary password is:

- six to twelve characters long
- of capitals letters, lower case letters, and digits

Agent Keys are not Correctly Generating in Systems Using Dynamic Key Rollover (54669)

This is no longer an issue. Improved detection and logging of bad keys prevents the agent or users of the agent API routines createSSOToken ( ) and decodeSSOToken ( ) from using the bad keys.

Before Installing SiteMinder Policy Server on HP 11i, Verify the Existence of Patch PHCO_29029 (54845).

A verification check was added for PHCO_29029 patch before Policy Server installation on HP 11i. You no longer have to check for this patch.

Directory Mapping and Certificate Mapping Dialogs Limited by MaxObject Registry Key (47146)

The Directory Mapping and Certificate Mapping dialogs would only display the number of objects specified by the HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\ObjectStore\MaxObjects registry key. This occurred even if the actual number of objects exceeded the registry key value. For example, if 75 user directories existed and MaxObjects was set to 50, only the first 50 user directories were available from Directory Mapping dialog. This is no longer an issue. Previous and Next buttons let you view the remaining objects.

Resetting Stats Information Requires Restarting the Policy Server (47332)

This is no longer required. The -resetstats switch lets you reset counter information without restarting the Policy Server. The switch is provided with smpolicysrv and works as follows:

```
$ smpolicysrv -resetstats
```

This switch lets you reset the following counters:

- Max Threads is reset to the Current Threads value.
- Max Depth of the message queue is reset to the Current Depth of the message queue.
- Max Connections is reset to Current Connections.
- Msgs, Waits, Misses, and Exceeded limit are reset to zero.

The -stats Output only Shows the MaxDepth in the Policy Server Stats Output (47485)

The -stats switch for the smpolicysrv now logs the Current Depth of the message queue in the smps.log file.

Product, Platform, and Version Information are not Populated (53190)

Product, Platform, and Version Information are not Populated on a OneView Monitor that runs on RedHat AS 3.0 Linux. This is no longer an issue.

Signature Verification of AuthnRequest on Solaris IDP and SLO Transactions Fail (53693)

Signature verification of AuthnRequest and Single Logout processing failed because of certificates with large serial numbers. This is no longer an issue, as restrictions on serial number length have been removed.

CaCertificate Search Scope May Cause Timeouts (53933)

The LDAP CaCertificate had a search scope of 2, which increased the chance of timeouts while authenticating users in certain LDAP configurations. This is no longer an issue. The LDAP CaCertificate searches with a search scope of 0, which reduces the chance of timeout while authenticating users.

ODBC-driver Message Appears Unnecessarily (53941)

The Policy Server installer displayed a warning message to update the ODBC drivers when the updated drivers were present. This is no longer an issue. The message only appears if the required drivers need to be installed.

List of Clusters Changes Order Each Time Changes are Saved (54021)

This problem was specific to using Novell eDirectory Server as a policy store. The list of clusters that appears on the Host Configuration Object Properties tab randomly changed order each time OK or Apply was clicked. This is no longer an issue.

DMS API SmDmsUser.changePassword() Method Results in Multiple TransactEMS Requests During a Password Change (54045)

This is a no longer an issue. Retry logic has been added to the TLI layer to handle interruptions from the BEA JRockit JVM.

Lower case 'l' is Appended to the Port Number in the smps.log (54196)

A lower case "l" was appended to the port number in the snmps.log when the user directory connection was lost. This is no longer an issue.

Global Responses are not Sent to an Added Agent (54102)

When an agent was added to an agent group, global responses were not sent until the Policy Server was restarted. This is no longer an issue because the Global Realm is invalidated when the agent group is modified, which ensures that a Global Response is sent to a recently added agent without having to restart the Policy Server.

Commas (",") in the SubjectDN Attribute Value Causes Authentication Schemes to Fail (54245)

CertAndForm and CertAndBasic authentication schemes were not able to support certificates in which the SubjectDN attribute values contained a "," (comma). This is no longer an issue.

Policy Server Crashes When a Valid User Name and Blank Password are Submitted (54262)

This problem is specific to Solaris. The Policy Server crashed when a valid user name and a blank password were submitted to an Oracle user directory with the OOTB function in the Authenticate User query. This is no longer an issue.

Policy Server does not Start after Upgrading to 6.0 SP4 (53697)

This is no longer an issue.

SiteMinder Policy Server Hangs and must be Rebooted to Regain Stability (53815)

This is no longer an issue. The Policy server does not hang when a custom authentication scheme is created with smauthntlm library to allow the clients authentication request to be processed by the server being accessed.

Password History Updates When a CustomAuth Scheme Authenticates Based on an Attribute Other than the Password (52323)

This is no longer an issue. A password is added to the Password History if the custom authentication scheme authenticates using the default password and in scenarios where the function UserContext->fAuthticate( ) is called. When any other function, such as UserContext->GetProp, is used for authentication, the password is not added to the Password History.

Password Change Fails When UserDN is Greater than 256 Characters (52424)

This is no longer an issue. The buffer length used for creating Password Message has been increased and will allow DNs longer than 256 characters.

Note: The combination of new password, old password, and user identity consisting of userID, Client IP, and timestamp must always be less than 1024 characters.

Account Lockout Rule Ignored if User is Enabled through DMS (53699)

This is no longer an issue. Policy Server was modified. Reactivating a user through the DMS system will not result in deactivation of password policies.

SecurId Authentication Scheme not Working (53985)

A previous change had introduced support for non-browser clients, but part of the fix was appending ";ACS=x" to the URL, which was to be removed later. This was not done for the SecureID template. This is no longer an issue. The ACS=x parameter is removed from the URL before returning it to the web agent.

Apache Web Server Crashes When Accessed by Multiple Agents (54064)

This is valid for RedHat Linux 3.0. This is no longer an issue.

SiteMinder appears to be Experiencing Memory Leaks (52673)

This is no longer an issue. The way entries are allocated and freed in the Authorization cache is improved. This improvement prevents the Authorization cache from appearing to grow unbound in certain load scenarios. The Authorization cache should grow no larger than twice the value the registry specifies.

Users are Authenticated with Valid and Invalid Passwords after Upgrading (52796)

Users were authenticated with valid or invalid passwords after upgrading to 6.0.4.2 if the SiteMinder environment was using the OOTB sample stored procedure and a DB2 database. This is no longer an issue. New Datadirect 5.1 patched drivers are provided, which prevent users from being authenticated with invalid passwords.

Password Change Failure Shows the New Password in Clear Text in the Policy Server logs (53213)

This is no longer an issue.

AgentTLI crashes in memcpy() Called from: intCSmSerializable::Serialize(const long,const void*) (53299)

This is no longer an issue.

Saving a SafeWord HTML Form authentication scheme removes required information (53416)

The data in the SafeWord Configuration File field was removed when OK or Apply was clicked. This prevented the authentication scheme from being properly saved and created. This is no longer an issue.

Policy Server SNMP Events are not being Registered in HP Systems Insight Manager (53438)

This is no longer an issue.

Java Policy Management API methods, getRealmRealms and getRealmRules, are not Working Properly in SDK 6.0 (47895)

This is no longer an issue. The method getRealmRealms() returns the realms in the specified realm instead of all realms under the given domain. The method getRealmRules() returns the rules under the specified realm instead of all rules under all realms under the given domain.

ODBC Connectivity Test Crashes SiteMinder Management Console on Solaris (52266)

This is no longer an issue.

Export SMDIF Function, doExport(), does not Export the Data in Unicode/UTF Format (52969)

This is no longer an issue. The doExport() using SiteMinder Java API was successful with UTF-8 characters and the exported file contained data in the expected UTF-8 format. Similarly doImport of SiteMinder Java SDK also works properly and was able to import the data in desired format.

SDK SmTest.exe Tool does not Work (53111)

When the SDK is installed on a windows computer without a Policy Server, and the SmTest.exe is attempting to run it returns missing SHSMP.dll error. This is no longer an issue.

Increase in Authentication Time after Upgrading from 5.5 SP3 to 6.0.4 on HPUX (53162)

The authentication time was increased when the user was using the same Oracle policy store and user store. The cursor type when performing queries will return only a single value to avoid potential error. This is no longer an issue. The cursor type will retry query on Oracle when user store schemas contain a union or view.

Running smpolicysrv -stats Appends the lowercase 'l' Character to the Output (53283)

This is no longer an issue. smpolicysrv -stats does not append lowercase 'l' character to the value of Msgs, Waits, and Misses in the Thread pool line and prints the messages in the correct format.

smpolicysrv - stoptrace Command Causes the Console Tracing to Shutdown (48431)

On Windows, when trace logging to console was enabled, on running the command smpolicysrv -stoptrace, the tracing console window was forced to close. This is no longer an issue.

Password Change Fails if it Matches the Encrypted Value of Userpassword or UserDisabled fields in LDAP(51546)

Profile Attributes is a numeric setting for password policies. When this was set, if a new password matched any other profile attribute by that number of characters in a row, the password was rejected. This is no longer an issue. When a password policy specifies a profile attribute length, the Policy Server no longer considers the user's password as part of the profile.

Policy Server Creates New Threads and Terminates Them after a Short Duration (52006)

This is no longer an issue.

C++ Comments in the Code are not Compatible with Some C Compilers (52130)

This is no longer an issue. All C++ styled comments in the C Agent SDK were replaced with C style comments.

Policy Server does not Serve Requests while Rebuilding Policy Cache (52278)

This is no longer an issue. When using the admin UI to change policy store objects, the operational delay was eliminated when rebuilding a large policy cache.

Policy Resolution Fails When a RADIUS Agent Group is Configured for a Realm (52371)

With Policy Server configured for RADIUS authentication, the user was not authenticated when RADIUS realm was configured with an Agent Group. This is no longer an issue. The Policy Server will not verify the value of realm hint attribute if an Agent Group has been configured for RADIUS realm, and the RADIUS realm configured with Agent Group will be added to realm cache.

SiteMinder using LDAP Referral over SSL fails to connect when the Port Number is not Part of the Referred URL (52425)

When using referred URL containing LDAPS, it was being sent to the referred server on non-SSL port 389 instead of SSL port 636. This is no longer an issue. The force assignment of 389 as the port number is disabled for all cases when port is not mentioned in the referred URL. The secure option of the parsed URL is verified and the port 389 or 636 is set accordingly.

LDAP Filter Generated using the LDAP Expression Editor Displays a Syntax Error in the smps log (52687)

LDAP Expression Editor was adding additional spaces while creating the expression, which generated the syntax error, logged in Smps log. This is no longer an issue. LDAP Expression Editor is corrected to create syntactically correct expression without the additional spaces.

Integration of SiteMinder and IAM Toolkit are not Allowed using the Java Policy Management API (52769)

This is no longer an issue. The Java PM API has been enhanced with capabilities to return user groups and user attributes.

Policy Server Experiences Performance Degradation with the Profiler Enabled on Solaris (46553)

This is no longer an issue. Policy Server performance has been optimized when the profiler is enabled on Solaris. Additionally, the BufferedTracing check box is available on the Profiler tab in Policy Server Management Console. When selected, BufferedTracing lets the Policy Server run with the trace messages being buffered when written to the logs.

This results in maximum performance. When unselected, messages are written to the trace logs without being buffered. This results in slower performance, but provides maximum compatibility with the previous log writing behavior.

Crash Related to Memory Corruption in the SmAuthCert library (43092)

While running STIs for some SmAuthCert changes, after the agentapi/authentication STI component was completed, the Policy Server was restarted. This caused memory corruption related crash in the SmAuthCert library. This is no longer an issue.

SiteMinder Single Sign-on (SSO) does not Work Across Multiple User Directories for the Same User Identity (45735)

This is no longer an issue. The Single Sign-on (SSO) feature of SiteMinder will now work across multiple user directories in disparate policy stores even if the user directory name or user DN differ across different user stores for the same actual user identity.

For this, a new Authentication-Validation directory mapping has been introduced. The Authentication-Validation maps authentication directory name to validation directory so that the user authenticated against one user directory can be validated against another user directory. The directory mapping can be done on Universal ID or User DN.

The Authentication-Validation mapping object has three attributes:

- Authentication directory name
- Validation directory OID
- Mapping Type

Policy Server Stops Logging to Oracle after the Database Instance is Shutdown and Restarted (48305)

Policy Server was configured for audit logging to an ODBC database using bulk insertion. When the database was stopped and restarted the logging functions were interrupted. This is no longer an issue. The bulk insertion was fixed to get a refreshed view whenever the database connection is reset.

Policy Server does not Respond when the Centralized OneView Monitor Computer cannot be Reached (48750)

When using a centralized OneView Monitor service, WebAgents relay information to the remote OneView by sending an agent message to the Policy Server. While processing the message, the thread sending the message to the remote OneView was locked and this blocked other threads attempting to relay messages. This is no longer an issue. Policy server and OneView monitor communication was improved. Any problem with OneView monitor or the connection to the monitor will not affect Policy Server functionality or performance.

Received Errors while Installing the Policy Server When Importing a 5.5 Policy Store File (48765)

Run the SmObjImport command twice with the following options:

smobjimport -imypolicystore.smdif -d -w -c -k -v -f

The second time command would run smoothly and no data will be lost. The error messages appear during import using smobjimport, as objects that cannot be imported in the first pass are captured and added into a list of failed objects. These are retried during second pass, and so on, until the list of failed objects stabilizes.

An informatory message Retrying failed objects appears during import of policy store using smobjimport, during every retry cycle when objects that failed to get imported from a previous cycle are imported again.

Received Error using Perl PPM with SiteMinder 6 SP4 (48775)

This is no longer an issue. The Windows reloc_perl command was updated to reflect the configured location in third party.

Received Session Timed Out Error in the Admin UI When Trying to Manage a Policy (48806)

When working with huge policy store, the Admin UI applet throws the "Your session may have timed out" error. This was due to the Admin UI applet trying to send a request to the policy-server using the TLI layer, which generates an exception. The problem was caused when the data received from Admin clients exceeded the dynamically allocated receive TLI buffer at the policy-server. The data is not received successfully at the policy-server and the connection was terminated, and Admin UI displayed the error. The value of maximum allowed size of TLI buffer at policy-server for handling Admin UI messages was set to 32KB.

This is no longer an issue. The buffer size for Admin UI and Policy Server communication is configurable using a registry key:

HKLM/Software/Netegrity/Siteminder/CurrentVersion/PolicyServer/Max AdmComm Buffer Size

If this key does not exist or has a value less than 256KB, the minimum default value is considered as 256 KB.

Changes in the User Directory Object will not Take Effect Without Restarting the Policy Server (48841)

This is no longer an issue. The User Directory cache for authentication or authorization is propagated without restarting the Policy Server.

Policy Rendered Non-editable in the Admin GUI Due to an Invalid IP address Passed in Custom Code (48918)

This is no longer an issue. An exception will be thrown when an invalid IP address is set. This validation check will prevent policy from being rendered non-editable.

Java Virtual Machine (JVM) Encounters Segmentation Violation and Terminates (48962)

When a null session object was passed to the Java AgentAPI authorize() method the JVM crashed. This is no longer an issue.

IP Restrictions not Returned Properly for a SiteMinder Policy (51509)

This is no longer an issue. The Java Policy Management API will return all IP restrictions for a SiteMinder policy.

The S98sm File is not Preserved or Backed up during Upgrade (51829)

This is no longer an issue. The existing S98sm script will be backed up during Policy Server upgrade. Additionally, nete_ps_root will be replaced by full path of SiteMinder installation in S98sm script during install, reinstall, or upgrade.

Authorization Server Threads Hang When Using ACE Authentication (48513)

When using ACE Authentication, the Authorization server threads hung and the Policy Server ran out of connection limits. This is no longer an issue. To avoid the possibility of hanging threads under heavy load conditions, RSA also suggests that RSA trace logging be turned off.

User Authentication Fails When LDAP Logic Operators are used in x.509 Custom Mapping (47908)

Using LDAP syntax to create search filters that contain logic operators caused user authentication to fail. A new registry key, LegacyCertMapping, allows legacy behavior in the certificate mapping and resolves the problem. The KeyType must be configured as REG_DWORD and the Value must be 0 (disabled) or 1 (enabled).

If a value other than 0x1 is configured, or the registry value does not exist, this feature is disabled. The registry key is disabled by default. If the registry key is not enabled, the current behavior is in effect. The registry key is located at HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\PolicyServer.

smnssetup Script is Obsolete (44965)

This is no longer an issue. smnssetup was removed from UNIX kits.

RSA Ace Authentication Server Version 6.0 does not Work Properly with SiteMinder (45984)

This is no longer an issue. RSA Ace authentication is certified to work with SiteMinder.

Separate Admin Account for Policy Store not Listed in Management GUI (47125)

This is no longer an issue. The Management GUI lists the directory name for administrative user when the directory name is not the default one.

SAML 2.0 Assertion Validation Fails on the Service Provider (47252)

SAML 2.0 transaction fails when a valid port is appended to the Assertion Consumer Service URL in Service Provider object on Windows platform. This is no longer an issue. The SAML 2.0 assertion consumer will now accept assertions which specify the default port for the assertion consumer URL.

Smps Log Displays Invalid Credentials Error Message (47265)

This is no longer an issue. When incorrect User Directory credentials are entered and then corrected, the error message is not logged.

Received Operations Error When Trying to View AD Users (47354)

This is no longer an issue. The Windows Policy Server does a better job determining if a SASL bind is necessary when communicating with AD or ADAM directories using the AD directory namespace.

Event not Generated for User Logout in the SiteMinder Audit Logs (47614)

When a user is logged out from the protected website, no event for Logout is generated in the SiteMinder Audit logs. This is no longer an issue. Logout event will be logged in SiteMinder Audit Logs, when auditing is enabled.

LDAP Provider's AddEntry(DsAttrs) does not Follow Referrals When Enhanced Referral Processing is Enabled (47937)

The LDAP provider's AddEntry(DsAttrs) function is using the LDAP SDK directly instead of LdapAdd. This is no longer an issue. Policy Server now properly handles enhanced LDAP referrals when adding entries to an LDAP directory.

When Allow Nested Groups is Selected Only Users Contained in the First Group are Authorized (47946)

If more than one group is listed in a user policy and Allow Nested Group is selected, the authorization is restricted to the first group only. This is no longer an issue. The user contained in any of the groups is authorized.

Custom Code Calling user.addToGroup() Causes smpolicysrv to Crash (48023)

This is no longer an issue. Users are added and removed successfully to or from the group without crashing the policy server.

SmPolicyApi.getPolicyLinks() Triggers a Full Policy Store Cache Refresh Resulting in Poor Performance (48122)

This is no longer an issue. Java API function SmPolicyApi.getPolicyLinks() does not trigger a full policy store cache refresh.

SmPolicyApi.getUserDirSearchOrder() Returns OIDs instead of Names (48221)

The Java Policy Management SDK returns OID strings instead of object names for some methods. This is no longer an issue. The Java Policy Management SDK returns OID strings only for SiteMinder objects which cannot be identified by name property, for example, certificate and directory mappings.

Smobjexport does not Include All Configuration Parameters for Authentication Scheme (48519)

This is no longer an issue. The smobjexport tool now properly exports the field mappings of DCC authentication schemes using the -e flag.

Invalid Value in AuthenticationInstant Attribute (48584)

This is no longer an issue. The value for SAML assertion's AuthenticationInstant attribute is set to the time the user was authenticated at the IdP site.

SiteMinder Installer Overwrites Configuration Files during Upgrade (48704)

Before upgrading SiteMinder, do the following:

- Add .properties to the list of filename extensions for backup under config subdirectory before upgrade.
- Add .ini to the list of filename extensions for backup under db subdirectory before upgrade.

Policy Server Crashes When Trying to View Users in FederationWSCustomUser Store Directory (48846)

This problem is specific to the UNIX platform. This is no longer an issue.

OneView Monitor Page Displays NullPointerException (48928)

OneView Monitor page displays NullPointerException if the Accept-Language HTTP header is not sent by the user's web browser. This is no longer an issue. The OneView Monitor now defaults to English if no Accept-Language header is sent by the user's web browser.

DisallowForceLogin Registry Key (47157)

This service pack includes a new DisallowForceLogin registry key that, when enabled, has the Policy Server display a wrong old password error message rather than redirecting users to a login page when they provide invalid credentials during the password change process.

The key is located here:

HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\PolicyServer

To enable this key, this registry value must be configured as REG_DWORD and contain a value of 0x1. If you set the key to a value other than 0x1 or if the value does not exist, this feature is disabled.

Note: This key is disabled by default.

There are three cases affected by the DisallowForceLogin value.

- Force password change or password expired.
- Self Password change.
- Optional password change.

Fix to SiteMinder Test Tool (47525)

When running in the basic or advanced modes, the SiteMinder Test Tool now successfully authenticates and authorizes users using x509 authentication.

Defects Fixed for 6.0 SP4

Release 6.0 SP4 contains the following fixes:

Fix in SiteMinder User Directory Dialog (19097)

The SiteMinder User Directory dialog is fixed so that if you enter extra characters after the port number when configuring an LDAP-based user store and then click View Contents, the Policy Server issues an error message. Before this fix, there was no error message.

Fix to Policy Server Management Console (42837)

When testing the connection between a Red Hat Linux AS 3.0-based Policy Server and a SQL Server-based policy store, the Policy Server Management Console issued an invalid warning message. This issue is now fixed and the Policy Server Management Console issues a successful connection message.

Policy Server and Sun v440 Servers (43735, 43492)

The Policy Server now has better performance running on Sun v440 servers.

Policy Server's Agent API Updated (44017)

The Policy Server's Agent API has been updated to correct an interaction between Web Agents (or other clients utilizing this API) and the Policy Server under certain load conditions.

Password Policy Pre-processing Updated (44293)

The Policy Server is updated to make sure that password policy pre-processing is applied to users' passwords during authentication.

Fix to smldapsetup -v option (44378, 41649)

When the Policy Server is using multiple LDAP policy stores for failover purposes and you run smldapsetup with the -v option, the utility now provides correct configuration information for each policy store. Previously, running the smldapsetup -v command did not correctly display all of the configuration information for each policy store.

Trusted Hosts and Directory Mappings Changes Now Written to Audit Logs (44379, 44216)

The Policy Server now logs any AuthAz directory mapping and TrustedHost object event activity changes to the SiteMinder audit log files.

Option Pack Variables Display Correctly in Policy Server User Interface (44395)

Policy Server Option Pack variables are now properly displayed in the Policy Server User Interface when the Policy Server is running in mixed mode. Mixed mode is where the 6.x Policy Server connects to a 5.x policy store.

Policy Server Enhancement for Active Directory-based User Stores (44721)

The Policy Server has been enhanced to improve its interaction with Active Directory-based user stores. When authenticating against an AD namespace, the Policy Server binds to Active Directory using SASL. If a user's common name (CN) is different from the user's Windows logon name, the user can still authenticate even if the EnableSaslBind registry setting exists on the Policy Server machine.

The EnableSaslBind setting is a DWORD registry key that you can set to 0 or 1:

HKLM\Software\Netegrity\SiteMinder\CurrentVersion\Ds\LDAPProvider\EnableSaslBind

This setting disables or enables the SASL protocol while authenticating users. For example, if EnableSaslBind does not exist and you configure this setting to 1, the bind occurs with SASL. If EnableSaslBind exists and you configure this setting to 0, the bind occurs with Simple Authentication mechanism.

Active Directory User Store Invalid Password Issue Fixed (44956)

If the Policy Server was connected to an Active Directory user store and was idle for a long period of time (for example, overnight), users could successfully authenticate after entering an invalid password. This issue is now fixed.

Oneview Monitor Failure Issue Fixed (44961)

This service pack fixes an issue where the Oneview Monitor failed under heavy SNMP load.

Renaming Host or Agent Configuration Object Not Allowed (45047, 36633)

The Policy Server User Interface no longer allows you to rename an existing Host or Agent Configuration Object.

Scope Switch Fix (45052, 44786)

This service pack includes a fix to the Policy Server to make sure that the scope switch specified for a given User Directory is adhered to during authentication.

- If you set the scope to One Level, only users present at one level below the search root are found by the Policy Server and authenticated.
- If you set the scope to Sub Tree, all the users present below the search root are found by the Policy Server and authenticated.

Policy Server Hanging Condition Fixed (45247, 45023)

This service pack includes a fix to a condition that caused the Policy Server to hang during shutdown.

Fix to Custom Certificate Mapping Feature (45362)

The Policy Server's custom certificate mapping feature involving multiple attributes of the same type are now handled correctly. The Policy Server now maps the particular index attribute in the certificate as specified in the certificate custom mapping expression.

OpenWave Directory Server Now Supported (46971, 46806)

The Policy Server is now certified to work with an OpenWave Directory Server user or policy store. The Openwave Directory Server does not support LDAP referrals.

Note: Configuration instructions exist in the SM60SPx_Openwave_Config.pdf file.

Shrink Memory Pool Enabled Registry Value (45457, 30630)

This service pack includes a new Shrink Memory Pool Enabled registry value that can be manually configure to shrink the amount of memory used by the Policy Server process. You can add this registry value at the following location:

HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\PolicyServer

- To enable the Shrink Memory Pool Enabled feature, configure the registry value as REG_DWORD that contains a value of 0x1 in order.
- To disable this feature, configure a value other than 0x1 or remove the registry value altogether. This feature is disabled by default.

Policy Server Relational Database Policy Store Issue (45462, 44294)

This service pack has a fix that allows the Policy Server to correct a failover to a secondary data source that is configured for an relational database policy store. Specifically, if the Policy Server is restarted and the policy store is shutdown or paused, the Policy Server connects to the secondary policy store.

Microsoft Active Directory Global Catalog User Store Enhancement (45879, 45054)

When the Policy Server is connected to a Microsoft Active Directory Global Catalog user store and a policy is configured to allow nested groups, the Policy Server uses a MemberOf attribute user record for more efficient searches.

ACE Debug Logging Fix (45882, 43976)

This service pack has a fix that allows the Policy Server to make sure that enabling ACE debug logging does not cause the Policy Server to terminate abnormally during authentication.

Policy Server Management Console Limitation on Red Hat AS 3.0 (47302) (42832)

If the Policy Server's policy store resided in either an Oracle or IBM DB2 database, the Policy Server Management Console failed when you click the "Test Connection" button on the Data tab. This issue in now fixed.

Perl Scripting Interface Limitation on Red Hat AS 3.0 (47304) (42834)

If the Policy Server's policy store resided in either an Oracle or IBM DB2 database, the Perl Scripting Interface failed at the following call while creating a new session:

```
$session=$pmgtbase->CreateSession()
```

This issue is now fixed.

DeadHandleListLiveTime Registry Setting Obsolete (47226) (47120)

The user directory LDAP server layer no longer relies on the DeadHandleListLiveTime registry setting. Now, dead LDAP handles are automatically managed by the Policy Server and no longer require any extra registry configuration by users. This change allows the Policy Server to manage user directory LDAP server issues more efficiently.

Due to this change, the following registry key is now obsolete:

HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Ds\LDAPProvider\DeadHandleListLiveTime

SafeWord Debug Logging Failure (45953, 43097)

SafeWord debug logging no longer causes the Policy Server authentication service to fail. Previously, if you had a SafeWord HTML Forms Authentication Scheme configured in the Policy Server and enabled SafeWord debug logging, the Policy Server failed. This issue is fixed.

Note: For a Solaris Policy Server, the operating system must be at Solaris 9 or higher. In addition, the Safeword server must have the 3.1.1 patch04_01 installed.

Scripting Interface for Perl User Directory Contents Issue Fixed (46141)

In the Scripting Interface for Perl, the user directory contents are now properly shown for calls to GetContents() for custom directories.

Regular Expression Pattern Matching Issue Fixed (46322)

The Policy Server no longer fails using regular expression pattern matching under heavy load.

Parameter List Does Not Maintain Specified Order in Host Configuration and Agent Configuration Object Dialogs (46415)

The parameter list ascending/descending order issue in the SiteMinder Host Configuration and SiteMinder Agent Configuration Object Dialogs is now fixed.

Update to Profiler Log Files (46425)

The Policy Server's Profiler log files have been modified so that the:

- User data field contains the login name of user.
- User DN contains complete DN of the user.

State Attribute of the LDAP Schema Changed from "s" to "st" (46740)

When loaded into the LDAP Expression Editor or Certificate Mapping Dialogs, the "s" attribute is no longer labeled as "State". Now, it appears as "s". The Policy Server's LDAP Expression Editor honors unrecognized attributes and does not change them. As a result, opening an expression containing an "s" attribute does not cause the Policy Server to converted it to "st".

Now, you need to manually enter the "s" attribute, as it no longer appears in the LDAP Expression Editor Dialog's drop-down menus. You can do this by typing "s" into the first field of the "Condition" input instead of selecting "st (State)" from the drop-down menu. You cannot create new certificate mappings using the "s" attribute, as such a configuration would not work.

For certificate mappings, a third-party library translates the state attribute's OID in the certificate into the string "st", which until this fix, would not be recognized by the Policy Server.

Certificate-based Authentication Issue Fixed (46999, 46149)

Certificate-based authentication requiring certificate validation against an Active Directory-based user store no longer fails under heavy load conditions.

Update to Password Services (47020)

Password Services allows users to disable the tracking of successful and failed logins separately. Password policies that only track failed logins modify the user store upon a successful login only if it is necessary to reset the number of failed logins. This prevents failed login tracking from counting the cumulative number of failed logins when successful login tracking is disabled.

Password Services Failure Tracking Issue Fixed (47110, 38445)

When failure tracking is enabled in Password Services, the Policy Server no longer sends duplicate requests to modify the user's password data attribute.

Policy Server Caching Problem Fixed (47122)

The service pack fixes a caching problem that caused the Policy Server to fail during authorization after a large number of different users are authorized.

NTLM Authentication Scheme Failure Issue Fixed (47123)

The Policy Server no longer fails under heavy load when it is using an NTLM authentication scheme.

SafeWord Debug Logging Failure (45953, 43097, 47258)

SafeWord debug logging no longer causes the Policy Server authentication service to fail. Previously, if you had a SafeWord HTML Forms Authentication Scheme configured in the Policy Server and enabled SafeWord debug logging, the Policy Server failed. This issue is fixed.

Note: For a Solaris Policy Server, the operating system must be at Solaris 9 or higher. In addition, the Safeword server must have the 3.1.1 patch04_01 installed.

Viewing Active Directory User Directory Issue Fixed (46238)

This service pack fixes an issue where you could not view the content of a Windows 2000 Active Directory User Directory configured with the AD Namespace without specifying a certificate database.

Defects Fixed for 6.0 SP3

Release 6.0 SP3 contains the following fixes:

Accessing Now Protected or Unprotected Realms Behaves as Expected (39443)

The Policy Server has been updated to make sure that resources in protected/unprotected realms are correctly protected or unprotected as expected.

CRLs Reporting Error Message Fixed (39446, 40045)

On Windows and Solaris systems, the Policy Server's Cert-C libraries has been updated to correct an issue with CRLs reporting a "Failure in RSA Cert-C library getting CRL" error message.

Entering non-ASCII Characters For User Directory Objects (39635)

The Policy Server User Interface now allows you to enter non-ASCII characters for username credentials when configuring user directory objects.

Enhancement to smreghost (39712)

The smreghost utility has been enhanced to include a new optional -o parameter that enables you to overwrite an existing trusted host.

New Registry Entry to Fix Audit Logging Exceptions (39991, 39307)

On Windows, the Policy Server has been enhanced to remove errors caused by audit logging exceptions. This enhancement includes a new ConnectionHangwaitTime registry entry that you can set to avoid audit logging exceptions. The minimum setting for this value is 30 seconds. If you set this value to less than 30 seconds, the Policy Server ignores this value and uses the minimum value of 30 seconds.

The new registry entry is located:

HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Database\ConnectionHangwaitTime

In addition, to avoid the audit logging exception, the following registry variables need to be tuned at the following location:

HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Database

QueryTimeout

Suggested tuning is 30 seconds

Default: 15 seconds

LoginTimeout

Suggested tuning is 30 seconds

Default: 15 seconds

ConnectionHangwaitTime

Suggested tuning is 60 seconds

Default: 30 seconds

Note: This tuning is done to avoid any audit data loss; however, this tuning may lead to some performance issues. To improve performance, you can configure audit logging in a text file instead of a database.

Policy Server and Oracle Encrypted Passwords (39411, 38408)

The Policy Server has been updated to correctly handle authentication of system users in an Oracle database if you are using the Oracle encrypted password feature.

Correct Time Being Returned for LAST_MESSAGE_TIME Element (39645)

The Policy Server has been fixed to return the proper time value in seconds for the LAST_MESSAGE_TIME sub element of the AGENT_CONNECTION element in an smpublish report.

Update to Policy Server trace Logging (39670)

The Policy Server trace logging now functions correctly when there are more than 255 connections (or file handles). It is also recommended that you use a utility like ulimit on Solaris to increase the soft limit of file descriptors that can be opened in a session.

Return Values for Perl Methods ValidatePassword() and SetPassword() (40153, 40345)

These Perl Policy Management API methods now return correct values to reflect success or failure of the call.

Windows Authentication Scheme Template Enhancement (40201)

You can now configure a Windows Authentication Scheme template in the Policy Server User Interface.

New Perl Methods for Converting Between v4.x Agents and v5.x Agents (40299, 39714)

The following Perl PolicyMgtAgent methods let you convert between v4.x agents and v5.x agents:

- ConvertFromLegacy()
- ConvertToLegacy()

LDAP User Property Searches Enhancement (40337, 38805)

The Policy Server has been enhanced to correct the handling of user property searches in LDAP-based user stores that return no results.

Active Directory Integration Update (40338, 39912)

With the Active Directory integration enabled, the Policy Server has been enhanced to make sure that a user is not prompted for a password change when the DONT_EXPIRE_PASSWORD flag in the AD user state is set or enabled.

Policy Server Handling User Names in Parenthesis (40444, 39977)

During authentication and authorization, the Policy Server is enhanced to handle user names enclosed in parenthesis if you set the following registry variable:

HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\CurrentVersion\Ds\AllowUserNameWithinParentheses

If this registry setting:

- Does not exist, the user names within the parentheses are not allowed during authentication and authorization.
- Exists and the value is 0, the user names within parentheses are not allowed during authentication and authorization.
- Exists and the value is 1, the user names with parentheses are allowed and not treated as a user attribute.

Realms and Resources Cache Searches Issue Fixed (40564)

The Policy Server now correctly performs realms and resources cache searches without failing.

Ignoring pwdLastSet in Active Directory Global Catalog (40627, 35293)

If the Policy Server is using Active Directory Global Catalog, the pwdLastSet attribute can be ignored if you manually add the following registry value:

SiteMinder\CurrentVersion\Ds\LDAPProvider\IgnoreADPwdLastSet

To enable this feature, set this REG_DWORD value to a non-zero value.

Note: This feature was removed in 6.0 SP2 and was added back in at v6.0 SP2_CR002.

API Enhancements (39725)

The Policy Server now includes the following C Policy Management API functions that retrieve any policy objects by name:

- Sm_PolicyApi_GetAgentByName()
- Sm_PolicyApi_GetAgentTypeByName()
- Sm_PolicyApi_GetAgentTypeAttrByName()
- Sm_PolicyApi_GetAgentConfigByName()
- Sm_PolicyApi_GetHostConfigByName()
- Sm_PolicyApi_GetTrustedHostByName()
- Sm_PolicyApi_GetTrustedHostExByName()
- Sm_PolicyApi_GetUserDirByName()
- Sm_PolicyApi_GetAdminByName()
- Sm_PolicyApi_GetSchemeByName()
- Sm_PolicyApi_GetRegistrationSchemeByName()
- Sm_PolicyApi_GetPasswordPolicyByName()
- Sm_PolicyApi_GetODBCQuerySchemeByName()
- Sm_PolicyApi_GetGroupByName()
- Sm_PolicyApi_GetDomainByName()
- Sm_PolicyApi_GetRealmByName()
- Sm_PolicyApi_GetRuleByName()
- Sm_PolicyApi_GetResponseByName()
- Sm_PolicyApi_GetPolicyByName()
- Sm_PolicyApi_GetGlobalRuleByName()
- Sm_PolicyApi_GetGlobalResponseByName()
- Sm_PolicyApi_GetGlobalPolicyByName()
- Sm_PolicyApi_GetVariableTypeByName()
- Sm_PolicyApi_GetVariableByName()
- Sm_PolicyApi_GetAffiliateDomainByName()
- Sm_PolicyApi_GetAffiliateByName()

The following existing PERL Policy Management APIs also had performance enhancements:

PolicyMgtSession methods

- GetAdmin()
- GetAffDomain()
- GetAgent()
- GetAgentConfig()
- GetAgentGroup()
- GetAgentType()
- GetAuthScheme()
- GetDomain()
- GetGlobalPolicy()
- GetGlobalResponse()
- GetGlobalRule()
- GetHostConfig()
- GetODBCQueryScheme()
- GetPwdPolicy()
- GetRegScheme()
- GetUserDir()
- GetVariableType()

PolicyMgtDomain methods

- GetPolicy()
- GetRealm()
- GetResponse()
- GetResponseGroup()
- GetRuleGroup()
- GetVariable()

PolicyMgtRealm methods

- GetChildRealm()
- GetRule()

PolicyMgtAffDomain methods

- GetAffiliate()

Import and Export of Perl Global... Methods (39979)

The Perl Policy Management API methods GlobalResponse(), GlobalRule(), and GlobalPolicy() can now be imported and exported correctly.

Policy Server Improved When Connecting to Large LDAP Policy Store (40062)

The Policy Server User Interface's performance has been improved if the Policy Server connects to LDAP-based policy store that contains extremely large amounts of data.

To improve of the performance of this type of configuration, set the following LDAP search timeout registry setting:

HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\LdapPolicyStore\SearchTimeout

You should set the LDAP search timeout registry setting at a value that is large enough to keep the Policy Server from timing out when it is retrieving large amounts of policy store data from an LDAP server. The default value is 20 seconds.

Before setting this registry setting, you should consider the following factors:

- Network speed and bandwidth
- Size of LDAP search query response
- LDAP directory server connection state
- LDAP directory server load

Also, the following is a new Max AdmComm Buffer Size registry entry that allows you to tune the buffer size for the Policy Server User Interface:

HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\PolicyServer\Max AdmComm Buffer Size

This value defines the maximum amount of byte data in a single packet passed from the Policy Server to the Policy Server User Interface.

You can set this value between 256 KB to 2 GB and, when no setting exists, the default is 256 KB.

Note: Increasing the buffer size could result in decreased Policy Server performance.

Improvement to Policy Server Shutdown Log Messages (40149)

If the Policy Server stops running due to lack of file descriptors, it now outputs detailed error messages to the log files that explain what the problem is.

Improvements to Policy Server Failure To Start Messages (40316)

If the Policy Server fails to start due to missing mandatory registry keys, it now outputs detailed error messages to the log files that explain what the problem is.

Improvements to Policy Server Idle Client Connection Messages (40626)

The Policy Server now outputs the correct error message to the log files if there is a closure of idle but established client connections.

Policy Server Handling of Oracle Server Error Codes (40630, 40629)

The Policy Server has been fixed to handle a ORA-12154 error code from the Oracle database server and maps it to an appropriate error message instead of issuing an "Invalid Credentials" message.

Policy Server Shutdown Issue on Solaris (40669)

On Solaris, when an administrator shuts down a Policy Server while it is running under heavy load, the server shuts down gracefully.

Memory Growth Issue Fixed (40828)

The Policy Server has been fixed to alleviate a memory growth issue that occurs during realm and rule updates to the policy store.

Host Configuration Object No Longer Has An Extra Space (40904)

The Policy Server User Interface no longer adds an extra space when you are creating a multi-value Host Configuration Object. Previously, before this fix, the extra space in the Host Configuration Object caused the Agent to connect to the Policy Server User with an empty IP address.

Update to Policy Server's SM<SERVICE> -publish Directive (40946, 40545)

The Policy Server's SM<SERVICE> -publish directive now generates well-formed XML output with all the AGENT_CONNECTION elements even if there are a large number of Web Agent connections.

Policy Server Connections to Audit Log Databases (40964, 40932)

The Policy Server now correctly handles connections to audit logging databases when there are logging exceptions.

Windows Authentication Scheme Creation Fix (41112)

The Policy Server User Interface now properly creates Windows Authentication schemes for LDAP or Active Directory-based user stores.

Policy Server starts as expected in Mixed Mode (41133)

When you disable the "Enable Agent Key Generation" option in the Policy Server Management Console and the Policy Server is using mixed versions of the policy (6.0) and key (5.5) stores, the Policy Server starts as expected.

User Names Containing a Comma No Longer Cause an Oracle Database Error (42122, 41838, 41108)

When the Policy Server is using an Oracle user directory, users that have a comma in their user name are authenticated with the out-of-the-box Oracle function. Previously, before this fix, this type of user name would cause the Policy Server to throw a database error.

Enhancement to Policy Server Request Processing Handling (40315)

The Policy Server has been enhanced to ensure fair processing of Agent API and Agent connect requests during normal request processing.

Update to Password Generation During Self-registration (40540)

The Policy Server has been fixed to ensure correct generation of passwords during self-registration when the Policy Server is using an:

- LDAP-based user directory with multi-byte character support.

  OR

- Oracle-based session store.

Update to the Policy Server Authentication Service (41008, 40306)

The Policy Server authentication service now accommodates the calling of the Policy API initialization (Sm_PolicyApi_Init) and Policy API release (Sm_PolicyApi_Release) methods inside the respective hook functions-SmAuthInit() and SmAuthRelease()-in a custom authentication scheme.

ODBC Tracing Fix for Policy Stores in Relational Databases (41098)

The Policy Server now properly executes when you enable ODBC tracing for a policy stores residing in a relational database.

Note: You should only enable ODBC tracing for troubleshooting purposes since it impacts Policy Server performance.

Policy Server Agent Key Management Issue (41497)

The Policy Server has been fixed to ensure proper Agent key management if the Policy Server is using separate policy and key stores residing in an Oracle databases.

Return Value for Perl Method GetAllRules() (41514)

This Perl Policy Management API method now returns the correct value when no rules are present in a given policy. This method is in object PolicyMgtPolicy.

Update to Policy Server Shared Secret Management (41519)

The Policy Server has been fixed to ensure correct handling of updates to temporal fields related to shared secret management when operating with legacy Web Agents.

Groups Returned from Perl Method GetAllAgentGroups() (41627)

This Perl Policy Management API method now returns all configured agent groups in the session. This method is in PolicyMgtSession.

Policy Server Startup Issue (41690)

On Solaris, the Policy Server is fixed to startup gracefully under heavy load conditions and to no longer dump core.

Solaris SiteMinder Agent API Shared Library Fix (41741, 41586)

The SiteMinder Agent API now modifies the linkage for the Agent API shared library on Solaris to be self-contained with respect to other third-party libraries used in the same process.

Policy Server Can Now Log Exceptions to Windows Event Viewer (41821, 41363)

The Policy Server has been enhanced to make sure that any exceptions occurring during audit logging are now recorded to the Windows Event Viewer, which is in addition to the SiteMinder logs.

Be aware of the following:

- Events are logged under the ObjAuditLog and AccessAuditLog categories.
- Any exceptions occurring in audit logging due to object management are recorded under the ObjAuditLog category.
- Any exceptions occurring in audit logging due to user-related activities such as authentication, authorization, administration, and affiliate activity are recorded under the AccessAuditLog category.

To enable Policy Server logging to the Windows Event Viewer

1. Open the Windows Registry Editor.
2. Go to:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Application\SiteMinder.

3. Change the CategoryCount registry key to 7.

Enhancement to SNMP Variables (41839, 41620)

The Policy Server is fixed to make sure that the following SNMP variables are correctly displayed in milliseconds:

- webAgentLoginAvgTime
- webAgentValidationAvgTime
- webAgentAuthorizeAvgTime

Policy Server Return Correct Reason Codes from Custom Authentication Schemes (41843, 37718)

The Policy Server has been fixed to return the correct reason code from custom authentication schemes when a password policy is enabled for that scheme.

Return Value for Perl Method GetAllUsers() (42032)

This Perl Policy Management API method now returns the correct value when no users are present in a given policy. This method is in PolicyMgtPolicy.

Policy Server Processes Policy Changes Faster (42523)

The Policy Server has been optimized to ensure faster processing of policy changes made by custom applications developed using the PERL or C Policy Management APIs.

To enable the faster processing of policy changes do one of the following

- Omit the PreLoadCache flag during the call to the initialization function.
- Introduce a small time delay in the custom application to make sure there is adequate time for cache processing before exit.

Policy Server Invalid Realm Processing (40665)

The Policy Server is updated to ensure correct processing of client requests containing invalid realms.

Policy Server's Handling of Users Changing Passwords (41930)

The Policy Server is fixed to make sure that a user in a "Change Password State" is handled correctly when this user provides invalid credentials during login.

Update to CRL Lookup Function (41977)

The Policy Server CRL lookup mechanism has been enhanced to accommodate the Certificate Distribution Point's (CDP) field containing URL's in client certificates.

Improvements to smobjexport and smobjimport (42210)

Using smobjexport and smobjimport, you can now transfer policy store data using administrators from an external directory.

Update to Certificate Mapping Enhancement (42233)

The Policy Server v6.0 SP 2 release introduced support for multi-value components in certificate Issuer and Subject DN fields. However, these changes caused existing certificate mappings to fail when attributes were part of a multi-value DN.

The Policy Server is fixed to enable existing mappings to continue to function correctly. This fix adds backwards-compatibility functionality for single-attribute and simple custom mappings.

Note: Custom mappings that relied on attributes which occur multiple times in a DN (for example %{CN2} or %{UID2}) still behave differently than they did before if any of the attributes being mapped are part of a multi-valued DN component.

Policy Server's Handling of a User With Different Passwords in Two User Stores (42356)

If a user with the same login ID exists into two disparate directories with varying passwords and the entry in the first user directory is disabled, the Policy Server now enables access to a resource based on the credentials available in the second user directory.

DeadHandleListLiveTime Registry Setting Value Increased (42528, 41818)

The minimum default value of the Policy Server's DeadHandleListLiveTime registry setting has been increased to 3 minutes.

The DeadHandleListLiveTime registry setting is located here:

HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Ds\LDAPProvider

Enhancement to Certificate Mapping Exact Match Functionality (42631)

The Policy Server certificate mapping exact match functionality has been enhanced to allow for optimized searches based on the DN field from the client certificate.

Update to PERL Policy Management API (CLI) (42771)

The PERL Policy Management API (CLI) has been corrected to make sure that Agent and Host configuration objects can now be correctly exported and imported.

Improvement to Certificate-based Authentication (42855, 42989)

The Policy Server has been fixed to ensure correct processing of attributes contained in a custom mapping expression during certificate-based authentication.

Policy Server's Policy Restrictions Updated (43063, 41644)

The Policy Server has been fixed to make sure that any password changes performed through the DMS API is validated to conform to policy restrictions set through the Policy Server User Interface.

Return Values for Perl Methods ValidatePassword() and SetPassword() (40153, 40345, 43120)

These Perl Policy Management API methods now return correct values to reflect success or failure of the call.

Policy Server Supports LDAP V3 Protocol (42979)

The Policy Server has been enhanced to use the LDAP V3 protocol for all applicable LDAP operations when this protocol is supported by a given LDAP directory server.

Flushing the Cache and Viewing Response Object Properties (27488)

While using the Policy Server User Interface, if you flush the cache, you cannot view response or global response object properties unless you click other objects in the UI and then click the original object again.

Limitation When Configuring Connections to Active Directory in Application Mode (ADAM) (30221, 29837)

SASL-based binds using Windows generic security services are not supported by ADAM. When the Policy Server is connected to an ADAM user store it will use simple LDAP binds instead of SASL-based LDAP binds.

Important! Simple LDAP binds are not secure. We strongly recommend using SSL-based LDAP connectivity for secure communication with ADAM.

Policy Server on Red Hat Enterprise Linux Advanced Server Could Hang when Using a DB2 User Store (31501)

When a Policy Server on Red Hat AS was configured to authenticate against a DB2 user store, the log and tracing files (smps.log and smtracedefault.log) grew rapidly in size. If this size exceeded that which was allowed by the operating system (typically 2GB), the Policy Server hanged. This issue is fixed.

The following was the workaround for this issue:

Set the smps.log (default name of the log file) file to roll over at less than 2 GB. CA recommends rolling the file at 1 GB. To configure log file rollover, use the Logs tab in the Policy Server Management Console. To minimize tracing to the smtracedefault.log (default name of the trace file) file, disable tracing or reduce the amount of information written to this file.

User Lookup With DB2 User Store May Not Work Correctly (31451)

The Policy Server cannot retrieve custom user attributes when using a DB2 user store. Error messages such as the following are recorded in the smps.log file:

[4212/3536][Tue Jun 08 2004 13:53:09]
[SmDsOdbcProvider.cpp:738][ERROR] Database Error executing query ('select rtrim(Disabled),rtrim(UserID) from SmUser where Name = 'user1''). Error: Internal Error:Database error. Code is -4007 (DBMSG: <<<State = HY000 Internal Code = -440 - [DataDirect][ODBC DB2 Wire Protocol driver][DB2]No function or procedure was found with the specified name (RTRIM) and compatible arguments.>>>) .

[4212/3536][Tue Jun 08 2004 13:53:09][SmDsOdbcProvider.cpp:738][ERROR] Database Error executing query ('select rtrim(Disabled),rtrim(UserID) from SmUser where Name = 'user1''). Error: Internal Error: Database error. Code is -4007 (DBMSG: <<< State = HY000 Internal Code = -440 - [DataDirect][ODBC DB2 Wire Protocol driver][DB2]No function or procedure was found with the specified name (RTRIM) and compatible arguments.>>>).

Fix Entering Incorrect AD/ADAM User Directory Information in Policy Server User Interface (31504)

This service pack fixes an error if you enter incorrect user directory information in the Policy Server User Interface when specifying the AD namespace for ADAM or Active Directory.

If the Policy Server is configured to use ADAM or Active Directory as a user store and you enter incorrect AD namespace information in the User Directory dialog, the Policy Server fails. The Policy Server also fails if the settings are correct but it cannot contact the AD server.

Workaround: Enter correct AD namespace information in the User Directory dialog.

Web Services Variables Fail When Configured to use SSL (27636)

Web Service variables may fail to be evaluated under load if they are configured to use an SSL connection to a Web service.

Running Scripts Built with the Policy Management API (28556)

A script built with the Policy Management API must run as the same user who installed the Policy Server (for example, smuser on UNIX platforms).

Password Services and Multiple User Directories in Policy Domain Issue (40147, 19135)

If you have Password Services configured in a policy domain that contains more than one user directory and users enter an incorrect password when they are required to change their password, they are now redirected to the password change confirmation screen. Previously, they were incorrectly redirected to the login form screen.

Before this fix, the Password Services redirect only fired if the user directory within the password policy was the last user directory in the search order.

Improvements to Session Server's Handling of Heavy Load (31430, 29967)

Symptom:

When the session server was under heavy load, it generated errors when it added or removed new sessions from the session server database tables. At the same time, the session server also stopped removing expired and idled-out sessions from the session store. These issues were caused by maintenance queries taking longer than what the Policy Server allowed in the default query timeout setting.

Solution:

In this service pack, all of the issues listed above are now fixed. The Policy Server can now better handle longer-running session server maintenance task queries-such as removing idled-out or expired sessions-using a new MaintenanceQueryTimeout registry setting.

You can modify the MaintenanceQueryTimeout setting at the following location:

HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\SessionServer

The default value is 60 seconds. However, if the session server is under heavy load, you need to increase this setting to a value large enough to allow the maintenance thread to complete all tasks successfully.

Policy Server Failed Due to Heavy Load from SMTest Script (43296)

The 6.0 SP2 CR03 Policy Server failed in DoAccounting when a policy domain was deleted under load created by a SitMinder Test script that included accounting and management requests. When the script was still running, the Policy Server core dumped each time smexec restarted the Policy Server. This is no longer an issue.

ODBC Tracing Caused Linux Policy Server to Dump Core (43676)

The Linux RHAS 2.1 Policy Server no longer core dumps when ODBC tracing is turned on.

Policy Server Uses Updated RSA ACE SDK Version (43221, 43815)

The Policy Server is upgraded to use the new RSA ACE SDK version 5.0.3.2

Policy Server Management Console Failure Fixed (42953)

The Policy Server Management Console no longer fails if you open the About dialog (Help > About) or set the SiteMinder super user password from the Super User tab.

Policy Server/User Directories Load Balancing Issue (43086) (41697)

In a load balancing configuration consisting of multiple LDAP user directories and Policy Servers, if one user directory is stopped, then all Policy Servers hang even though there are other user directories available for failover. In this example, you stop the user directory using the pstop command.

In this service pack, this issue is fixed and the user directory failover happens as expected.

ODBC Trace Logging Fix (42541)

The Policy Server no longer fails under load if ODBC trace logging is enabled.

This issue still exists on the Red Hat Enterprise Linux AS 3.0 platform.

Entering a Host Name in the SiteMinder Agent Dialog (44172)

The SiteMinder Agent Dialog now allows you to enter a host name in the IP Address or Host Name field if you are configuring a 4.x Agent. Previously, before this fix, the Policy Server would only allow you to enter an IP Address and not a host name.

Defects Fixed for 6.0 SP2

Release 6.0 SP2 contains the following fixes:

Resource in Unprotected Realm when Rule is Not Associated with a Policy (30672)

The Policy Server now protects a resource matching a rule under an unprotected realm when the rule is not associated with a policy.

New GetUserContext Function in C Policy API (31014, 29981)

A new GetUserContext function in the C Policy API populates the Sm_Api_UserContext_t structure.

Fix in Oracle Encrypted Password Feature (31266, 30582)

If you enable the Oracle encrypted password feature for an Oracle user store and then access this store using the Oracle Call Interface (OCI) namespace, authentication succeeds. Previously, before this fix, the Oracle encrypted password feature did not work when using OCI connections to the user store.

Improvements to CoInitialize() (31291, 31131)

The error handling and logging of function calls to CoInitialize() are improved. Now, if any of the CoInitialize() calls fail, the Policy Server now prints the error message along with the return value for CoInitialize().

smobjimport Failed When Importing Rules with a Large String Length (31330, 33709, 31187)

When importing a large policy store using the smobjimport utility, if a rule group has rules with object ID's containing a string length of more than 4095 characters, the utility no longer fails.

New Connections Caused Policy Server to Create Web Agent Handshake Timeouts (31362, 31003)

This service pack fixes a condition where new connections to the Policy Server would not receive the correct priority handling, which resulted in handshake timeouts with Web Agents.

Certificate Authentication Scheme Enhanced (31583, 31154)

The certificate authentication scheme for cert-only authentication is enhanced so that the Policy Server only performs certificate mapping functionality during the disambiguation and not in the authentication phase.

Policy Server Custom Authentication Scheme Race Condition Fixed (31604, 30989)

A failure, which results from a Policy Server race condition caused by a custom authentication scheme returning failure in the SmAuthInit() hook function, is fixed.

Migration Fix for Scripting Interface for Perl (31620, 31273)

When using the Scripting Interface for Perl, migrating policy store data now works correctly if you change from one policy store to another in the same Perl script.

Policy Server Clears Object Cache Correctly (31690, 31544)

The Policy Server now clears the object cache correctly when policy store context is released.

Fix for Policy Server User Interface When Using DMS Wizard (33682, 31199)

The Policy Server User Interface no longer hangs when running the DMS Configuration Wizard multiple times.

Policy Server Writing Keys to Separate ODBC Database (33698)

The Policy Server now updates key information correctly when it is configured to use a separate ODBC-based key store than the one used for the policy store.

Custom Active Response Causing Policy Server to Fail (33723, 31648)

This service pack fixes a Policy Server failure caused by a custom active response calling the SmQueryVersion() function.

Policy Server User Store Connection Enhancement (33920, 31616)

The Policy Server now tries to reestablish an LDAP connection immediately after it fails to connect to a user directory. Before this fix, the Policy Server had to wait for 30 seconds before it could reestablish the user store connection.

Certificate Authentication Schemes Enhancement (33940, 31652)

The Certificate+Basic and Certificate+Forms authentication schemes now only authenticate a user when the user name presented in the form is an exact match of the one in the certificate.

Missing Active Directory Policy Store Upgrade File Included (33845)

The 6.0 Policy Server installation program was missing the AD_Upgrade_SM4x_To_SM60.ldif file, which is required to upgrade a 4.61 SP5 Active Directory policy store to 6.0. This service pack includes this upgrade .ldif file.

For instructions on using the AD_Upgrade_SM4x_To_SM60.ldif file, see the *Upgrade Guide*.

Enhancement to Policy Server Certificate Authentication Library (33936, 31595)

This service pack includes a fix that extends the list of well-known extensions handled by the Policy Server certificate authentication library. The Policy Server can now handle the dmdName attribute (OID 2.5.4.54), which allows certificates issued by issuers with a dmdName attribute in the IssuerDN to be used for successful authentication.

Policy Server Authentication Service calling Policy API Init and Release Functions (33966, 31579)

The Policy Server authentication service now accommodates calling the Policy API init and release functions at any location inside a custom authentication scheme.

Dynamic Search No Longer Causes Policy Server to Time Out (34157, 33822)

The Policy Server no longer times out when searching for users in dynamic groups if there is a large number of users that meet the dynamic group search filter criteria. Previously, before this fix, this dynamic search caused the Policy Server to time out, which resulted in users not getting authorized.

Policy Server No longer Hangs Due to SQL Server ODBC Connection (34215, 34084)

The SQL Server ODBC connection to the Policy Server no longer hangs. Previously, before this fix, this connection would hang since the Policy Server attempted to continuously reconnect to the SQL Server policy store.

Authorization or Authentication Event Rule Type Fix (33766)

The Policy Server did not protect resources that matched an Authorization or Authentication event rule type. In this service pack, this issue is fixed.

6.0 and 5.5 Policy Server Sharing Same Policy Store Issue (34079)

When a 6.0 and 5.5 Policy Server are sharing the same LDAP policy store, the 6.0 Policy Server now generates errors under load if you delete rules using the 5.5 Policy Server Policy Server User Interface.

Policy Server Does Not Fail When Removing Web Agent Connections (34265)

The Policy Server no longer fails intermittently when cleaning up Web Agent connections that are under heavy load.

Policy Server Resource Protection Status Issue (34418)

The Policy Server now returns the correct resource protection status when there is a rule with a wildcard (*) on the resource.

Certificate-based Authentication OCSP Connection Issue (34587) (34541)

During certificate-based authentication, if the you assign the IgnoreNonceExtension attribute to the value YES (which is case sensitive) in the smocsp.conf file, then the Nonce extension is disabled in the OCSP request, which is required by the CoreStreet responder for OCSP processing of certificate validity.

The following example smocsp.conf file shows the Nonce extension as being disabled in the OCSP request:

```
[
OCSPResponder
IssuerDN C=de,O=InsecureTestCertificate,CN=For Tests Only next
generation,E=insecure@test.insecure
```

AlternateIssuerDN C=de,O=InsecureTestCertificate,CN=For Tests Only next generation,E=insecure@test.insecure
CACertDir 172.25.135.174:2351
CACertEP uid=CA Manager,ou=ocsp,dc=clearcase,dc=com
ResponderCertDir 172.25.135.174:2351
ResponderCertEP uid=Responder Manager,ou=ocsp,dc=clearcase,dc=com
ResponderCertAttr cacertificate
ResponderLocation ocsp.openvalidation.org:80
IgnoreNonceExtension YES
]

If the IgnoreNonceExtension attribute does not exist in the smocsp.conf file, then the Nonce extension remains enabled in the OCSP request, which is the default.

Java 1.4-based Policy Server User Interface Can Display All Agents (34410)

The Java 1.4-based Policy Server User Interface can now display larger number of Web Agents (for example, over 20) in an Agent group. Previously, before this fix, it was unable to display all of the Agents in an Agent group.

Policy Server and Oracle Wire Protocol Driver Issue (34524)

After applying this service pack, the Policy Server's ODBC connections to an Oracle policy store do not hang when using the Oracle wire protocol driver.

Active Directory User No Longer Generates Policy Errors (34636, 34125)

The Policy Server no longer generate errors when a user from an Active Directory user store changes their password on next login using the Active Directory console.

Error Messages in LDAP Policy Store Log Files (34643, 34212)

When the Policy Server encounters error messages while performing policy store searches in Active Directory, these messages now contain the correct LDAP error code. Previously, before this fix, these error codes were incorrect.

Policy Server Correctly Rolls Over Dynamic Agent Keys (34644, 34292)

If you set dynamic Agent keys to rollover either once or several times a day using the Set Rollover Frequency dialog box, the Policy Server did not rollover keys as configured. Now, the Policy Server correctly rolls over keys during the selected hour.

Policy Server Error Message When Using Replicated Policy Stores (34755, 34058)

In a Policy Server environment that contained several replicated LDAP policy stores, the Policy Server issued an incorrect "Object not found" error message instead of a "Your session may have timed out" message when it experienced a delay in propagation of newly created objects across the policy stores. In this service pack, this issue is fixed.

SNMP Traps Show the Community for Events in snmptrap.conf File (34795, 34251)

SNMP traps now show the community for the event set in the snmptrap.conf file.

This service pack includes an updated snmptrap.conf file. Before installing this service pack, back up and save the original snmptrap.conf file, which is located in <siteminder_installation>\config. This allows you to preserve any custom changes that you made to this file.

Policy Server and Active Directory Policy Store Errors (35194, 34319)

The Policy Server no longer shuts down when LDAP errors are encountered during a search in an Active Directory policy store.

However, the Policy Server does shut down if it encounters:

- an ADMINLIMIT_EXCEEDED or SIZELIMIT_EXCEEDED error
- a problem creating or parsing sorting and paging controls, which are essential in performing Active Directory-based searches.

Enhancements to JVMOptions.txt File (35251, 34632)

The JVMOptions.txt (located in <siteminder_installation>\config) initialization file now supports up to 63 options and can handle values that are up to 8K in size for each option.

Mapped User's Attribute in a SAML Assertion (29622)

This service pack includes a SAML assertion plugin solution that allows you to put a mapped user's attribute into a SAML assertion by allowing the Policy Server to obtain an arbitrary user's properties using the user directory's UserContext.GetDnProp().

Password Policy Fix (34086)

When the Policy Server is using an LDAP user directory, the Policy Server's password policy did not work properly if the user directory contained multiple users with the same user ID under different organizational units. Users are now redirected to the correct Web page if the number of failed login attempts exceeds the number specified in the password policy. Previously, users would get redirected to an error page.

Password Services Handling Account Lockout Fix (34176)

In the Policy Server's Password Services feature, this service pack fixes an error in handling account lockout due to the incorrect number of passwords being exceeded in a password policy.

Previously, if the password policy specified the account to be re-enabled after the lockout delay, users (who exceeded the maximum number of incorrect password attempts) would be incorrectly redirected to the "password expired" page if they again supplied an incorrect password in their first login attempt after the lockout time had passed.

Now, users are allowed to configure a number of bad password attempts immediately after the lockout time has expired.

Deleting a Rule Caused Policy Server to Fail (34673)

When running under heavy load, the Policy Server does no longer fails after you delete a rule using the Policy Server User Interface.

Ignoring pwdLastSet Attribute in Active Directory Global Catalog Support (35293)

The Policy Server's user store supports the Global Catalog Support feature in Active Directory. If you are using Active Directory Global Catalog Support, you can ignore the pwdLastSet attribute by doing the following:

Windows systems

1. From the Windows Start menu, select Run.
2. Enter regedit in the Run dialog box and click OK.
3. In the Registry Editor, navigate to:

   \HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Ds\LDAPProvider
4. Add the IgnoreADPwdLastSet REG_DWORD registry key and set to a non-zero value to ignore the pwdLastSet attribute.

UNIX systems

1. Navigate to <install dir>/siteminder/registry
2. Open sm.registry in a text editor.
3. Locate the following text in the file:

   \HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Ds\LDAPProvider
4. Locate the line that follows the line from step 3 and create the IgnoreADPwdLastSet REG_DWORD registry key.
5. Set the value to a non-zero value to ignore the pwdLastSet attribute.

IdentityMinder 6.0 Environments and Roles in the Policy Server User Interface (35381)

The 6.0 Policy Server now supports IdentityMinder 6.0 environment and role objects in the Policy Server User Interface.

Password Services Password Data Written to User Directory Fix (35693, 35436)

In the Policy Server's Password Services feature, this service pack fixes an error in password policy processing that caused password data to be written to the user directory when you set the password policy to disable login tracking.

After this fix, only certain exception conditions cause a write of the password data when you have login tracking disabled.

smobjimport/smobjexport Support IdentityMinder 6.0 Objects (35596) (35380)

The smobjimport and smobjexport utilities now support IdentityMinder 6.0 objects. To distinguish between IdentityMinder 5.6 and 6.0 objects, the following arguments have been added to smobjimport/smobjexport to use with the existing IdentityMinder arguments:

-im5

Used with -i, -j, -m to export IdentityMinder version 5 objects only.

-im6

Used with -i, -j, -m to export IdentityMinder version 6 objects only.

-m5

Used with -m to import IdentityMinder version 5 objects only.

-m6

Used with -m to import IdentityMinder version 6 objects only.

Affiliates Now Displayed for FederationWSCustomUserStore User Store (35412)

After applying this service pack to a Policy Server with the Option Pack installed, the Policy Server User Interface now correctly displays the affiliate objects associated with the FederationWSCustomUserStore user store. Previously, viewing the contents of the FederationWSCustomUserStore user store caused a session timeout. Further, if no affiliates exist, the user interface displays an Error 60 message.

Administrators From External User Directories Importing/Exporting Policy Store Data (36126, 35305)

Administrators, with system-level permissions, created in external user directories can now import and export policy store data using smobjimport or smobjexport if they supply the appropriate SiteMinder administrator credentials during import or export.

smobjexport Exports Specific Policy Domain Objects (36174, 35192)

The smobjexport utility now exports specific policy domain objects using the -e option if:

- any of the realms contain an AuthAzMap object.
- one of the user directories in the AuthAzMap object has an applicable PasswordPolicy.

Previously, before this fix, smobjexport would issue a bus error during export if the criteria from the list above was met.

Deleting Rule No Longer Causes the Policy Server to Fail (35957)

The Policy Server no longer fails when you delete a rule that is also accessed by a client application.

Policy Server Supports 5.2 SunOne LDAP Directory Server as a Policy Store (36133)

The Policy Server now supports a 5.2 SunOne LDAP Directory Server as a policy store. Previously, the smldapsetup utility would issue errors if you tried to import SiteMinder schema into a 5.2 SunOne LDAP Directory Server.

Improvement to Policy Store Type Identification (36747)

The Policy Server now performs optimal policy store type identification during startup or failover when using policy stores that reside in LDAP Directory Servers.

Agent API Supports 1024 File Descriptors on Solaris (36235) (34972)

On Solaris, the Agent API has been modified to accommodate environments that utilize more than 1024 file descriptors concurrently.

Policy Server Correctly Reconnects to Oracle Policy Store (36753,36425)

The Policy Server now reconnects correctly to an Oracle policy store when using the Oracle Wire protocol driver to communicate with an Oracle server that has been restarted due to a backup of the server.

Update to Policy Management API for Scripting Interface for Perl (36934, 36378)

The Policy Management API has been corrected to return a list of Agents from the policy store to the Scripting Interface for Perl regardless of Agent type or the correlation of the Agent's name to a trusted host.

Password Services and Users' Accounts Disabled Issue Fixed (37217, 36997, 37271)

On the SiteMinder Password Policy Dialog's Expiration tab in the Policy Server User Interface, if you configured a password policy to have the Policy Server disable users' accounts after three wrong login attempts and also selected the re-enable account option with the number of minutes left blank, users are disabled as expected. Previously, users accounts were enabled if they entered an invalid password a fourth time.

You access the SiteMinder Password Policy Dialog by selecting Edit > System Configuration > Create Password Policy.

In addition, the users' accounts remain disabled until they are re-enabled by an administrator.

Scripting Interface Can Import/Export Agent Configuration and Host Configuration Objects (37226, 36255)

You can now import or export Agent Configuration and Host Configuration Objects using the Scripting Interface for Perl. Before this fix, you were unable to do this.

Sm_Api_Version_V4_1 and Sm_Api_Version_V4 Not Supported (36275, 37239)

The API version constants Sm_Api_Version_V4_1 and Sm_Api_Version_V4 are not supported as documented in the *Developer's Guide for C*. These constants are intended for internal use only and you should use Sm_Api_Version_V3.

Update to Java DMS API Method (36234)

The Java DMS API method to modify a user's password now returns the correct status and reason code if you supply invalid credentials in the method call.

Policy Server Fix to Protect Resources Processed Against Blank Realms (36626)

The Policy Server is updated to make sure that resources processed against blank realms, which have rules defined in the realm, are protected.

Policy Server Fix Returns Correct Redirect Messages From Authentication Attempts (36925)

The Policy Server now correctly returns any user, error, and redirect messages from authentication attempts in domains that use multiple user directories.

Policy Server Processing Responses Improvement (37269, 36342)

The Policy Server now processes responses during a OnAccessReject action even if the Authorization user directory, which is configured in the Auth-AZ mapping, is not available.

The responses returned on an OnAccessReject action is limited to user class "ALL" when the Authorization user directory is not available.

IdentityMinder 5.6 Environment Objects Not Displaying in the Policy Server User Interface (37745, 37296)

The Policy Server now properly displays IdentityMinder 5.6 environment object trees in the Policy Server User Interface. After applying Policy Server v6.0 SP1 CR003, CR004, CR005, or CR006, IdentityMinder objects would not appear in the Policy Server User Interface. Now, this issue is fixed.

IdentityMinder 6.0 Environment Objects Not Displaying in the Policy Server User Interface (37743, 37469)

When the Policy Server is using an LDAP-based policy store, the Policy Server User Interface now displays IdentityMinder 6.0 environment objects. Previously, before this fix, these objects did not appear in the Policy Server User Interface.

IdentityMinder 5.6 and Policy Evaluation for RBAC Policies (37744) (37536)

Policy evaluation for role-based policies (RBAC) has been fixed for IdentityMinder 5.6 deployments.

Active expressions Fix (37517)

Active expressions using variable names containing character combinations including strings such as null, false, and true are correctly parsed.

Date Range Increased for Certificates Requiring OCSP Validation (37625, 37024)

The Policy Server now handles certificates requiring OCSP validation when the maximum year in the date range contains a year greater than 2038.

Policy Server Optimizes Cache Updates When Creating New Web Agents (37702, 37282)

The Policy Server has been fixed to optimize cache updates during creation of new Web Agents. The existing Agent groups are no longer removed from the policy store cache when you create new Agents.

Policy Server User Interface Certificate Mapping Update (37705, 37139)

The Policy Server User Interface now allows certificate mapping updates to be saved to the policy store if you enable the "Take from Certificate Extension" and perform CRL checking options.

Trace Logs and SQL_ATTR_QUERY_TIMEOUT Connection Attribute (37206)

The Policy Server trace logs do not contain any error messages pertaining to setting the SQL_ATTR_QUERY_TIMEOUT database connection attribute due to lack of support for this option in the driver used for the connection. In this service pack, this issue is fixed.

Race Conditions in Update of Policy Objects (37567)

The Policy Server can now accommodate any race conditions in the update of policy objects in a distributed configuration containing replicated policy stores. The Policy Server also returns an appropriate error response to requests made when the cache rebuild has failed in the Policy Server.

Policy Server Removal of Idle Agent Connections (37568)

The Policy Server has been fixed to ensure proper removal of idle Agent connections under certain load conditions.

Policy Server Logs Updated (37569, 38100)

The Policy Server logs contain correct error messages pertaining to the Policy Server accessing invalid or deleted realms under certain load conditions.

Policy Server Return Correct Reason Codes from Custom Authentication Schemes (37718)

The Policy Server has been fixed to return the correct reason code from custom authentication schemes when a password policy is enabled for that scheme.

Policy Server logs Updated for UserAz Cache (37993)

The Policy Server logs now contain correct messages pertaining to the state of the UserAz cache.

Policy Server Errors When Using ADAM Policy Store (38008)

During startup, the Policy Server no longer generates exceeding size limits errors for ADAM-based policy stores.

Policy Server Fires Rules Ending With a Wildcard (38181)

The Policy Server has been updated to accommodate the firing of rules in unprotected realms when the rule ends with a wildcard (*) character.

Policy Server Realms and Dependent Policy Objects Update (38409)

The Policy Server has been updated to make sure that realms and dependent policy objects are correctly updated in a distributed configuration that contains replicated policy stores.

Policy Server Returns Correct SMAUTHREASON Code (38803, 38411)

The Policy Server is fixed to accommodate the return of the correct SMAUTHREASON code upon user initiated password changes when a user is disabled and password services is enabled.

Updated to Java-based API Method AgentApi.init() (38813)

The Java-based API method AgentApi.init() is corrected to accommodate conditions when a null ServerDef object is added to an InitDef object that is used as a parameter to the init() method.

User Names Cannot Contain Parenthesis () (38963, 38923, 38707)

The Policy Server no longer permits users to log in with a user name that contains parenthesis (). For example, the Policy Server does not accept user names such as (Robm) or (Lisap). The Policy Server notes these login attempts as failures and puts a 'Username may not be enclosed within parenthesis: Can't proceed' error message in the authentication log file.

Fix for X.509 Certificates Larger Than 4096 Bytes (39366, 39051)

The Policy Server has been fixed so that X.509 certificate authentication works properly for certificates larger than 4096 bytes. This fix increases the limit for certificate binaries from 4096 to 8192 bytes and DNs from 1000 to 2000 bytes.

Policy Server and Shared Secret Rollover Configuration (39367, 38403)

The Policy Server User Interface now shows the saved Shared Secret Rollover configuration correctly. Before this fix, if you selected the Rollover Shared Secret every radio button in the Shared Secret Rollover tab on the SiteMinder Key Management dialog and specified a rollover period, the period value would change to zero after you saved the configuration.

SM_USERIMPERSONATORDIRNAME User Attribute HTTP Header Response Issue (39368, 39004)

The Policy Server now sets the SM_USERIMPERSONATORDIRNAME user attribute as an HTTP header response.

Policy Server No Longer Malforms the IssuerDN (39369, 39008)

For certificate mapping, if any attributes in the IssuerDN contain a comma, the Policy Server now properly reverses the IssuerDN. Before this fix, the Policy Server would malform the IssuerDN.

Defects Fixed for 6.0 SP1

Release 6.0 SP1 contains the following fixes:

1000 Entry Limit on Retrievals from Active Directory Policy Stores Removed (28006, 27667)

When configured to use an Active Directory policy store, the Policy Server can now successfully retrieve more than 1000 entries for any particular object.

IP Address Lookup While Configuring Agents 19100(15210)

When creating an Agent in the Policy Server User Interface, performing a valid IP address lookup will no longer result in a DNS lookup error.

Error 81 When Authenticating Against Active Directory Over SSL Using Enhanced LDAP Referrals (27945, 27544)

With the Policy Server configured to use enhanced referrals with Active Directory over SSL it will now correctly authenticate a user in the event of a connection timing out. Prior to this, error 81 was being returned to the authentication log.

List of Directories in the Manage User Dialog Incomplete (27892, 27678, 27875)

In the Policy Server User Interface, the Manage Users dialog box (Tools > Manage Users) contains a User Directory drop down list. This list now displays all user directories.

Problem Changing a Password Through Password Services When Agent and Policy Server Clocks are not Synchronized (27944, 27727)

In the event that password services is being used with an Agent that is communicating with two Policy Servers in round robin load balancing and the Policy Server clocks are out of synchronization, a new registry setting has been provided to ensure a user password can be successfully changed.

In the event that Policy Servers are running with different clock settings, create a registry entry:

ServerCommandTimeDelay (DWORD format)

under the

Hkey_localmachine\Software\Netegrity\SiteMinder\CurrentVersion\ObjectStore\

and set the value to the number of seconds that represents the time difference between the two Policy Servers.

Policy Server Cannot Make a Distribution Point Request to a PKI Certificate Authority (27974, 27599)

The Policy Server has been fixed to correctly retrieve distribution points from a certificate and thus can correctly make a formal Distribution Point request to the PKI Certificate Authority.

Supported formats are:

- URL - ldap://<server-name>:<port_number>/<DN-of-Entity containing the CRL>

  Example:

  [1] CRL Distribution Point
  Distribution Point Name:
  Full Name:
  URL=ldap://server.company.com:8080/uid=Certificate Manager,ou=people,dc=netegrity,dc=com

- Directory Address - <DN-of-Entity containing the CRL>

  Example:

  [1] CRL Distribution Point
  Distribution Point Name:
  Full Name:
  Directory Address: uid=Certificate Manager,ou=people,dc=netegrity,dc=com

Additional notes on supported formats:

- When using the URL format, the server name and port contained in the URL has to exist in the list of configured user directories in the Policy Server. This is because the Policy Server needs credentials to access this user store when searching for the CRL attribute. Thus the directory server configured in the Certificate Mapping dialog box is not used.
- When using the Directory Address format, the Policy Server uses the info obtained from the distribution point string as an entry point for searching the directory server configured in the Certificate Mapping dialog box.

- When there are multiple distribution points in the certificate, the first Directory Address formatted distribution point gets used. Similarly when there are no Directory Address formatted distribution points, the first URL formatted distribution point gets used.

Erroneous Log Message for Asynchronous Calls Registry Setting (27998, 27893)

There was an error when the following registry value was set to 1:

Netegrity\SiteMinder\CurrentVersion\Database\AsynchronousCalls

The message written to the Policy Server logs has been fixed to indicate asynchronous database calls have been enabled.

Policy Management API Case-sensitivity (25113, 24697)

The policy management API login function has been updated to be case-insensitive.

LDAP Search Scope for CRL Retrieval (28202, 28090)

The scope of the LDAP search performed by the Policy Server for retrieving CRLs is now always scope base. Prior to this it was dependent on the user setting specified for the directory.

Error with Form Post Variables for Non-Option Pack Agents (28408, 28210)

The Policy Server will no longer go into an infinite loop if a form post variable is triggered by a Web Agent that does not have the Web Agent Option Pack installed.

-hc parameter Added to Usage Statement for smreghost (28492, 28307)

The usage statement for smreghost has been updated to include the required "-hc" parameter.

Perl Scripting Interface Allows Imports of Multiple Policies (28577, 28141)

The Scripting Interface for Perl has been fixed to import multiple policies.

Perl Scripting Interface Correctly Exports Trusted Host Objects (28580, 28145)

The Scripting Interface for Perl now correctly exports a trusted host object.

getAttribute and copyAttribute Methods Are Now Case Insensitive (27929, 27402)

The getAttribute and copyAttribute methods of the SDK's DMS API have been updated to be case-insensitive and as such now conform to RFC 2252.

smobjexport Now Correctly Handles Nested Realms (28572)

Searches for Realms are now correctly formulated against an LDAP store in order for SmObjExport to export nested realms correctly.

Global Rules Can Be Configured with Agent Groups (28865)

Global rules can now be configured with Agent groups.

OneView Monitor Correctly Displays Details Page (28910)

The OneView monitor has been fixed to display the 'Details' page correctly.

Policy Server Shuts Down Cleanly if Attempting to Connect to a Policy Store with IdentityMinder Objects (28700)

A Policy Server to be used with IdentityMinder requires Policy Server Extensions for IdentityMinder. Once the extensions have been installed, the Policy Server can connect to a Policy Store that includes IdentityMinder objects.

Prior to this fix the Policy Server would fail if it attempted to read a policy store that contained IdentityMinder objects. Now the Policy Server has been fixed so that if extensions are not installed, it will shutdown cleanly.

Impersonators and Impersonatees Can Exist in Different User Directories (29177)

The SiteMinder 6.0 Impersonation facility has been fixed such that Impersonator and Impersonatee can exist in different user directories.

Certificate Map Test Dialog Box Shows All Directories (29106)

The Policy Server User Interface has been fixed to correctly show all the LDAP directories from the directory drop-down list on the Certificate Map Test dialog box.

Accounting Service No Longer Consumes CPU (29621, 29528)

The accounting service has been fixed so that it will no longer spin and consume CPU time.

Trailing Spaces Removed from Responses with SQL Server Data (29367, 29008)

The Policy Server has been updated to ensure that any responses containing user attributes from a SQL Server user store are properly right-trimmed to remove trailing spaces. This ensures that the response to the client is also correctly formatted.

Policy Server Supports Active Directory 2003 Policy Stores (29320, 28820)

The Policy Server has been fixed to work with Active Directory 2003-based policy stores.

Policy Server Option Pack Correctly Parses Dates (29443)

The Policy Server Option Pack has been updated to correctly parse dates in SAML assertions when millisecond values are not present.

Terminating an Administration Session No Longer Conflicts with Other Administration Sessions (29401, 29052)

The administration server has been updated so that it will not fail when two sessions are connected to it and one of the two ends its session.

smobjexport -e Correctly Exports Password Policies (29924, 29577)

When using smobjexport with the -e option, password policies associated with a user directory of the domain are correctly exported.

Modified Response Attributes Maintain OID (29925, 29529)

Response attributes modified via the Policy Server User Interface are no longer saved with a new OID.

Policy Server Correctly Responds to ACE Server Failover (29995, 29793)

The Policy Server has been updated to correctly failover from one ACE server to another in the event of an ACE server failure.

Policy Server Behavior if an Oracle Policy Store is Not Available (29750, 29559)

The Policy Server will shut down or fail to start (and then attempt to restart) if the policy store (Oracle) is not available. This is to ensure all policy information has been completely and correctly read before managing access to resources.

Policy Server Correctly Handles CRL Distribution Points When Connected to the Secure Proxy Server (29523, 29221)

The Policy Server has been updated to correctly accommodate receipt and processing of CRL distribution point information from certificates handled by the Secure Proxy Server platform for certificate-based authentication.

Members of Dynamic Groups Can Be Authorized with a Scope of One (29939, 29361)

Users who are members of a dynamic LDAP group can now be authorized when the member URL has a scope of one.

getDomainObject and getObject API Functions Handle Mismatched Parameters (27366, 27145)

The Policy Server has been updated to gracefully handle the policy API functions getDomainObject() and getObject() being passed mismatched parameters.

Policy Server Option Pack Now Allows Rules to be Added to Custom Agent Types (30297, 29850)

The Policy Server has been updated so that if the Policy Server Option Pack is installed rules can continue to be added to a rule group that is configured with a custom Agent type.

Global Policies Now Function Correctly with Agent Groups (29942)

Global policies will now correctly fire for domain realms that use Agent groups and for global rules that use Agent groups.

Password Services Redirect Behavior with Active Directory (30273)

A User disabled (or password change required) in Active Directory will be redirected properly to the Password Services page when the User Directory is configured with the "AD" namespace.

IdentityMinder Domain Show/Hide Option (30016)

The Policy Server User Interface option to hide IdentityMinder Domains no longer hides non-IdentityMinder domains.

Safeword with HTML Forms Authentication Support for Multiple Authenticators (30299, 29532)

The Safeword HTML forms Auth Scheme has been updated to support multiple Safeword authenticators. This fix requires Web Agent 5QMR6 HF-004 OR 6.0 HF-005 or later.

Logging of Password Change Failures with Active Directory User Stores (30600, 30101)

When a password change fails because it is rejected by Active Directory, "****" is be written in the logs instead of the new password.

OnAuthReject Responses for ACE Users in Next Token Mode or New Pin Mode (30561, 30063)

When using ACE authentication, the Policy Server will no longer fire the standard OnAuthReject responses for the users in Next Token Mode or New Pin Mode.

Null Value Handling for Required Parameters Using the JAVA API SDK Methods (30563, 29582)

In the event that a Java Agent API SDK method receives a null value for a required parameter it will now return an error. Previously it would cause the JVM to fail.

Improved User Cache Flush Handling (29690, 28909)

The Policy Server's user authorization cache has been updated to support improved flush user functionality. As a result IdentityMinder role assignment changes will be immediately reflected in the IdentityMinder user console.

Policy Server User Interface Searches (30589, 30417)

When performing searches in the Policy Server User Interface, searches using strings with characters such as "*(" will no longer cause the administration server to shut down.

Configuring a Time Delay for Rebinding Attempts in LDAP Directories (30640, 30534, 30647)

When the Policy Server is using Active Directory as a user store over LDAP (using the AD namespace), the LDAP connections are frequently "Marked Close Pending". The Policy Server thread or ping server thread waits or sleeps for 5 seconds after a connection is Marked Close Pending and attempting to bind a new connection.

Users can configure a new registry setting 'BindLDAPServerDelay' in seconds to determine the amount of delay required before attempting to rebind to an LDAP server.

To set this registry value

Windows

1. From the Windows Start menu, select Run.
2. Enter regedit in the Run dialog box and click OK.
3. In the Registry Editor, navigate to:

   \HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Ds\LDAPProvider
4. Create or modify the following BindLDAPServerDelay registry key and set the value that you want in seconds. The key must be of the type REG_DWORD.

Note: If you do not manually configure this setting on the machine where the Policy Server.

UNIX

1. Navigate to <install dir>/siteminder/registry
2. Open sm.registry in a text editor.
3. Locate the following text in the file:

   \HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Ds\LDAPProvider
4. Locate the line that follows the line from step 3 and begins with:

   BindLDAPServerDelay
5. Create or modify the following BindLDAPServerDelay registry key and set the value that you want in seconds.

Note: If you do not manually configure this setting on the machine where the Policy Server installed, then the Policy Server waits for 5 seconds, the default value.

Executing Java Active Expressions (30836)

The activeExpression.properties file is now included in the config\properties subdirectory of the Policy Server installation directory to accommodate execution of Java ActiveExpressions through the Java Authorization API.

Configuring a Time Delay for Cleanup of Connections Marked as "Closed Pending" (30839, 30838)

Users can create a new registry setting, DeadHandleListLiveTime, to configure the number of minutes that must elapse before LDAP connections marked Closed Pending will be cleaned up.

The value should be created in the following key:

HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Ds\LDAPProvider

It should be named DeadHandleListLiveTime and be of type REG_DWORD.

When this registry key is not found (recommended), a default of 10 minutes will be used. When this registry key is found and has a value of less than 1 minute, a default of 1 minute will be used.

Using the getAgentTypeAttr Function to Obtain the Agent Type Name (30909, 30336)

The Agent Type Attribute Name can be obtained if the Agent Type Attribute OID is known by using the newly added getAgentTypeAttr() function in the Java Policy API.

The sample code for this would be:

```
SmResponseAttr responseAttr = (SmResponseAttr) responseAttrs.get(i);
String agentTypeAttrOid = responseAttr.getAgentTypeAttr();
System.out.println( "Agent Type Attribute OID = " +  agentTypeAttrOid);
SmAgentTypeAttr agentattr = new SmAgentTypeAttr();
result = policyApi.getAgentTypeAttr(agentTypeAttrOid.getOidString(),
agentattr);
System.out.println( "Agent Type Attribute Name = " +  agentattr.getName());
```

UpdateAttributes Agent Call Recalculates Active Response Values (30912, 30213)

The UpdateAttributes call by the Agent will now recalculate active responses that originally had no data.

smobjexport -s No Longer Exports IdentityMinder Environments (30936, 30358)

IdentityMinder Environments are no longer exported when using the smobjexport utility to export a domain with the -s option.

smldapsetup Passing Large Policy Store Name Values (30963, 30572)

The smldapsetup utility no longer fails on passing large values for LDAP policy store server names.

Modifying Agent Configuration Objects with the PERL CLI (30969, 30554)

The PERL CLI no longer fails on modifying an association with a large value of AgentConfigObjects.

Processing Search Filters for DNs with Spaces Following Commas (30993, 30850)

SiteMinder will process valid search filters with DNs containing spaces after the comma character without reporting any errors.

Policy Server and Servlet Exec on Red Hat Enterprise Linux Advanced Server with Apache 1.3.28 (28444, 29045)

On Red Hat AS, the Policy Server and Servlet Exec are now functional with Apache Web Server v1.3.28.

Additional Components for TransactionMinder in the Profiler (30083, 30197)

If you have installed TransactionMinder, the following components are now available for the Profiler:

- TXM
- JNI
- License
- MetaData

To access the Profiler, go to the Profile Tab of the Policy Server Management Console. For information about using the Profiler, see the *Policy Server Management* document.

Chapter 10: International Support

An *internationalized* product is an English product that runs correctly on local language versions of the required operating system and required third-party products, and supports local language data for input and output. Internationalized products also support the ability to specify local language conventions for date, time, currency and number formats.

A *translated* product (sometimes referred to as a *localized* product) is an internationalized product that includes local language support for the product's user interface, online help and other documentation, as well as local language default settings for date, time, currency, and number formats.

In addition to the English release of this product, CA supports *only* those languages listed in the following table.

Language	Internationalized	Translated
Brazilian-Portuguese	No	No
Chinese (Simplified)	Yes	No
Chinese (Traditional)	No	No
Czech	Yes	No
Danish	Yes	No
Dutch	Yes	No
Finnish	Yes	No
French	Yes	No
German	Yes	No
Greek	Yes	No
Hungarian	Yes	No
Italian	Yes	No
Japanese	Yes	No
Korean	Yes	No
Norwegian	Yes	No
Polish	Yes	No
Russian	Yes	No

Language	Internationalized	Translated
Spanish	Yes	No
Swedish	Yes	No
Turkish	Yes	No

Note: If you run the product in a language environment *not* listed in the table, you may experience problems.

Chapter 11: Documentation

This section contains the following topics:

SiteMinder Bookshelf

You can find complete information about SiteMinder by installing the SiteMinder bookshelf. The SiteMinder bookshelf lets you:

- Use a single console to view all documents published for SiteMinder.
- Use a single alphabetical index to find a topic in any document.
- Search all documents for one or more words.

SiteMinder product documentation is installed separately. We recommend that you install the documentation before beginning the installation process.

Documentation installation programs are available for download from the CA Technical Support site.

Readme Documentation

The information previously available in the Policy Server Readme, Web Agent Readme, SAML Affiliate Agent Readme, and the Option Pack Readme is now available in the Policy Server Release Notes, the Web Agent Release Notes, the SAML Affiliate Agent Release Notes, and the Federation Security Services Release Notes.

Option Pack Readme

The *Option Pack Readme* no longer exists. The *Policy Server and Web Agent Option Pack Guide* contains installation information and specifies the features that require Option Pack installation. The *Federation Security Services Release Notes* contain the known issues and defects fixed information previously available in the *Option Pack Readme*.

Release Numbers on Documentation

The release number on the title page of a document might not correspond to the current product release number; however, all documentation delivered with the product, regardless of release number on the title page, will support your use of the current product release.

The release number changes only when a significant portion of a document changes to support a new or updated product release. If no substantive changes are made to a document, the release number does not change. For example, a document for r12 may still be valid for r12 SP1. Documentation bookshelves always reflect the current product release number.

Occasionally, we must update documentation outside of a new or updated release. To indicate a minor change to the documentation that does not invalidate it for any releases that it supports, we update the edition number on the cover page. First editions do not have an edition number.

Chapter 12: Contact Technical Support

For online technical assistance and a complete list of locations, primary service hours, and telephone numbers, contact Technical Support at http://ca.com/support.

Appendix A: Third-Party Acknowledgements

This section contains the following topics:

Apache

Portions of this product include software developed by the Apache Software Foundation:

- Apache SOAP
- Apache Xalan-J
- Apache Xerces-C
- Apache Xerces-J
- Apache XML Security Java

The Apache software is distributed in accordance with the following license agreement.

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

RSA

This product includes code licensed from RSA Data Security.

Portions of this product include the following products licensed by RSA, the Security Division of EMC:

- BSAFE Cert-C
- BSAFE Cert-J
- BSAFE Crypto-C
- BSAFE SSL-J

Rhino

The source code version of Rhino 1.5 Release 4.1 is licensed under the Netscape Public License Version 1.1 which can be found at http://www.mozilla.org/NPL/ and is made available for download from http://opensrcd.ca.com/ips/3039_8/

AMENDMENTS

The Netscape Public License Version 1.1 ("NPL") consists of the Mozilla Public License Version 1.1 with the following Amendments, including Exhibit A-Netscape Public License. Files identified with "Exhibit A-Netscape Public License" are governed by the Netscape Public License Version 1.1.

Additional Terms applicable to the Netscape Public License.

I. Effect.

These additional terms described in this Netscape Public License -- Amendments shall apply to the Mozilla Communicator client code and to all Covered Code under this License.

II. "Netscape's Branded Code" means Covered Code that Netscape distributes and/or permits others to distribute under one or more trademark(s) which are controlled by Netscape but which are not licensed for use under this License.

III. Netscape and logo.

This License does not grant any rights to use the trademarks "Netscape", the "Netscape N and horizon" logo or the "Netscape lighthouse" logo, "Netcenter", "Gecko", "Java" or "JavaScript", "Smart Browsing" even if such marks are included in the Original Code or Modifications.

IV. Inability to Comply Due to Contractual Obligation.

Prior to licensing the Original Code under this License, Netscape has licensed third party code for use in Netscape's Branded Code. To the extent that Netscape is limited contractually from making such third party code available under this License, Netscape may choose to reintegrate such code into Covered Code without being required to distribute such code in Source Code form, even if such code would otherwise be considered "Modifications" under this License.

V. Use of Modifications and Covered Code by Initial Developer.

V.1. In General.

The obligations of Section 3 apply to Netscape, except to the extent specified in this Amendment, Section V.2 and V.3.

V.2. Other Products.

Netscape may include Covered Code in products other than the Netscape's Branded Code which are released by Netscape during the two (2) years following the release date of the Original Code, without such additional products becoming subject to the terms of this License, and may license such additional products on different terms from those contained in this License.

V.3. Alternative Licensing.

Netscape may license the Source Code of Netscape's Branded Code, including Modifications incorporated therein, without such Netscape Branded Code becoming subject to the terms of this License, and may license such Netscape Branded Code on different terms from those contained in this License.

VI. Litigation.

Notwithstanding the limitations of Section 11 above, the provisions regarding litigation in Section 11(a), (b) and (c) of the License shall apply to all disputes relating to this License.

EXHIBIT A-Netscape Public License.

"The contents of this file are subject to the Netscape Public License Version 1.1 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.mozilla.org/NPL/

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.

The Original Code is Mozilla Communicator client code, released March 31, 1998.

The Initial Developer of the Original Code is Netscape Communications Corporation. Portions created by Netscape are Copyright (C) 1998-1999 Netscape Communications Corporation. All Rights Reserved.

Contributor(s): _____.

Alternatively, the contents of this file may be used under the terms of the _____ license (the "[___] License"), in which case the provisions of [_____] License are applicable instead of those above. If you wish to allow use of your version of this file only under the terms of the [_____] License and not to allow others to use your version of this file under the NPL, indicate your decision by deleting the provisions above and replace them with the notice and other provisions required by the [___] License. If you do not delete the provisions above, a recipient may use your version of this file under either the NPL or the [___] License."

MOZILLA PUBLIC LICENSE

Version 1.1

---

1. Definitions.

1.0.1. "Commercial Use" means distribution or otherwise making the Covered Code available to a third party.

1.1. "Contributor" means each entity that creates or contributes to the creation of Modifications.

1.2. "Contributor Version" means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3. "Covered Code" means the Original Code or Modifications or the combination of the Original Code and Modifications, in each case including portions thereof.

1.4. "Electronic Distribution Mechanism" means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. "Executable" means Covered Code in any form other than Source Code.

1.6. "Initial Developer" means the individual or entity identified as the Initial Developer in the Source Code notice required by Exhibit A.

1.7. "Larger Work" means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1.8. "License" means this document.

1.8.1. "Licensable" means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. "Modifications" means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

A. Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.

B. Any new file that contains any part of the Original Code or previous Modifications.

1.10. "Original Code" means Source Code of computer software code which is described in the Source Code notice required by Exhibit A as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.10.1. "Patent Claims" means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.11. "Source Code" means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. "You" (or "Your") means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. Source Code License.

2.1. The Initial Developer Grant.

The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims:

(a) under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and

(b) under Patents Claims infringed by the making, using or selling of Original Code, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Code (or portions thereof).

(c) the licenses granted in this Section 2.1(a) and (b) are effective on the date Initial Developer first distributes Original Code under the terms of this License.

(d) Notwithstanding Section 2.1(b) above, no patent license is granted: 1) for code that You delete from the Original Code; 2) separate from the Original Code; or 3) for infringements caused by: i) the modification of the Original Code or ii) the combination of the Original Code with other software or devices.

2.2. Contributor Grant.

Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license

(a) under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and

(b) under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: 1) Modifications made by that Contributor (or portions thereof); and 2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).

(c) the licenses granted in Sections 2.2(a) and 2.2(b) are effective on the date Contributor first makes Commercial Use of the Covered Code.

(d) Notwithstanding Section 2.2(b) above, no patent license is granted: 1) for any code that Contributor has deleted from the Contributor Version; 2) separate from the Contributor Version; 3) for infringements caused by: i) third party modifications of Contributor Version or ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or 4) under Patent Claims infringed by Covered Code in the absence of Modifications made by that Contributor.

3. Distribution Obligations.

3.1. Application of License.

The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section 2.2. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section 6.1, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section 3.5.

3.2. Availability of Source Code.

Any Modification which You create or to which You contribute must be made available in Source Code form under the terms of this License either on the same media as an Executable version or via an accepted Electronic Distribution Mechanism to anyone to whom you made an Executable version available; and if made available via Electronic Distribution Mechanism, must remain available for at least twelve (12) months after the date it initially became available, or at least six (6) months after a subsequent version of that particular Modification has been made available to such recipients. You are responsible for ensuring that the Source Code version remains available even if the Electronic Distribution Mechanism is maintained by a third party.

3.3. Description of Modifications.

You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4. Intellectual Property Matters

(a) Third Party Claims.

If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs.

If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the LEGAL file.

(c) Representations.

Contributor represents that, except as disclosed pursuant to Section 3.4(a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

3.5. Required Notices.

You must duplicate the notice in Exhibit A in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in Exhibit A. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear than any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.6. Distribution of Executable Versions.

You may distribute Covered Code in Executable form only if the requirements of Section 3.1-3.5 have been met for that Covered Code, and if You include a notice stating that the Source Code version of the Covered Code is available under the terms of this License, including a description of how and where You have fulfilled the obligations of Section 3.2. The notice must be conspicuously included in any notice in an Executable version, related documentation or collateral in which You describe recipients' rights relating to the Covered Code. You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

3.7. Larger Works.

You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

4. Inability to Comply Due to Statute or Regulation.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the LEGAL file described in Section 3.4 and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Application of this License.

This License applies to code to which the Initial Developer has attached the notice in Exhibit A and to related Covered Code.

6. Versions of the License.

6.1. New Versions.

Netscape Communications Corporation ("Netscape") may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2. Effect of New Versions.

Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License published by Netscape. No one other than Netscape has the right to modify the terms applicable to Covered Code created under this License.

6.3. Derivative Works.

If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename Your license so that the phrases "Mozilla", "MOZILLAPL", "MOZPL", "Netscape", "MPL", "NPL" or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the Mozilla Public License and Netscape Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in Exhibit A shall not of themselves be deemed to be modifications of this License.)

7. DISCLAIMER OF WARRANTY.

COVERED CODE IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE COVERED CODE IS FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGING. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE COVERED CODE IS WITH YOU. SHOULD ANY COVERED CODE PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL DEVELOPER OR ANY OTHER CONTRIBUTOR) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED CODE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

8. TERMINATION.

8.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2. If You initiate litigation by asserting a patent infringement claim (excluding declatory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You file such action is referred to as "Participant") alleging that:

(a) such Participant's Contributor Version directly or indirectly infringes any patent, then any and all rights granted by such Participant to You under Sections 2.1 and/or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively, unless if within 60 days after receipt of notice You either: (i) agree in writing to pay Participant a mutually agreeable reasonable royalty for Your past and future use of Modifications made by such Participant, or (ii) withdraw Your litigation claim with respect to the Contributor Version against such Participant. If within 60 days of notice, a reasonable royalty and payment arrangement are not mutually agreed upon in writing by the parties or the litigation claim is not withdrawn, the rights granted by Participant to You under Sections 2.1 and/or 2.2 automatically terminate at the expiration of the 60 day notice period specified above.

(b) any software, hardware, or device, other than such Participant's Contributor Version, directly or indirectly infringes any patent, then any rights granted to You by such Participant under Sections 2.1(b) and 2.2(b) are revoked effective as of the date You first made, used, sold, distributed, or had made, Modifications made by that Participant.

8.3. If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2.1 or 2.2 shall be taken into account in determining the amount or value of any payment or license.

8.4. In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

9. LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED CODE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

10. U.S. GOVERNMENT END USERS.

The Covered Code is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Code with only those rights set forth herein.

11. MISCELLANEOUS.

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by California law provisions (except to the extent applicable law, if any, provides otherwise), excluding its conflict-of-law provisions. With respect to disputes in which at least one party is a citizen of, or an entity chartered or registered to do business in the United States of America, any litigation relating to this License shall be subject to the jurisdiction of the Federal Courts of the Northern District of California, with venue lying in Santa Clara County, California, with the losing party responsible for costs, including without limitation, court costs and reasonable attorneys' fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License.

12. RESPONSIBILITY FOR CLAIMS.

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

13. MULTIPLE-LICENSED CODE.

Initial Developer may designate portions of the Covered Code as "Multiple-Licensed". "Multiple-Licensed" means that the Initial Developer permits you to utilize portions of the Covered Code under Your choice of the NPL or the alternative licenses, if any, specified by the Initial Developer in the file described in Exhibit A.

EXHIBIT A -Mozilla Public License.

``The contents of this file are subject to the Mozilla Public License Version 1.1 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.mozilla.org/MPL/

Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF

ANY KIND, either express or implied. See the License for the specific language governing rights and

limitations under the License.

The Original Code is _____.

The Initial Developer of the Original Code is _____. Portions created by

_____ are Copyright (C) _____
_____. All Rights

Reserved.

Contributor(s): _____.

Alternatively, the contents of this file may be used under the terms of the _____ license (the "[___] License"), in which case the provisions of [_____] License are applicable instead of those above. If you wish to allow use of your version of this file only under the terms of the [_____] License and not to allow others to use your version of this file under the MPL, indicate your decision by deleting the provisions above and replace them with the notice and other provisions required by the [___] License. If you do not delete the provisions above, a recipient may use your version of this file under either the MPL or the [___] License."

[NOTE: The text of this Exhibit A may differ slightly from the text of the notices in the Source Code files of the Original Code. You should use the text of this Exhibit A rather than the text found in the Original Code Source Code for Your Modifications.]