Tivoli SecureWay Policy Director
Release Notes

Version 3.7 / 3.7.1

Revised Date: December 31, 2001
Contents

Release Notes - Version 3.7 / 3.7.1 (Revised Date: 31 Dec 2001)

1 General Information .................................................................2
  1.1 Release Notes Revision History ..............................................2
  1.2 Adobe Acrobat Reader, version 4.05 Recommended .....................5
  1.3 Navigating Policy Director PDF Documentation .......................5
  1.4 Policy Director 3.7.1 CD Distribution (30 March 2001) .............6
  1.5 The Policy Director Documentation Set .................................7
  1.6 Revised Documentation Set Available on Support Site ..............8
  1.7 Policy Director Public Software Download Page .....................8
  1.8 Contacting Customer Support ..............................................8
  1.9 Problem Determination Checklist .......................................9

2 Policy Director 3.7.1 Information ...........................................11
  2.1 About Policy Director Version 3.7.1 ....................................11
  2.2 Upgrading from Policy Director 3.7 to 3.7.1 ..........................11
  2.3 New GSKit Package Available for WebSEAL Installations .........11
  2.4 New LDAP 3.2 db2ldif Utility Patch ....................................12
  2.5 Domino Registry Supported by Policy Director .......................12
  2.6 Mounting / Unmounting the Policy Director CD on HP ............13

3 Important Supplemental Information ......................................14
  New Installation Information .....................................................15
  3.1 Configuring DCE to Start Automatically (IY20147) ...................15
  New Base Information ............................................................16
  3.2 Effect of an ACL Modification is Delayed ............................16
  3.3 ivadmin Utility Only Provided for Backward Compatibility .......16
  3.4 General Backup and Restore Procedures ..............................17
  3.5 Enabling Policy Director Servers to Read SSL Key DataBase Files.17
  3.6 DCE Requires Integrated Login Service on Windows 2000 ..........18
  3.7 Audit Record Format Change .............................................19
  3.8 Base Installation Guides: New Section 5.2.2 .........................20
  3.9 Applying Policy Director ACLs to New LDAP Suffixes ..............21
  3.10 Policy Director LDAP Schema ..........................................29
New WebSEAL Information .......................................................... 30
3.12 Required WebSEAL SSL Configuration (GSKit Cache Size) .... 30
3.13 Configuring a Default Quality of Protection Level ................. 33
3.14 Understanding GSKit Key Database File Types ....................... 34
3.15 Consequences of Incorrect Step-up Authentication Configuration ... 36
3.16 Starting the junctioncp Utility ................................................. 36
3.17 Configuring Multiple Junctions to Same Server (IY19635) ......... 37
AIX i500 Separation Release Notes ............................................. 38
3.18 AIX i500 Separation Release Notes .......................................... 38

4 Corrections to the January 2001 Documentation ......................... 43
Corrections to the Installation Guides ........................................... 44
4.1 Incorrect SSL Certificate File Name ........................................... 44
4.2 Base Installation Guides: Revised Section 4.4.3 ......................... 44
Corrections to the Base Administration Guide ............................... 46
4.3 Time-of-Day POP Attribute .................................................... 46
4.4 Traverse Permission ............................................................ 46
4.5 Directing Messages to Standard Output - Debug Mode .............. 48
Corrections to the WebSEAL Administration Guide ....................... 49
4.6 Updating WebSEAL for Dynamic URLs (WebSEAL 6.3.3) ......... 49
4.7 WebSEAL Personalization Junction (WebSEAL 5.7) ................. 49
4.8 WebSEAL Only Supports HTTP/1.0 Across Junctions ............... 49
4.9 GSKit Session ID Timeout Parameters ..................................... 50
4.10 Correction to ssl-cache-inactive-timeout Text (IY21674) .......... 50
Corrections to the WebSEAL Developer Reference ....................... 51
4.11 Deploying the Template CDAS Server (Section 4.4) ................. 51
Corrections to the Console Administration Guide .......................... 52
4.12 Management Console Administration Guide Corrections ......... 52

5 Software Limitations .............................................................. 53
5.1 NetSEAL Kernel Trap is Not Supported on SMP Systems .......... 53
5.2 NetSEAL and NetSEAT Backward Compatibility ...................... 53
5.3 pdadmin Functionality Not Available on the Management Console. 53
5.4 Language Limitations Involving Double-byte Characters .......... 54
5.5 LDAP Does Not Treat User Names as Case-sensitive ...................... 54
5.6 pdconfig Utility May Fail on Japanese HP-UX Systems ............... 55
5.7 Management Console Online Help Inconsistencies ..................... 55
5.8 Untranslated Graphs Used in Translated Console Online Help ........ 56
5.9 pdadmin policy set min-password-reuse-num (IY18451) .............. 56

6 Known Software Defects and Workarounds .................................. 57

6.1 Upgrading Policy Director 3.6 WebSEAL .................................... 58
6.2 IBM SecureWay Directory 3.2 Requires AIX 4.3.3 Patches .......... 61
6.3 IBM SecureWay Directory DMT Utility Fails to Start ................. 62
6.4 NetSEAT Installation Requires GSKit 4.0 (IY22179) ................. 62

Base Defects and Workarounds ....................................................... 63
6.5 Configuring the Management Server on Solaris ....................... 63
6.6 LDAP 3.1.x to LDAP 3.2 Migration Procedure Revisions .......... 63
6.7 IBM DCE 3.1 Patch 3 Solves Management Server Memory Leak .... 65
6.8 Correction to set min-password-alphas Help Message (IY18408) ... 65

WebSEAL Defects and Workarounds .............................................. 66
6.9 Additional WAP Gateway Support .............................................. 66
6.10 Deleted User Credentials Remain in WebSEAL Cache .............. 66
6.11 Certificate Authentication for CDSSO Causes WebSEAL Failure .... 67
6.12 Forms Re-login Can Result Loss of POST Data (IY21348) .......... 68

NetSEAL Defects and Workarounds ............................................... 69
6.13 AIX Trap Defect ................................................................. 69
6.14 Solaris Patch Requirements ................................................... 69

Management Console Defects and Workarounds ............................ 70
6.15 Management Console Defects and Workarounds ...................... 70

LDAP Defects and Workarounds ................................................... 72
6.16 WebSEAL Can Become Unstable with LDAP Configuration .......... 72
Release Notes - Version 3.7 / 3.7.1
(Revised Date: 31 Dec 2001)

This Release Notes document contains new and revised technical information for Policy Director 3.7 (version 3, release 7, modification 0) and Policy Director 3.7.1 (version 3, release 7, modification 1).

This document is regularly updated with the latest information regarding Policy Director. A revision history table (found in the General Information section) tracks all additions and changes that occur to this document.

Numbers in parentheses refer to an internal tracking system.

Table of Contents:
1. General Information
2. Policy Director 3.7.1 Information
3. Important Supplemental Information
4. Corrections to the January 2001 Documentation
5. Software Limitations
6. Known Software Defects and Workarounds
1 General Information

Note: If you are a Policy Director administrator, it is essential that you read Section 3 “Important Supplemental Information” in its entirety.

- 1.1 - Release Notes Revision History
- 1.2 - Adobe Acrobat Reader, version 4.05 Recommended
- 1.3 - Navigating Policy Director PDF Documentation
- 1.4 - Policy Director 3.7.1 CD Distribution (30 March 2001)
- 1.5 - The Policy Director Documentation Set
- 1.6 - Revised Documentation Set Available on Support Site
- 1.7 - Policy Director Public Software Download Page
- 1.8 - Contacting Customer Support
- 1.9 - Problem Determination Checklist

1.1 Release Notes Revision History

The following Revision History table lists all changes made to this document since its first publication date:

<table>
<thead>
<tr>
<th>Date</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 Dec 2000</td>
<td>First version supplied with CD distribution.</td>
</tr>
<tr>
<td>16 Dec 2000</td>
<td>Section 3.4: “General Backup and Restore Procedures”</td>
</tr>
<tr>
<td>16 Dec 2000</td>
<td>Section 6.6: “LDAP 3.1.x to LDAP 3.2 Migration Procedure Revisions”</td>
</tr>
<tr>
<td>17 Jan 2001</td>
<td>Section 1.6: “Revised Documentation Set Available on Support Site”</td>
</tr>
<tr>
<td>17 Jan 2001</td>
<td>Section 3.3: “ivadmin Utility Only Provided for Backward Compatibility”</td>
</tr>
<tr>
<td>17 Jan 2001</td>
<td>Section 6.7: “IBM DCE 3.1 Patch 3 Solves Management Server Memory Leak”</td>
</tr>
<tr>
<td>07 Mar 2001</td>
<td>Section 1.3: “Navigating Policy Director PDF Documentation”</td>
</tr>
<tr>
<td>07 Mar 2001</td>
<td>Section 1.7: “Policy Director Public Software Download Page”</td>
</tr>
<tr>
<td>Date</td>
<td>Topic</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>07 Mar 2001</td>
<td>Section 3.5: “Enabling Policy Director Servers to Read SSL Key DataBase Files”</td>
</tr>
<tr>
<td>07 Mar 2001</td>
<td>Section 3.6: “DCE Requires Integrated Login Service on Windows 2000”</td>
</tr>
<tr>
<td>07 Mar 2001</td>
<td>Section 3.7: “Audit Record Format Change”</td>
</tr>
<tr>
<td>07 Mar 2001</td>
<td>Section 3.8: “Base Installation Guides: New Section 5.2.2”</td>
</tr>
<tr>
<td>07 Mar 2001</td>
<td>Section 3.9: “Applying Policy Director ACLs to New LDAP Suffixes”</td>
</tr>
<tr>
<td>07 Mar 2001</td>
<td>Section 3.13: “Configuring a Default Quality of Protection Level”</td>
</tr>
<tr>
<td>07 Mar 2001</td>
<td>Section 3.14: “Understanding GSKit Key Database File Types”</td>
</tr>
<tr>
<td>07 Mar 2001</td>
<td>Section 3.15: “Consequences of Incorrect Step-up Authentication Configuration”</td>
</tr>
<tr>
<td>07 Mar 2001</td>
<td>Section 3.16: “Starting the junctioncp Utility”</td>
</tr>
<tr>
<td>07 Mar 2001</td>
<td>Section 4.1: “Incorrect SSL Certificate File Name”</td>
</tr>
<tr>
<td>07 Mar 2001</td>
<td>Section 4.2: “Base Installation Guides: Revised Section 4.4.3”</td>
</tr>
<tr>
<td>07 Mar 2001</td>
<td>Section 4.3: “Time-of-Day POP Attribute”</td>
</tr>
<tr>
<td>07 Mar 2001</td>
<td>Section 4.6: “Updating WebSEAL for Dynamic URLs (WebSEAL 6.3.3)”</td>
</tr>
<tr>
<td>07 Mar 2001</td>
<td>Section 4.7: “WebSEAL Personalization Junction (WebSEAL 5.7)”</td>
</tr>
<tr>
<td>07 Mar 2001</td>
<td>Section 4.8: “WebSEAL Only Supports HTTP/1.0 Across Junctions”</td>
</tr>
<tr>
<td>07 Mar 2001</td>
<td>Section 4.11: “Deploying the Template CDAS Server (Section 4.4)”</td>
</tr>
<tr>
<td>07 Mar 2001</td>
<td>Section 4.12: “Management Console Administration Guide Corrections”</td>
</tr>
<tr>
<td>07 Mar 2001</td>
<td>Section 5.5: “LDAP Does Not Treat User Names as Case-sensitive”</td>
</tr>
<tr>
<td>07 Mar 2001</td>
<td>Section 6.1: “Upgrading Policy Director 3.6 WebSEAL”</td>
</tr>
<tr>
<td>07 Mar 2001</td>
<td>Section 6.2: “IBM SecureWay Directory 3.2 Requires AIX 4.3.3 Patches”</td>
</tr>
<tr>
<td>01 Apr 2001</td>
<td>Section 2: “Policy Director 3.7.1 Information”</td>
</tr>
<tr>
<td>01 Apr 2001</td>
<td>Section 3.10: “Policy Director LDAP Schema”</td>
</tr>
<tr>
<td>01 Apr 2001</td>
<td>Section 3.18: “AIX i500 Separation Release Notes”</td>
</tr>
</tbody>
</table>
## General Information

<table>
<thead>
<tr>
<th>Date</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>01 Apr 2001</td>
<td>Section 4.9: “GSKit Session ID Timeout Parameters”</td>
</tr>
<tr>
<td>01 Apr 2001</td>
<td>Section 5.6: “pdconfig Utility May Fail on Japanese HP-UX Systems”</td>
</tr>
<tr>
<td>01 Apr 2001</td>
<td>Section 5.7: “Management Console Online Help Inconsistencies”</td>
</tr>
<tr>
<td>01 Apr 2001</td>
<td>Section 5.8: “Untranslated Graphs Used in Translated Console Online Help”</td>
</tr>
<tr>
<td>01 Apr 2001</td>
<td>Section 6.11: “Certificate Authentication for CDSSO Causes WebSEAL Failure”</td>
</tr>
<tr>
<td>18 June 2001</td>
<td>Section 1.9: “Problem Determination Checklist”</td>
</tr>
<tr>
<td>18 June 2001</td>
<td>Section 2.6: “Mounting / Unmounting the Policy Director CD on HP”</td>
</tr>
<tr>
<td>18 June 2001</td>
<td>Section 3.12: “Required WebSEAL SSL Configuration (GSKit Cache Size)”</td>
</tr>
<tr>
<td>18 June 2001</td>
<td>Section 4.4: “Traverse Permission”</td>
</tr>
<tr>
<td>18 June 2001</td>
<td>Section 6.16: “WebSEAL Can Become Unstable with LDAP Configuration”</td>
</tr>
<tr>
<td>31 Dec 2001</td>
<td>Section 3.1: “Configuring DCE to Start Automatically (IY20147)”</td>
</tr>
<tr>
<td>31 Dec 2001</td>
<td>Section 3.11: “pdadmin user create -no-password-policy Option (IY19307)”</td>
</tr>
<tr>
<td>31 Dec 2001</td>
<td>Section 3.17: “Configuring Multiple Junctions to Same Server (IY19635)”</td>
</tr>
<tr>
<td>31 Dec 2001</td>
<td>Section 4.10: “Correction to ssl-cache-inactive-timeout Text (IY21674)”</td>
</tr>
<tr>
<td>31 Dec 2001</td>
<td>Section 5.9: “pdadmin policy set min-password-reuse-num (IY18451)”</td>
</tr>
<tr>
<td>31 Dec 2001</td>
<td>Section 6.4: “NetSEAT Installation Requires GSKit 4.0 (IY22179)”</td>
</tr>
<tr>
<td>31 Dec 2001</td>
<td>Section 6.8: “Correction to set min-password-alphas Help Message (IY18408)”</td>
</tr>
<tr>
<td>31 Dec 2001</td>
<td>Section 6.12: “Forms Re-login Can Result Loss of POST Data (IY21348)”</td>
</tr>
</tbody>
</table>
1.2 Adobe Acrobat Reader, version 4.05 Recommended

It is highly recommended that you use Adobe® Acrobat® Reader™, version 4.05 to view and print Policy Director PDF documents.

Adobe Acrobat Reader, version 4.05 is free from the Adobe Web site:

http://www.adobe.com/products/acrobat/readstep2.html

1.3 Navigating Policy Director PDF Documentation

Policy Director documentation in PDF format is designed for easy navigation to the information you need. Many parts of a Policy Director PDF file contain active hypertext.

Your mouse cursor changes to a “pointing hand” icon when you move the cursor over a hypertext area. When you click on a hypertext area, the PDF view jumps to the appropriate location inside or outside of the document.

The following parts of a Policy Director PDF file contain hypertext links:

- All bookmarks (which can also be expanded and contracted)
- Table of Contents entries
- Index page numbers
- URLs (shown in blue text)
- Section cross-references (shown in blue text)
1.4 Policy Director 3.7.1 CD Distribution (30 March 2001)

Policy Director CD Set:

- Tivoli SecureWay Policy Director Base for AIX (Version 3.7.1, 128-bit)
- Tivoli SecureWay Policy Director Base for Solaris (Version 3.7.1, 128-bit)
- Tivoli SecureWay Policy Director Base for Windows (Version 3.7.1, 128-bit)
- Tivoli SecureWay Policy Director Base for HP-UX (Version 3.7.1, 128-bit)
- Tivoli SecureWay Policy Director WebSEAL/NetSEAL for AIX, Solaris, and Windows (Version 3.7.1, 128-bit)
- Tivoli SecureWay Policy Director WebSEAL/NetSEAL for HP-UX (Version 3.7.1, 128-bit)
- Tivoli SecureWay Policy Director Management Console for Windows (Version 3.7.1, 128-bit)

CD Directory Content Description:

Note: The Policy Director CD for your specific platform may not contain each of these directories.

- /Doc contains basic technical documentation for Policy Director (This documentation, plus additional documentation, is also available on the Tivoli support site.)
- /Policy_Director contains the Policy Director installation image
- /GSKIT is the IBM implementation of SSL.
- /Schema contains the LDAP schema files required by Policy Director
- /SecureWay_Directory contains the IBM LDAP 3.2 installation image
- /Security_Services contains the IBM DCE installation image
- /Security_Service_Client for the WebSEAL/NetSEAL CD and the Console CD is the NetSEAT client
1.5 The Policy Director Documentation Set

The latest versions of all Tivoli SecureWay Policy Director documents are located on the Policy Director 3.7 / 3.7.1 support page.

<table>
<thead>
<tr>
<th>Installation Guides</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Director Base for AIX Installation Guide</td>
</tr>
<tr>
<td>Policy Director Base for HP-UX Installation Guide</td>
</tr>
<tr>
<td>Policy Director Base for Solaris Installation Guide</td>
</tr>
<tr>
<td>Policy Director Base for Windows Installation Guide</td>
</tr>
<tr>
<td>Policy Director WebSEAL Installation Guide</td>
</tr>
<tr>
<td>Policy Director NetSEAL Installation Guide</td>
</tr>
<tr>
<td>Policy Director Management Console for Windows Installation Guide</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Administration Guides</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Director Base Administration Guide</td>
</tr>
<tr>
<td>Policy Director WebSEAL Administration Guide</td>
</tr>
<tr>
<td>Policy Director NetSEAL Administration Guide</td>
</tr>
<tr>
<td>Policy Director Management Console for Windows Administration Guide</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Developer References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Director Authorization ADK Developer Reference</td>
</tr>
<tr>
<td>Policy Director Authorization API Java Wrappers Developer Reference</td>
</tr>
<tr>
<td>Policy Director WebSEAL Developer Reference</td>
</tr>
<tr>
<td>Policy Director Administration API Developer Reference</td>
</tr>
<tr>
<td>Policy Director CDAS API Developer Reference</td>
</tr>
<tr>
<td>Policy Director CDMF API Developer Reference</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Supplemental Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Director Performance Tuning Guide</td>
</tr>
<tr>
<td>Policy Director Lotus Domino Registry Supplement</td>
</tr>
<tr>
<td>Policy Director Migration Tool Administration Guide</td>
</tr>
</tbody>
</table>
1.6 Revised Documentation Set Available on Support Site

The Policy Director 3.7 / 3.7.1 support site now contains revised versions of the Policy Director Installation Guides, Administration Guides, and Developer References. The new revisions replace the documentation that was included on the original (December, 2000) Policy Director 3.7 CD-ROMs. The new revisions are dated January, 2001.

All hardcopy and translated Policy Director 3.7 documentation is based on this January 2001 version. The Policy Director 3.7.1 CD distribution also contains this updated January 2001 documentation.

1.7 Policy Director Public Software Download Page

The following page on the Tivoli support site contains links to supplemental software downloads for all versions of Policy Director:

http://www.tivoli.com/support/secureway/policy_dir/downloads.html

1.8 Contacting Customer Support

The Tivoli Customer Support Handbook at:

http://www.tivoli.com/support/handbook/

provides complete information about Tivoli Customer Support, including the following:

- Registration and eligibility
- How to contact support, depending on the severity of your problem
- Telephone numbers and e-mail addresses (country-specific)
- What information you should gather before contacting support
1.9 **Problem Determination Checklist**

Please use the following checklist to gather information about a problem with your Policy Director installation before you contact Customer Support.

1. Describe the hardware involved in this problem. Provide:
   - System types and models
   - Hostnames and IP addresses for all interfaces in each system

2. Describe the network involved.
   - Which interfaces on each system share a network?
   - What are the physical network types (for example, ethernet, token ring, FDDI)?
   - Is this configuration connected to the internet?

3. Is DCE used?
   - What DCE version is installed on each system?
   - Where are the security and directory servers located?
   - Is DCE replication used in the DCE cell?

4. Is LDAP used?
   - What version of the LDAP server and client is used?
   - Where are the LDAP servers located?

5. What is the version and build level of Policy Director on each system?

6. Identify the Policy Director components configured on each system:
   - NetSEAT (NT-only client)
   - Management Server (ivmgrd)
   - Management Console (ivconsole)
   - WebSEAL (secmgrd)
   - NetSEAL (secmgrd - IVTrap/PDTrap)
   - Authorization Server (ivacld)
   - Authorization ADK
   - Token CDAS
   - Certificate CDAS
   - Custom CDAS
General Information

7. Gather all *log files and *conf files under /opt/intraverse and /opt/dcelocal and all files under /opt/intraverse/www/log.
   (On NT, gather the files from under the Policy Director installation directory.)

8. Use junctioncp list to list all junctions on the WebSEAL servers and junctioncp show to provide junction details.

9. Provide a detailed set of steps that led to the problem, including all commands typed and buttons pressed.

10. Can you recreate the problem? If so, what are the detailed steps required to recreate the problem?

11. If a core dump is generated, gather the core, the binary causing the core, and all libraries used by the core. Send this information to customer support for analysis.
2 Policy Director 3.7.1 Information

- 2.1 - About Policy Director Version 3.7.1
- 2.2 - Upgrading from Policy Director 3.7 to 3.7.1
- 2.3 - New GSKit Package Available for WebSEAL Installations
- 2.4 - New LDAP 3.2 db2ldif Utility Patch
- 2.5 - Domino Registry Supported by Policy Director
- 2.6 - Mounting / Unmounting the Policy Director CD on HP

2.1 About Policy Director Version 3.7.1

Policy Director 3.7.1 is a National Language Support (NLS) release. The product supports data handling and message display for nine languages: Spanish, German, French, Italian, Brazilian Portuguese, Japanese, Korean, Simplified Chinese, and Traditional Chinese.

All the messages in these languages are provided by separate language packs which are posted on the Policy Director Software download web page:

http://www.tivoli.com/support/secureway/policy_dir/downloads.html

2.2 Upgrading from Policy Director 3.7 to 3.7.1

- The Policy Director 3.7.1 CD distribution does not support automatic code upgrade from version 3.7 to version 3.7.1.
- Customers who would like to upgrade an existing 3.7 installation to the 3.7.1 level without reconfiguration must download and install Policy Director 3.7 FixPack 2 to the existing Policy Director 3.7 installation. This process will preserve all configuration data.

The FixPack 2 package can be obtained from the Tivoli support site at: https://www.tivoli.com/secure/support/patches/

2.3 New GSKit Package Available for WebSEAL Installations

The following discussion applies to a Policy Director 3.7.1 WebSEAL installation.
The Policy Director 3.7.1 product includes several versions of GSKit:
- GSKit version 61 (Policy Director 3.7.1 Base for AIX CD)
- GSKit version 57 (Policy Director 3.7.1 Base for Solaris CD)
- GSKit version 65 (Policy Director 3.7.1 Base for HP-UX CD)
- GSKit version 58 (Policy Director 3.7.1 Base for Windows CD)
- GSKit version 126 (Policy Director 3.7.1 WebSEAL CD)

The latest version of GSKit (126) contains enhancements that improve WebSEAL performance and solves an SSL connection to LDAP server problem on Solaris installations. You must use this version of GSKit with any installation of WebSEAL.

If you do not have a WebSEAL installation, the GSKit package from the original platform-specific Base CD is still appropriate.

### 2.4 New LDAP 3.2 db2ldif Utility Patch

Recent IBM SecureWay Directory (LDAP) performance improvement patches distributed with the Policy Director 3.7.1 CD distribution cause the `db2ldif` LDAP administration utility to fail. The `db2ldif` utility was not updated to understand the correct format for the storage of users as members of groups.

A new `db2ldif` patch for each LDAP server platform—located in the `/Patch` directory of the Policy Director 3.7.1 CD—corrects this problem.

See also Section 1.7: “Policy Director Public Software Download Page”.

### 2.5 Domino Registry Supported by Policy Director

The Domino registry is supported by Policy Director 3.7.1 for Windows NT only. The Domino server itself can be set up on any of its supported platforms, but Policy Director 3.7.1 must be installed and configured on Windows NT.

The required Policy Director meta-data database template for Domino registry support (`PDMdata.ntf`) can be located in the `/schema` directory on the Policy Director 3.7.1 Base CDs.

The revised *Lotus Domino Registry Supplement* document can be found on the Policy Director 3.7 / 3.7.1 support page.
Policy Director 3.7.1 Information

Policy Director 3.7.1 for Windows NT supports both Domino 4.6.x and 5.0.x releases. Configuration for a Domino registry on Policy Director 3.7.1 involves the following Policy Director packages: PDRTE, PDMgr, and PDWeb.

Policy Director 3.7.1 configured for a Domino registry does not support client-side certificate authentication or Cross Domain Single-Sign On (CDSSO) functionality.

2.6 Mounting / Unmounting the Policy Director CD on HP

The following command syntax is required to mount and unmount the Policy Director 3.7 / 3.7.1 CD-ROM on a system running HP-UX:

To mount the CD:

```
# nohup /usr/sbin/pfs_mount &
# nohup /usr/sbin/pfsd &
# /usr/sbin/pfs_mount <mount-device> <mount-point>
```

For example:

```
# /usr/sbin/pfs_mount /dev/dsk/c0t0d0 /cdrom
```

To unmount the CD:

```
#/usr/sbin/pfs_umount <mount-point>
```

For example:

```
# /usr/sbin/pfs_umount /cdrom
```
3 Important Supplemental Information

- New Installation Information
- New Base Information
- New WebSEAL Information
- AIX i500 Separation Release Notes
New Installation Information

- 3.1 - Configuring DCE to Start Automatically (IY20147)

3.1 Configuring DCE to Start Automatically (IY20147)

This information supplements Section A.14 of the Tivoli SecureWay Policy Director Base for Solaris Installation Guide, “Installing and Configuring IBM DCE 3.1”.

During DCE installation and configuration, the system start-up scripts are automatically modified to provide for automatic start-up of the DCE server whenever Policy Director starts.
New Base Information

- 3.2 - Effect of an ACL Modification is Delayed
- 3.3 - ivadmin Utility Only Provided for Backward Compatibility
- 3.4 - General Backup and Restore Procedures
- 3.5 - Enabling Policy Director Servers to Read SSL Key DataBase Files
- 3.6 - DCE Requires Integrated Login Service on Windows 2000
- 3.7 - Audit Record Format Change
- 3.8 - Base Installation Guides: New Section 5.2.2
- 3.9 - Applying Policy Director ACLs to New LDAP Suffixes
- 3.10 - Policy Director LDAP Schema
- 3.11 - pdadmin user create -no-password-policy Option (IY19307)

3.2 Effect of an ACL Modification is Delayed

ACL policy update processing is now triggered after an idle timeout period of 15 seconds.

The timeout value (in seconds) can be configured by manually adding the notifier-wait-time parameter to the [ivmgrd] stanza of the ivmgrd.conf configuration file. For example:

```
notifier-wait-time = 25
```

See also Section 6.6.2 of the January 2001 Tivoli SecureWay Policy Director Base Administration Guide.

3.3 ivadmin Utility Only Provided for Backward Compatibility

The ivadmin utility is replaced in Policy Director 3.7 by the pdadmin utility. The functionality of the two utilities is exactly the same. In Policy Director 3.7, the ivadmin utility is only provided for backward compatibility.

The change in the utility name resulted from the change in the product name. Before Policy Director ("pd"), the product was known as IntraVerse ("iv").
3.4 General Backup and Restore Procedures

Detailed backup and restore procedures for Policy Director are typically developed on a per-customer basis, depending on the configuration. All start with the same basic formula:

- For DCE backup and restore, refer to the appropriate DCE documentation. In particular, the `dceback` command reference, has noteworthy information.

  The following link locates this information for Transarc DCE:


- For Policy Director, back up the main installation file system (`/opt/PolicyDirector` on UNIX systems, and `Program Files\Tivoli\Policy Director` on Windows NT systems).

- Restore operations can be done while the system continues to process transactions since redundancy and high availability in a properly replicated Policy Director environment minimizes the likelihood of real-time disasters.

3.5 Enabling Policy Director Servers to Read SSL Key DataBase Files

Problem:

Policy Director fails silently if the SSL key database file used for LDAP client authentication cannot be read.

This problem only applies to SSL key database files that are created by an administrator in order to enable SSL communication between IBM SecureWay Directory clients and IBM SecureWay Directory servers.

This problem does not apply to the two SSL key database files that are created during configuration of Policy Director Management Server and Policy Director WebSEAL.

Explanation:

IBM SecureWay Directory Clients can optionally use the Secure Socket Layer (SSL) communication protocol for communication with an IBM SecureWay
Important Supplemental Information

Directory LDAP server. Policy Director uses this communication channel as part of the process for making authentication and authorization decisions.

Successful use of SSL communication relies on use of a key database file. This key database file must be readable by the Policy Director user, which typically run as user, ivmgr. This permission is not assigned by default when the LDAP administrator creates a key database file for use between the LDAP client and the LDAP server.

Solution:

Creation of the SSL key database file is described in each of the Base Installation Guides in the following sections:

<table>
<thead>
<tr>
<th>Document</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Director Base for Solaris Installation Guide</td>
<td>7.3.1, 7.4.1</td>
</tr>
<tr>
<td>Policy Director Base for AIX Installation Guide</td>
<td>6.3.1, 6.4.1</td>
</tr>
<tr>
<td>Policy Director Base for Windows Installation Guide</td>
<td>7.3.1, 7.4.1</td>
</tr>
<tr>
<td>Policy Director Base for HP-UX Installation Guide</td>
<td>6.3.1, 7.4.1</td>
</tr>
</tbody>
</table>

In each of the guides, the section Creating the Key Database File and the Certificate contains a numbered list of actions items from 1 to 10 on how to create the key database file using the GUI tool gsk4ikm. Add the following text, as step 11, to the end of the list:

11. After creating the key database file, change the file ownership of the key database file to ivmgr. Use the appropriate operating system command for changing file ownership.

   For example, on UNIX enter:

   `# chown ivmgr <keyfile>`

3.6 DCE Requires Integrated Login Service on Windows 2000

Problem:

After installing NetSEAT and Policy Director on Windows 2000, users are unable to login to the DCE cell.
Explanation:

Windows 2000 introduced a new service called Integrated Login Service. This service must be enabled in order for DCE logins to succeed.

Solution:

Enable the Windows 2000 Integrated Login Service. DCE logins now succeed.

Note: The Windows 2000 Integrated Login Service is unrelated to the NetSEAT integrated login feature. The NetSEAT integrated login feature should not be enabled. The NetSEAT integrated login is not enabled by default.

3.7 Audit Record Format Change

Note: The following information updates the content in Sections 8.5 and 8.6 of the Tivoli SecureWay Policy Director Base Administration Guide.

The original Policy Director 3.7 XML-formatted audit record inadvertently reused the element tag name <event>. The first use of <event> enclosed an entire “audit event” document. A nested use of <event> was intended to denote an event action identifier.

The second element tag name has now been changed to <action>. The version number of the event record has been incremented and a new version attribute has been added to the <component> element.

A sample of a newly formatted event appears as follows:

```xml
<event rev="1.1">
  <date>2001-02-22-01:25:54.452+00:00I-----</date>
  <outcome status="0">0</outcome>
  <originator blade="ivmgrd"><component rev="1.1">azn</component>
    <action>0</action>
    <location>azn_id_get_creds</location>
  </originator>
  <accessor name="unauthenticated">
    <principal auth="IV_UNAUTH_V3.0">Unauth</principal>
  </accessor>
  <target resource="3"><object>IV_UNAUTH_V3.0:unauthenticated</object></target>
  <data>
  </data>
</event>
```
3.8 Base Installation Guides: New Section 5.2.2

Summary:
Add a new Section 5.2.2 to each of the Policy Director Base Installation Guides. Add the text contained in the following section of these Release Notes:

- 5.2.2 Adding ACLs to Policy Director Suffixes

Explanation:
Each of the Policy Director Base Installation Guides contains a Chapter 5, entitled “Configuring a Netscape LDAP Server”. This chapter describes how to specify certain Policy Director information for use with Netscape LDAP servers. The instructions in this chapter are performed prior to the installation and configuration of the Policy Director servers.

Section 5.2 describes the addition of new suffixes to the Netscape Directory Server. The handling of Access Control Lists (ACLs) on these new suffixes is not discussed.

Create a new Section 5.2.2 containing the following text:

5.2.2 Adding ACLs to Policy Director Suffixes

When Policy Director is configured, it automatically attempts to add appropriate ACLs to every suffix in the LDAP Server, in order to allow Policy Director to create and update user and group information within those suffixes.

However, for any suffixes which the LDAP administrator adds after the initial configuration of Policy Director, the administrator must add the appropriate ACLs manually.

For instructions on adding appropriate ACLs to suffixes after Policy Director has been configured, see the following Policy Director 3.7 Release Note section:

3.9 - Applying Policy Director ACLs to New LDAP Suffixes.
3.9 Applying Policy Director ACLs to New LDAP Suffixes

Introduction

Note: The following information applies to both IBM SecureWay Directory Server and Netscape LDAP Server.

When an LDAP administrator adds LDAP suffixes after the initial configuration of Policy Director, the administrator must apply the appropriate Access Control Lists (ACLs) to allow Policy Director to manage users and groups defined in these new suffixes.

For IBM SecureWay Directory, use the Directory Management Tool to apply ACLs. For Netscape LDAP server, use the Netscape Console.

Use the appropriate LDAP administration interface to apply the following ACLs to every new Policy Director suffix:

<table>
<thead>
<tr>
<th>LDAP Group</th>
<th>Access Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn=SecurityGroup,secAuthority=Default</td>
<td>• full access</td>
</tr>
<tr>
<td>cn=ivacl-servers,cn=SecurityGroups,secAuthority=Default</td>
<td>• read</td>
</tr>
<tr>
<td></td>
<td>• search</td>
</tr>
<tr>
<td></td>
<td>• compare</td>
</tr>
<tr>
<td>cn=remote-acl-users,cn=SecurityGroups,secAuthority=Default</td>
<td>• read</td>
</tr>
<tr>
<td></td>
<td>• search</td>
</tr>
<tr>
<td></td>
<td>• compare</td>
</tr>
</tbody>
</table>

These controls apply when the administrator has selected LDAP for the Policy Director user registry and a new LDAP suffix has been created after Policy Director is initially configured. It is assumed that you are the Policy Director administrator and are familiar with both Policy Director and LDAP. It is further assumed that, as administrator, you have the proper authority to update the LDAP Directory Information Tree.
When Policy Director is configured, it attempts to apply appropriate ACLs to every LDAP suffix that exists at that time in the LDAP server. This access control allows Policy Director to create and manage user and group information within these LDAP suffixes.

However, if a suffix is created after Policy Director has been configured, and Policy Director must later be able to create and manage user and group information within this new suffix, then the appropriate access controls need to be applied manually. Without these access controls, Policy Director does not have the appropriate LDAP permission to create and manage user and group information specified to be within this new suffix.

To apply the appropriate access controls to the newly created LDAP suffix, perform the following steps for either the IBM SecureWay Directory or the Netscape Directory Server, depending on the LDAP server type being used.

Note that the procedures assume that the newly created suffix is called “o=neworg,c=us”. You should substitute the actual newly created suffix for this value in the following descriptions.

**Procedures for the IBM SecureWay Directory Server**

To apply the appropriate Policy Director access controls to the newly created suffix for the IBM SecureWay Directory Server, follow these steps:

1. Start the LDAP Directory Management Tool (DMT).
   - **Windows:** Start > Programs > IBM SecureWay Directory > Directory Management Tool
   - **UNIX:** # /usr/bin/dmt

2. The following warning might appear:
   - **Warning:** Entry o=neworg,c=us does not contain any data.

   If this warning appears, it indicates that the entry represented by the newly created suffix, does not yet exist. Access controls cannot be applied to the newly created suffix until the entry represented by the suffix has been created.

   Dismiss the warning and proceed with Step 3. You will create the organization entry specified in the new suffix in Step 6.

   If this warning does not appear, the organization entry specified in the newly created suffix already exists.

   Proceed with Step 3 and skip Step 6.
3. Click the Add Server button at the bottom of the left hand frame. The Add Server window appears.

4. Enter values for the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name:</td>
<td>ldap://&lt;hostname&gt;</td>
<td>For example, ibm007.ibm.com</td>
</tr>
<tr>
<td>Port:</td>
<td>389</td>
<td>389 is the default port</td>
</tr>
<tr>
<td>User DN:</td>
<td>cn=root</td>
<td>DN of the LDAP administrator</td>
</tr>
<tr>
<td>User Password:</td>
<td>abc123</td>
<td>Password of the LDAP administrator</td>
</tr>
</tbody>
</table>

5. Click OK. The Directory Management Tool page appears.

6. If the organization entry specified in the newly created suffix does not yet exist (that is, you received the warning message described in Step 2), create the entry by following Section 4.4.2 in the Tivoli SecureWay Policy Director Base Installation Guide.

   When you have successfully created the entry, skip Step 9 in the Base Installation Guide and proceed with Step 7 below.

   If the organization entry already exists, continue with Step below.

7. From the left pane of the Directory Management Tool, select:
   Directory Tree > Browse Tree

8. Highlight the newly created suffix in the Browse Tree pane on the right.

9. Click the ACL button at the top of the pane.
   The current Access Control List settings for the suffix are displayed in the Edit an LDAP ACL window.

10. In the Subject area of the Edit an LDAP ACL window, enter the following Distinguished Name:
    
    cn=SecurityGroup,secAuthority=Default

    Check the group Type and click the Add button.
11. When the panel is redisplayed, choose the following settings:
   The Rights should be Grant for Add child and Delete entry.
   All permissions (Read, Write, Search, and Compare) should be granted for all Security classes.
   To do this, be sure each selection indicates Grant for all classes within each column for Read, Write, Search, and Compare.
   Be sure that the “Descendant directory tree entries inherit from this entry” is selected at the top of the DN entry pane.
   Once all selections have been made, click OK at the bottom of the pane.

12. Again highlight the newly created suffix in the Browse Tree pane on the right.

13. Click the ACL button at the top of the pane.
   Verify that the `cn=SecurityGroup,secAuthority=Default` group is listed and the settings for the group are correct. Note that the alphabetic case of the group name does not matter.

14. In the Subject area of the Edit an LDAP ACL window, enter the following Distinguished Name:
   `cn=ivacld-servers,cn=SecurityGroups,secAuthority=Default`
   Check the group Type and click the Add button.

15. When the panel is redisplayed, choose the following settings:
   The Rights should be Unspecified for Add child and Delete entry.
   Read, Search and Compare permissions only should be granted for the Normal Security class.
   To do this, select Grant for just the Normal Security class within each column for Read, Search, and Compare.
   The Write permission for the Normal Security class should be Unspecified.
   All permissions for the Sensitive and Critical Security classes, should be Unspecified.
   Be sure that the “Descendant directory tree entries inherit from this entry” is selected at the top of the DN entry pane.
   Once all selections have been made, click OK at the bottom of the pane.
16. Again highlight the newly created suffix in the Browse Tree pane on the right.

17. Click the ACL button at the top of the pane. Verify that the 
   `cn=ivacld-servers,cn=SecurityGroups,secAuthority=Default` group is 
   listed and the settings for the group are correct. Note that the alphabetic 
   case of the group name does not matter.

18. In the Subject area of the Edit an LDAP ACL window, enter the following 
   Distinguished Name: 
   `cn=remote-acl-users,cn=SecurityGroups,secAuthority=Default` 
   Check the group Type and click the Add button.

19. When the panel is redisplayed, choose the following settings:
   - The Rights should be Unspecified for Add child and Delete entry.
   - Read, Search, and Compare permissions only should be granted for the 
     Normal Security class.
   - To do this, be sure to only select Grant for just the Normal Security class 
     within each column for Read, Search, and Compare.
   - The Write permission for the Normal Security class should be 
     Unspecified.
   - All permissions for the Sensitive and Critical Security classes should be 
     Unspecified.
   - Be sure that the “Descendant directory tree entries inherit from this entry” 
     is selected at the top of the DN entry pane.
   - Once all selections have been made, click OK at the bottom of the pane.

20. The Access Control List changes are now complete. 
   Select the Exit button to complete the Directory Management Tool.
Procedures for the Netscape Directory Server

To apply the appropriate Policy Director access control to the newly created suffix for the Netscape Directory Server, follow these steps:

1. Start the Netscape Directory Console
   
   **Windows:** Start > Programs > Netscape Server Products > Netscape Console
   
   **UNIX:** In the Netscape server install directory:
   
   `# ./startconsole`

2. In the Netscape Console login window, enter the administrator ID, password, and URL to access the Netscape administration page.
   
   For example:

<table>
<thead>
<tr>
<th>User ID:</th>
<th>cn=Directory Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password:</td>
<td>abc123</td>
</tr>
<tr>
<td>Administration URL:</td>
<td><a href="http://ibm007.ibm.com">http://ibm007.ibm.com</a>:&lt;port number&gt;</td>
</tr>
</tbody>
</table>

   Click the OK button to login.

3. Expand the server name within the domain configured for the Netscape Directory Server you are using.
   
   Then expand the Server Group and highlight the Directory Server you are using.
   
   Click the Open button in the right pane.
   
   Another window is displayed with a set of tabs showing the operations which may be performed on the Directory Server.

4. Select the Directory tab.

5. If the newly created suffix appears in the left pane, proceed with Step 6.

   If the newly created suffix (**o=neworg,c=us**) does not appear in the left pane, it indicates that the entry for the new suffix does not yet exist.
   
   Access controls cannot be applied to the newly created suffix until the entry has been created.
   
   If this is the case, select Object in the task bar at the top of the window and select:
   
   `New > Other...`
The New Object selection window appears. Scroll down and highlight “Organization” as the new object entry type. Then click OK.

The Property Editor window appears. Fill in the Organization field as “neworg,c=us” and click OK. Remember, these instructions assume an example suffix. Create the entry type and name which corresponds to your actual suffix.

Now select View from the task bar at the top of the window and select Refresh.

The new suffix entry should appear in the left pane.

6. Highlight the neworg entry in the left pane and select Object in the task bar at the top of the window. Then click on Set Access Permissions…

The Multi-value ACI Selector window appears.

Click the New button to display the Set Access Permissions window.

7. Click on the Allow/Deny field and set it to Allow.

8. Double click on the User/Group field. The Select Users and Groups window appears.

Set the type to Add Group to List and enter the group name as:

```
cn=SecurityGroup,secAuthority=Default
```

Click the Add button.

Then click OK at the bottom of the panel.

9. When the Set Access Permissions window is redisplayed, ensure that the group name is listed properly in the User/Group field and that the Rights field indicates All.

10. Click the Add Rule button. Another rule is added with default values.

11. Within the newly added rule, click on the Allow/Deny field and set it to Allow.

12. Double click on the User/Group field. The Select Users and Groups window appears.

Set the type to Add Group to List and enter the group name as:

```
cn=ivacld-servers,cn=SecurityGroups,secAuthority=Default
```

Click the Add button.

Then click OK at the bottom of the panel.
13. When the Set Access Permissions window is redisplayed, ensure that the group name is listed properly in the User/Group field.

14. Double click the Rights field and check only the Read, Search, and Compare affected rights. All other rights should be deselected. Then click OK.

15. Click the Add Rule button. Another rule is added with default values.

16. Within the newly added rule, click on the Allow/Deny field and set it to Allow.

17. Double click on the User/Group field. The Select Users and Groups window appears.
   Set the type to Add Group to List and enter the group name as:
   ```
   cn=remote-acl-users,cn=SecurityGroups,secAuthority=Default
   ```
   Click the Add button.
   Then click OK at the bottom of the panel.

18. When the Set Access Permissions window is redisplayed, ensure that the group name is listed properly in the User/Group field.

19. Double click the Rights field and check only the Read, Search, and Compare affected rights. All other rights should be deselected.
   Then click OK.

20. When the Set Access Permissions window is redisplayed, all three group rules should be shown.
   Click OK at the bottom of the panel.

21. The access controls have now been added.
   You can exit the Netscape Console by selecting (from the task bar):
   ```
   Console > Exit
   ```
3.10 Policy Director LDAP Schema

Policy Director uses a standards-based LDAP schema to implement all user registry functions. This schema makes Policy Director compatible with the user and group management capabilities of most other LDAP-based applications.

Because Policy Director supports a wide range of authorization functionality, extensions to this standards-based schema are provided in the form of custom Policy Director LDAP object definitions. The schemas for these custom objects are published in the LDAP directory during Policy Director installation and are visible to other LDAP applications.

Occasionally it may be necessary to modify the schema definitions of these custom objects and add new object definitions. Although Policy Director can conceal these changes during a Policy Director upgrade, the changes will not be transparent to other applications. Therefore, it is recommended that third-party applications not use the custom Policy Director LDAP object definitions provided at installation time.

An API is available for third-party applications that need to maintain authorization information independent of the Policy Director administration tools. Refer to the Tivoli SecureWay Policy Director Administration API Developer Reference (available on the Policy Director support page).

3.11 pdadmin user create -no-password-policy Option (IY19307)

The –no-password-policy option to the pdadmin user create command allows the administrator to create the user with a password that is not checked by the existing global password policies. If this option is not present in the command, the password is checked against the global password policies. In this case, the user create command fails if the password is invalid and the error message includes information on what conditions were not met.

However if the administrator applies the pdadmin user modify password, the –no-password-policy option is not available. Therefore, the modified password is always checked against the global password policy settings.

Similarly, if the user changes the password (/pkmspasswd), the new password is always checked against the global password policy settings.
New WebSEAL Information

- 3.12 - Required WebSEAL SSL Configuration (GSKit Cache Size)
- 3.13 - Configuring a Default Quality of Protection Level
- 3.14 - Understanding GSKit Key Database File Types
- 3.15 - Consequences of Incorrect Step-up Authentication Configuration
- 3.16 - Starting the junctioncp Utility
- 3.17 - Configuring Multiple Junctions to Same Server (IY19635)

3.12 Required WebSEAL SSL Configuration (GSKit Cache Size)

**Background:**

By default, the WebSEAL SSL cache size is limited to:

- 512 entries (SSL V3)
- 256 entries (SSL V2)

This size is not sufficient for most production deployments.

WebSEAL SSL services are provided by the GSKit component of Policy Director. When the GSKit SSL session cache becomes full, WebSEAL rejects all new SSL-based authentications.

You can configure the size of the GSKit SSL session cache with an environment variable.

The space requirements for the GSKit SSL session cache is determined primarily by the interaction of two factors:

- The number of authentications per second
  
  This authentication rate results in adding entries to the cache.

- The session ID lifetime value ([ssl-v2-timeout](#) or [ssl-v3-timeout](#) parameter)
  
  This parameter results in eliminating entries from the cache.

**Configuration Guidelines:**

The GSKit SSL session cache size is specified in an environment variable ([GSK_V3_SIDCACHE_SIZE](#)). You can estimate the optimal size of the cache by:
1. Determining an average authentications per second access rate, and

2. Setting an appropriate session ID timeout value in the ssl-v2-timeout or ssl-v3-timeout parameter (located in secmgrd.conf configuration file).

Default values at installation:

- GSK_V3_SIDCACHE_SIZE = 512 (entries)
- ssl-v2-timeout = 100 (seconds)
- ssl-v3-timeout = 7200 (seconds, or 2 hours)

WebSEAL session ID management involves the combined interaction between the GSKit session ID cache and the WebSEAL credentials cache. Therefore, you should additionally set the WebSEAL credentials cache timeout (ssl-cache-timeout) to equal the GSKit ssl-v2-timeout or ssl-v3-timeout values.

The ssl-cache-timeout parameter is located in secmgrd.conf configuration file. Default value at installation:

- ssl-cache-timeout = 3600 (seconds, or 1 hour)

The following formula allows you to determine an appropriate size for the GSKit SSL session cache:

\[
\text{authentications/second} \times \text{ssl-v3-timeout value} = \text{cache-size}
\]

For example, a conservative estimate of the authentications per second rate for a single WebSEAL server is 40 per second. If you leave the ssl-v3-timeout parameter at the default value (7200), the cache size becomes:

\[
40 \text{ entries/sec} \times 7200 \text{ sec} = 288000 \text{ entries}
\]

Modify this variable prior to starting Policy Director:

1. Stop Policy Director:
   
   # iv stop

2. Set the GSK_V3_SIDCACHE_SIZE environment variable:
   
   # GSK_V3_SIDCACHE_SIZE=288000
   # export GSK_V3_SIDCACHE_SIZE

3. Start Policy Director:
   
   # iv start
Note: The GSKit code rounds down the GSK_V3_SIDCACHE_SIZE value to the nearest power of 2. For example, a value of 24000 is reduced to 16384, 144000 to 131072, 4096 to 4096, and so forth.

If you reboot the WebSEAL machine, this environment variable value is lost and reset to the default value (512). To avoid this problem, insert the appropriate export command in the iv start script.

The consequence of increasing the GSKit SSL session cache size is increased memory usage by the WebSEAL process (secmgrd). A GSKit SSL session cache size of 144000 can increase the WebSEAL process memory usage by as much as 100MB. Memory usage also increases for ivmgrd and ivacld, if they reside on the same machine.

By decreasing the value of the ssl-v3-timeout (or ssl-v2-timeout) parameter (which shortens the maximum lifetime for each cache entry), you can specify a smaller cache size.

Special Note for Supporting Internet Explorer:

A special situation exists for users of Microsoft Internet Explorer, which currently exhibits a problem that causes session renegotiation approximately every two minutes. If you use Internet Explorer, you most likely configure WebSEAL to take advantage of the HTTP session state cookie mechanism for SSL (ssl-cookie-sessions) to maintain login sessions.

However, the renegotiated session IDs continue to populate the GSKit session ID cache. The session ID timeout, as discussed previously, is determined by the value of the ssl-v2-timeout or ssl-v3-timeout parameter. If the authentication rate is high, a large value for this parameter would result in a rapid filling of the cache.

In this scenario, you might consider setting the ssl-v2-timeout or ssl-v3-timeout parameter to equal 3 or 4 minutes. This would closely match the Internet Explorer renegotiation rate and serve to keep the GSKit cache from filling with these renegotiated session IDs.

Special Note Regarding AIX Performance

For AIX systems, a large value for the GSK_V3_SIDCACHE_SIZE environment variable results in poor performance. This performance problem can be avoided by setting the AIXTHREAD_MUTEX_DEBUG environment variable to “OFF”.
For example:

```
# export AIXTHREAD_MUTEX_DEBUG=OFF
```

You can also automate this condition by adding his command to the `iv_start` script.

**Related Issues:**

Another related issue involves configuring the size of the WebSEAL SSL credentials cache. The parameter that specifies this value is `ssl-cache-max-sessions` (located in the `secmgrd.conf` file).

This parameter controls how many concurrent SSL sessions are allowed in this cache. The parameter affects the performance of SSL session creation and should not be increased without considering this fact. If you want to change this parameter, do some performance testing using various settings.

For further information on managing session states for WebSEAL, refer to Section 4.2 of the *Tivoli SecureWay Policy Director 3.7 WebSEAL Administration Guide*.

### 3.13 Configuring a Default Quality of Protection Level

You can control the default level of encryption required for SSL access to WebSEAL by managing the quality of protection. Default quality of protection management is controlled using two parameters in the `iv.conf` configuration file:

- **ssl-qop-mgmt**
- **Entries in the `[ssl-qop-mgmt-default]` stanza**

1. Enable quality of protection management:

   ```
   [wand]
   ssl-qop-mgmt = yes
   ```

2. Specify the default encryption level for SSL access:

   ```
   [ssl-qop-mgmt-default]
   # default = ALL | NONE | cipher-level
   # ALL (enables all ciphers)
   # NONE (disables all ciphers and uses an MD5 MAC check sum)
   # DES-40
   # DES-56
   # DES-168
   # RC2-40
   # RC2-128
   ```
Important Supplemental Information

# RC4-40
# RC4-128
default = ALL

Note that you can also specify a selected group of ciphers:

[ssl-qop-mgmt-default]
default = RC4-128
default = RC2-128
default = DES-168

Note: The ssl-qop-mgmt = yes parameter also enables any settings in the
[ssl-qop-mgmt-hosts] and [ssl-qop-mgmt-networks] stanzas. These
stanzas allow quality of protection management by specific
host/network/netmask IP address. The [ssl-qop-mgmt-default] stanza
lists the ciphers used for all IP addresses not matched in the

The [ssl-qop-mgmt-hosts] and [ssl-qop-mgmt-networks] stanzas are
provided for backward compatibility only. It is not recommended that you
use them for Policy Director 3.7 configuration.

3.14 Understanding GSKit Key Database File Types

Note: The following information enhances the content in Section 2.6 of the Tivoli
SecureWay Policy Director WebSEAL Administration Guide.

The IBM Key Management tool (iKeyman) uses several file types that are
summarized in the following table.

A CMS key database consists of a file with the extension .kdb and possibly two
or more other files. The .kdb file is created when you create a new key
database. A key record in a .kdb file can be either a certificate or a certificate
with its encrypted private key information.

The .rdb and .crl files are created when you create a new certificate request.
The .rdb file is required throughout the CA certificate request process.

<table>
<thead>
<tr>
<th>File Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.kdb</td>
<td>The “key database” file. Stores personal certificates, personal certificate requests, and signer certificates. For example, the default WebSEAL key database file is pdsrv.kdb.</td>
</tr>
</tbody>
</table>
The "stash" file. Stores an encrypted version of the key database password. The stem name of this file is the same as the associated .kdb file.

The "request" database file. Automatically created when you create a .kdb key database file. The stem name of this file is the same as the associated .kdb file. This file contains certificate requests that are outstanding and have not yet been received back from the CA.

When a certificate is returned from the CA, the .rdb file is searched for the matching certificate request (based on the public key). If a match is found, the certificate is received and the corresponding certificate request is deleted from the .rdb file.

If a match is not found, the attempt to receive the certificate is rejected. Included in the certificate request is the common name, organization, street address, and other information that was specified at the time of the request, as well as the public and private key associated with the request.

The "certificate revocation list" file. This file normally contains the list of certificates that have been revoked for one reason or another. However, iKeyman does not provide any support for certificate revocation lists, so it is empty.

An ASCII encoded binary file. A .arm file contains a base-64 encoded ASCII representation of a certificate, including its public key, but not its private key. The original binary certificate data is transformed into an ASCII representation.

When a user receives a certificate in a .arm file, iKeyman decodes the ASCII representation and places the binary representation into the appropriate .kdb file. Similarly, when a user extracts a certificate from a .kdb file, iKeyman converts the data from binary to ASCII and places it in a .arm file.

The ASCII data in the .arm file is what you send to the CA during the certificate request process.

Note: Any file type is acceptable to use (other than .arm), as long as the file itself is a Base64 encoded file.

<table>
<thead>
<tr>
<th>File Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.sth</td>
<td>The &quot;stash&quot; file. Stores an encrypted version of the key database password. The stem name of this file is the same as the associated .kdb file.</td>
</tr>
<tr>
<td>.rdb</td>
<td>The &quot;request&quot; database file. Automatically created when you create a .kdb key database file. The stem name of this file is the same as the associated .kdb file. This file contains certificate requests that are outstanding and have not yet been received back from the CA.  When a certificate is returned from the CA, the .rdb file is searched for the matching certificate request (based on the public key). If a match is found, the certificate is received and the corresponding certificate request is deleted from the .rdb file.  If a match is not found, the attempt to receive the certificate is rejected. Included in the certificate request is the common name, organization, street address, and other information that was specified at the time of the request, as well as the public and private key associated with the request.</td>
</tr>
<tr>
<td>.crl</td>
<td>The &quot;certificate revocation list&quot; file. This file normally contains the list of certificates that have been revoked for one reason or another. However, iKeyman does not provide any support for certificate revocation lists, so it is empty.</td>
</tr>
<tr>
<td>.arm</td>
<td>An ASCII encoded binary file. A .arm file contains a base-64 encoded ASCII representation of a certificate, including its public key, but not its private key. The original binary certificate data is transformed into an ASCII representation.  When a user receives a certificate in a .arm file, iKeyman decodes the ASCII representation and places the binary representation into the appropriate .kdb file. Similarly, when a user extracts a certificate from a .kdb file, iKeyman converts the data from binary to ASCII and places it in a .arm file.  The ASCII data in the .arm file is what you send to the CA during the certificate request process.  Note: Any file type is acceptable to use (other than .arm), as long as the file itself is a Base64 encoded file.</td>
</tr>
</tbody>
</table>
### 3.15 Consequences of Incorrect Step-up Authentication Configuration

Incorrect configuration of step-up authentication levels in the [authentication-levels] stanza of the iv.conf configuration file results in the disabling of step-up functionality within WebSEAL. This situation can lead to unexpected authentication behavior, such as the password login page being issued for objects protected by a POP that requires the token-card authentication level.

After modifying step-up authentication levels, check the secmgrd.log file for reports of any configuration errors.

### 3.16 Starting the junctioncp Utility

**Note:** The following information updates the content in Sections 5.2.1 and C.1 of the Tivoli SecureWay Policy Director WebSEAL Administration Guide.

Before you can use the junctioncp utility, you must:

1. **Login as the root user or the ivmgr user.**
   
   The junctioncp utility must be able to read the secmgrd.conf file, which is owned by ivmgr.
2. Additionally, you must perform a `dce_login` (UNIX or Windows) or a `netseat_login` (Windows).

3. Finally, invoke the `junctioncp` command as described in the documentation.

### 3.17 Configuring Multiple Junctions to Same Server (IY19635)

Creating multiple WebSEAL junctions that point to the same back-end application server/port can cause unpredictable control of access to resources and therefore is not a recommended or supported Policy Director configuration strategy.

Each WebSEAL junction can be secured by a unique set of access controls (ACLs). However, the ACL policy of each newly created junction overlays the policies of previously created junctions attached to the same back-end server/port. Subsequent junctions secured with more permissive ACLs can compromise previous junctions secured with less permissive ACLs. WebSEAL and the Policy Director authorization model cannot guarantee secure access control with this type of junction implementation.
AIX i500 Separation Release Notes

Introduction

These notes are based on and reference Chapter 6 (Configuring a LiveContent Server) of the Tivoli SecureWay Policy Director 3.7 Base for Solaris Installation Guide.

Installation and configuration of Policy Director 3.7.1 on AIX against a LiveContent(i500) directory is a multistep operation. Following is a summary of the steps required.

1. Install the Policy Director 3.7.1 package on the AIX host.
2. Copy the i500 specific configuration files to the i500 host.
3. Configure the required Policy Director 3.7.1 components except for PDAcld. PDAcld cannot be configured until PDMgr is configured into the i500 directory.
4. Copy the i500 configuration data file produced in the previous step to the i500 host
5. Perform configuration of the i500 directory on the i500 host using the i500 external configuration script.
6. Repeat steps 3, 4, and 5 to install the PDAcld server or any other server
Steps 3, 4, and 5 can be repeated for unconfiguring any or all Policy Director 3.7 components.

Software Requirements

This distribution supports only the installation of Policy Director on AIX against i500 Directory on Solaris. The version of i500 supported is the same as for Policy Director 3.7:

- LiveContent DSA V8.3.1.12
- LDAP Server V8.2.4.8
Installing Policy Director 3.7.1 on AIX

Install Policy Director 3.7.1 according to the Tivoli SecureWay Policy Director 3.7 Base for AIX Installation Guide and the Policy Director Release Notes. The directory /opt/PolicyDirectory/i500_external is created. The contents of this directory need to be transferred to a directory on the i500 server since they contain the i500 specific configuration files:

<any-i500o-host-directory>/i500_external

Configuring LiveContent Directory

Follow Section 6.2 in the Tivoli SecureWay Policy Director 3.7 Base for Solaris Installation Guide. The condition in Step 2 is optional for Policy Director 3.7.1.

An environment variable I500_DAP_PORT can be defined to contain the DAP port number. Otherwise the DAP port will default to one less than the LDAP port number.

Loading the Policy Director Schema

Follow Section 6.3 in the Tivoli SecureWay Policy Director 3.7 Base for Solaris Installation Guide. The directory containing the schema files is:

<any-i500o-host-directory>/i500_external/lib

The directory i500_external is the one copied from the AIX installation.

Configuration of the Policy Director Host System

Follow Section 6.4 in the Tivoli SecureWay Policy Director 3.7 Base for Solaris Installation Guide. The operations take place on the i500 Solaris host and not the Policy Director AIX host. Since i500 is already configured, Section 6.4.1, Steps 1 to 5, are not appropriate. Instead, perform the following operation on the i500 host:

- Copy/append the $ODSRELEASE/<dsa-name>/oidslocal to $ODSRELEASE/scripts.
Important Supplemental Information

**Configuring the IBM LDAP client**

Follow Section 6.5 in the *Tivoli SecureWay Policy Director 3.7 Base for Solaris Installation Guide*.

**Synchronizing LiveContent Schemas**

Follow Section 6.6 in the *Tivoli SecureWay Policy Director 3.7 Base for Solaris Installation Guide*. The DAC files can be copied from either:

- `/opt/PolicyDirector/i500_external/lib`
- `<any-i500-host-directory>/i500_external/lib`

**Configuring Policy Director on AIX**

Policy Director can now be configured on the AIX machine according to Chapter 7 of the *Tivoli SecureWay Policy Director 3.7 Base for AIX Installation Guide*.

All components except PDAcld can be configured at this time. Before PDAcld can be configured correctly, PDMgr must be fully configured on the i500 host.

If configuration completes successfully, a file `/tmp/aaa_details.cfg` is created. This file contains the passwords of the Policy Director security daemons and therefore contains only read and write permissions for “root”. This file must be transferred to the i500 host machine for configuration to continue.

**Configuring Policy Director on the i500 Host**

1. Go to the directory:
   `<any-i500-host-directory>/i500_external/bin`

2. Enter the following:
   ```
   perl i500_ext_config -h <hostname> -p <LDAP-port#> -P <DAP-port#> -D <i500-admin-DN> -w <i500-admin-pwd>
   ```

   The following menu appears:

   **Policy Director i500 External Configuration**
   1. Add Access Control Information to Policy Director DIT
   2. Remove Access Control Information from Policy Director DIT
   3. Add Server Daemons as Administrative Agents
   4. Remove Server Daemons as Administrative Agents
   5. Delete AAA file
   6. Exit

   Select menu entry:
3. Select entry 1. The following request appears:

   Enter Distinguished Name of GSO suffix:

4. Enter the name of the GSO suffix that was entered for the same request during the Policy Director configuration. When the operation is complete the menu reappears.

5. Select entry 3. The following request appears:

   Enter directory/filepath of AAA file:

6. Enter the name and path of the file copied from /tmp/aaa_details.cfg on the AIX host. The default is the same filepath.
   The contents of this file are the DNs and passwords of the servers that were configured on the AIX machine. When the operation is complete, the menu reappears.

7. Select entry 5. The following request appears:

   Enter directory/filepath of AAA file:

8. Re-enter the name of the aaa_details.cfg file.
   The file will be deleted for security. When the operation is complete the menu reappears.

9. Select entry 6 to exit the configuration tool.
   It is now safe to configure PDAcl on the AIX host or configure other Policy Director blades on other hosts if required.

**Unconfiguring Policy Director on AIX**

Policy Director can be unconfigured on the AIX host according to Chapters 7 in the *Tivoli SecureWay Policy Director 3.7 Base for AIX Installation Guide*.

When unconfiguration completes successfully, the file /tmp/aaa_details.cfg is created. This file must be transferred to the i500 host machine for unconfiguration to continue.
Unconfiguring Policy Director on the i500 Host

1. Go to the directory:
   `<any-i500-host-directory>/i500_external/bin`

2. Enter the following:
   ```
   Perl i500_ext_config -h <hostname> -p <LDAP-port#> -P <DAP-port#> -D <i500-admin-DN> -w <i500-admin-pwd>
   ```
   The following menu appears:
   Policy Director i500 External Configuration
   1. Add Access Control Information to Policy Director DIT
   2. Remove Access Control Information from Policy Director DIT
   3. Add Server Daemons as Administrative Agents
   4. Remove Server Daemons as Administrative Agents
   5. Delete AAA file
   6. Exit
   Select menu entry:

3. Select entry 2.
   When the operation is complete the menu reappears.

4. Select entry 4. The following request appears:
   Enter directory/filepath of AAA file:

5. Enter the name and path of the file copied from `/tmp/aaa_details.cfg` on the AIX host. The default is the same filepath.
   The contents of this file are the DNs of the servers that were configured on the AIX machine. When the operation is complete, the menu reappears.

6. Select entry 5. The following request appears:
   Enter directory/filepath of AAA file:

7. Re-enter the name of the `aaa_details.cfg` file.
   The file is deleted for security. When the operation is complete, the menu reappears.

8. Select entry 6 to exit the configuration tool.
   Policy Director or any component of Policy Director is now unconfigured.
4 Corrections to the January 2001 Documentation

- Corrections to the Installation Guides
- Corrections to the Base Administration Guide
- Corrections to the WebSEAL Administration Guide
- Corrections to the WebSEAL Developer Reference
- Corrections to the Console Administration Guide
Corrections to the January 2001 Documentation

**Corrections to the Installation Guides**

- 4.1 - Incorrect SSL Certificate File Name
- 4.2 - Base Installation Guides: Revised Section 4.4.3

### 4.1 Incorrect SSL Certificate File Name

The installation guides for Policy Director 3.7 Base for AIX, Solaris, HP-UX, and Windows contain the incorrect file name for the text file that stores the SSL certificate that is created and configured during installation of the Policy Director Management Server.

The correct name is:

```
pdcacert.b64
```

**not:**

```
pdacert.b64.
```

The complete path for the file is:

**Solaris, AIX, and HP-UX:**

```
/opt/PolicyDirector/ivmgrd/keytabs/pdcacert.b64
```

**Windows:**

```
C:\Program Files\Tivoli\Policy Director\ivmgrd\keytabs\pdcacert.b64
```

### 4.2 Base Installation Guides: Revised Section 4.4.3

**Summary:**

The contents of Section 4.4.3 in each of the Policy Director Base Installation Guides have been revised. Replace Section 4.4.3 with the information below entitled:

- **4.4.3 Adding ACLs to Policy Director Suffixes**

**Explanation:**

Each of the Policy Director Base Installation Guides contains a Chapter 4, entitled “Configuring IBM LDAP”. This chapter describes how to specify
certain Policy Director information for use with IBM SecureWay Directory servers. The instructions in this chapter are performed prior to the installation and configuration of the Policy Director servers.

Chapter 4 contains Section 4.4.3 “Adding the Policy Director Group to LDAP ACLs”. The section describes how to make Policy Director the owner of the Policy Director suffixes in the LDAP Directory Information Tree (DIT).

The instructions in Section 4.4.3 have been revised. Policy Director does not need to be the owner of the Policy Director suffixes. Policy Director can make full use of LDAP without being the owner of the Policy Director suffixes.

If Policy Director owns the suffixes, there could be future LDAP administration difficulties. For example, if the Policy Director servers are removed prior to the removal of the suffixes from the DIT, the LDAP administrator would not have complete control over the remaining suffixes.

Replace the entire Section 4.4.3 with the following text:

4.4.3 Adding ACLs to Policy Director Suffixes

When Policy Director is configured, it automatically attempts to add appropriate ACLs to every suffix in the LDAP Server, in order to allow Policy Director to create and update user and group information within those suffixes.

However, for any suffixes which the LDAP administrator adds after the initial configuration of Policy Director, the administrator must add the appropriate ACLs manually.

For instructions on adding appropriate ACLs to suffixes after Policy Director has been configured, see the following Policy Director 3.7 Release Note section:

3.9 - Applying Policy Director ACLs to New LDAP Suffixes.
Corrections to the January 2001 Documentation

Corrections to the Base Administration Guide

- 4.3 - Time-of-Day POP Attribute
- 4.4 - Traverse Permission
- 4.5 - Directing Messages to Standard Output - Debug Mode

4.3 Time-of-Day POP Attribute

The following note is a point of clarification for Section 4.2.3 of the Tivoli SecureWay Policy Director Base Administration Guide:

The optional time zone parameter (representing the time zone of the Policy Director server) is set to local by default.

4.4 Traverse Permission

Note: The following information replaces the text and graphic found in Section 3.5.3 of the Tivoli SecureWay Policy Director Base Administration Guide. Section 3.7.2 of the same document should also be modified accordingly.

Policy Director access control depends on two conditions.

1. The ACL that controls the requested object must contain appropriate access permissions for the requesting user.
2. The requested object must be accessible to the requesting user.
   Accessibility to protected objects is controlled by the traverse (T) permission.

The traverse permission is only applied to container objects in the WebSEAL protected object space. The traverse permission specifies that a user, group, any-authenticated, or unauthenticated identified in the ACL entry has permission to pass through this container object in order to gain access to a protected resource object below in the hierarchy.

A protected object is accessible to a requester if the requester possess the traverse permission on each ACL attached to container objects above the requested resource on the path towards root and including root.
The following example illustrates how the traverse permission works. Within the ACME Corporation, there is an Engineering container object (directory), which also contains a TechPubs container object (sub-directory). User kate, a member of the Sales department, requires traverse to the Engineering/TechPubs directory to review a release note file.

The administrator provides traverse for any-authenticated at the root. The administrator provides traverse for group sales on the Engineering directory. The TechPubs directory inherits the ACL from the Engineering directory. Although Kate has no other permissions in these two directories, she can pass (traverse) through these directories in order to access the release_note file. Because this file has read permission for user kate, she can view the file.

Figure 4-1: Traverse Permission

You can easily restrict access to the hierarchy below a given container object — without resetting individual permissions on these objects. Simply remove the traverse permission from the appropriate ACL entry. Removing traverse permission on a directory object protects all objects lower in the hierarchy, even if those objects contain other less restrictive ACLs.

For example, if group sales did not have the traverse permission on the Engineering directory, Kate could not access the release note file, even though she has read permission for the file.
4.5 Directing Messages to Standard Output - Debug Mode

The command option for directing warning and error messages to standard output, as stated in section 8.2.3 of the Policy Director 3.7 Base Administration Guide is incorrect. The correct option is `-foreground` (not `-debug`):

```
# /opt/PolicyDirector/secmgr/bin/secmgrd -foreground
```
Corrections to the WebSEAL Administration Guide

4.6 Updating WebSEAL for Dynamic URLs (WebSEAL 6.3.3)

The path name for locating the WebSEAL server when using the `dynurlcp` utility—as stated in Section 6.3.3 of the January 2001 Tivoli SecureWay Policy Director WebSEAL Administration Guide—is incorrect. Change the `PolicyDirector` directory to `intraverse`:

```
dynurlcp -e /:.:/subsys/intraverse/secmgr/server/<host> update
```

4.7 WebSEAL Personalization Junction (WebSEAL 5.7)

The HTTP header variable—specified as `HTTP_PD_PORTAL` in Section 5.7 of the January 2001 Tivoli SecureWay Policy Director WebSEAL Administration Guide—is incorrect. The variable is `PD_PORTAL`.

In addition, the second comment in the Notes of Section 5.7.2:

“Mapping the same back-end URL to multiple object:permission pairs in the configuration file results in a concatenated list of objects.”

is not true.

4.8 WebSEAL Only Supports HTTP/1.0 Across Junctions

The table in Section 5.1.2 of the Tivoli SecureWay Policy Director WebSEAL Administration Guide contains the incorrect RFC numbers for the supported protocols. The following table contains the correct references:

<table>
<thead>
<tr>
<th>Connection</th>
<th>Supported Protocol</th>
<th>RFC Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Front-end</td>
<td>HTTP/1.0 and HTTP/1.1</td>
<td>RFC2068</td>
</tr>
<tr>
<td>(client-to-WebSEAL)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4.9  **GSKit Session ID Timeout Parameters**

Section 2.3 of the January 2001 *Tivoli SecureWay Policy Director WebSEAL Administration Guide* (“Configuring Timeout Values”) incorrectly categorizes and defines the `ssl-v2-timeout` and `ssl-v3-timeout` parameters.

These two parameters are not timeout parameters for HTTP/HTTPS connections. Instead, they are parameters that define the lifetime of session IDs in the GSKit session ID cache. The value set for one of these parameters, combined with the rate of authentication, determines how fast the GSKit session cache fills up. Both parameters are located in the `[ssl]` stanza of the `secmgrd.conf` configuration file:

The discussion of these parameters is more appropriate under section 4.2: “Managing Session States.”

- **ssl-v2-timeout**
  For SSL v2 communication, this parameter defines the length of time a session ID can remain in the GSKit session cache. Default value is 100 (seconds).

- **ssl-v3-timeout**
  For SSL v3 communication, this parameter defines the length of time a session ID can remain in the GSKit session cache. Default value is 7200 (seconds).

### 4.10  Correction to `ssl-cache-inactive-timeout` Text (IY21674)

The `ssl-cache-inactive-timeout` parameter is appropriate for Forms login, client-side certificates, and Basic Authentication.
Corrections to the WebSEAL Developer Reference

4.11 Deploying the Template CDAS Server (Section 4.4)

Note: The following material clarifies the instructions in the original document. This section is relevant to developing a customized CDAS server.

Amend Section 4.4 of the Tivoli SecureWay Policy Director WebSEAL Developer Reference (“Configuring WebSEAL to Use the Template CDAS Server”) as follows:

Section 4.4.1
The template CDAS server is demonstration code only. It is hard-coded to recognize the cdas_test user (password: “tivoli”) and map this user to the Policy Director test-user.

1. Follow original instructions.
2. Follow original instructions.
3. Create a test ACL policy based on the default-webseal ACL. This ACL policy should contain an entry for the test user with the T, r, and x permissions granted.
4. Attach this test policy to some object in the WebSEAL object space.
5. Continue to Section 4.4.2 to test the ability of the CDAS server to access this protected object.

Section 4.4.2
1. Follow original instructions.
2. Test the CDAS server by accessing the protected object using:
   Username: cdas_test
   Password: tivoli
3. The template CDAS server should successfully map this user to the test_user Policy Director identity and allow you to access the protected object.
Corrections to the Console Administration Guide

4.12 - Management Console Administration Guide Corrections

4.12 Management Console Administration Guide Corrections

The Management Console online help system contains a list of corrections to the Console documentation.
5 Software Limitations

- 5.1 - NetSEAL Kernel Trap is Not Supported on SMP Systems
- 5.2 - NetSEAL and NetSEAT Backward Compatibility
- 5.3 - pdadmin Functionality Not Available on the Management Console
- 5.4 - Language Limitations Involving Double-byte Characters
- 5.5 - LDAP Does Not Treat User Names as Case-sensitive
- 5.6 - pdconfig Utility May Fail on Japanese HP-UX Systems
- 5.7 - Management Console Online Help Inconsistencies
- 5.8 - Untranslated Graphs Used in Translated Console Online Help
- 5.9 - pdadmin policy set min-password-reuse-num (IY18451)

5.1 NetSEAL Kernel Trap is Not Supported on SMP Systems
The NetSEAL kernel trap is not supported on Symmetric Multiprocessor Systems (SMP) systems.
Do not enable the kernel trap when configuring PDNet on multiprocessor systems.

5.2 NetSEAL and NetSEAT Backward Compatibility
NetSEAL 3.7 cannot be used with previous versions of the NetSEAT client.

5.3 pdadmin Functionality Not Available on the Management Console
The following Policy Director 3.7 functions exist in the pdadmin utility but not in Management Console:
- Server management functions
- NetSEAL management
- ACL action/action group management
- Object space and object management
- Password policy management
- Delegated administration functions
- User and Group Import Commands
5.4 Language Limitations Involving Double-byte Characters

The following limitations and conditions apply when you run Policy Director in a non-English environment:

- When using Basic Authentication to authenticate to WebSEAL from a Netscape browser, you must limit the username and password to the portable character set (7-bit US-ASCII).

   For environments where user names include double-byte characters, set up WebSEAL to use Forms-based login for passing client identity information.

   When using Forms-based login, the code page used to create the form must be the same code page that WebSEAL is running in.

- If user data contains characters other than those in the portable character set (7-bit US-ASCII), you must ensure that all Policy Director components run using the same code page to properly share data among these components.

- Only the IBM SecureWay Directory can be used as the user registry when Policy Director is configured to run on a non-English platform and non-portable-character-set data creation is required.

- When creating a new junction with the junctioncp utility, the name of the junction point must be limited to the portable character set.

There are multiple code sets for each of the Asian languages. HTTP does not define which code set to use for URLs. Therefore, URLs that use any character codes other than the portable character set (7-bit US-ASCII) result in compatibility problems.

5.5 LDAP Does Not Treat User Names as Case-sensitive

This information applies to both IBM and Netscape LDAP.

Policy Director stores a user’s name in the principalName attribute of the secUser object in an LDAP registry.

The LDAP schema defines the principalName attribute as a case-insensitive string. The original case indicated in the user’s name is, however, preserved when the value is initially stored in the LDAP database.

Therefore, “Test User” is treated the same as “test user”.
5.6 pdconfig Utility May Fail on Japanese HP-UX Systems

If you are logged into a system using the ja_JP.SJIS locale or the ja_JP.eucJP locale, `pdconfig` may fail when you attempt to configure Policy Director. The workaround for this problem is to login to the system using the “C” locale and configure Policy Director using English.

If you use this workaround, Policy Director initially thinks it is running under the “C” locale. After logging out and logging back into the system, using either the ja_JP.SJIS or the ja_JP.eucJP locale, Policy Director should be stopped and restarted so that it can recognize the ja_JP.SJIS (or ja_JP.eucJP) locale.

This problem has been observed on HP-UX systems only.

5.7 Management Console Online Help Inconsistencies

Some inconsistencies exist between the online help documentation provided by the Management Console and the actual panels/tabs shown in the Console itself.

The first type of inconsistency is caused by the adoption of the latest Java swing class in the Console code. The screen captures (.gif files) used in the online help were obtained prior to that code change. The panel/tab outlook change resulting from this change is minor and should not cause any functional problems or confusion.

The second type of inconsistency occurs because the code base for the Console is Component Manager, a Tivoli project originally designed as a unified administration console framework for various products. Each product managed by Component Manager requires an adapter that is plugged in to the framework. Some functional panels/tabs shown in the online help reveal this plug-in capability of the Component Manager framework. However, the Management Console itself is actually a result of the Policy Director adapter and can only provide Policy Director-related functionality.
5.8 Untranslated Graphs Used in Translated Console Online Help

The Management Console online help (HTML files) and the messages used by the code are translated to nine languages. However, the graphs used in translated online help have not yet been translated. Currently, the English graphs are used.

5.9 pdadmin policy set min-password-reuse-num (IY18451)

By design, the pdadmin policy set min-password-reuse-num command is not available for Policy Director WebSEAL. This command was originally part of the policy management command set that was specifically for use by the IBM SecureWay Boundary Server.
6 Known Software Defects and Workarounds

- Installation and Upgrade Defects and Workarounds
- Base Defects and Workarounds
- WebSEAL Defects and Workarounds
- NetSEAL Defects and Workarounds
- Management Console Defects and Workarounds
- LDAP Defects and Workarounds
Installation and Upgrade Defects and Workarounds

- 6.1 - Upgrading Policy Director 3.6 WebSEAL
- 6.2 - IBM SecureWay Directory 3.2 Requires AIX 4.3.3 Patches
- 6.3 - IBM SecureWay Directory DMT Utility Fails to Start
- 6.4 - NetSEAT Installation Requires GSKit 4.0 (IY22179)

6.1 Upgrading Policy Director 3.6 WebSEAL

Note: This problem occurs on Solaris, AIX, and HP-UX systems. This problem does not occur on Windows systems.

Problem:

When configuring a Policy Director 3.7 WebSEAL server during an upgrade from Policy Director 3.6, the WebSEAL server might fail to start. The following error message might appear:

symbol IV_UraF: referenced symbol not found

Explanation:

If any Policy Director 3.6 server processes are still running when the Policy Director 3.7 WebSEAL server attempts to start, the new WebSEAL server might access a Policy Director 3.6 shared library that is cached in memory. The Policy Director 3.6 shared library does not contain all the library routines required by the Policy Director 3.7 WebSEAL server. This prevents the new WebSEAL server from starting.

This problem can also occur if any Policy Director 3.6 Authorization API Client programs are running when the Policy Director 3.7 WebSEAL server attempts to start.

Workaround:

If you encounter this error during the Policy Director 3.7 WebSEAL server configuration, complete the following steps:

1. Exit the Policy Director Configuration Menu by selecting “x”.
2. Exit the Policy Director Setup Menu by selecting “x”. 
3. Stop all Policy Director servers and client programs that use the Policy Director 3.6 Authorization API. To stop Policy Director servers, enter the following commands:
   - **AIX**
     # /etc/iv/iv stop
   - **Solaris**
     # /etc/init.d/iv stop
   - **HP-UX**
     # /sbin/init.d/iv stop

4. Verify that the Policy Director 3.6 authorization library is installed, and remove it:
   - **AIX**
     # ls -l /usr/lib/libivauthzn.a
     # rm -f /usr/lib/libivauthzn.a
   - **Solaris**
     # ls -l /usr/lib/libivauthzn.so
     # rm -f /usr/lib/libivauthzn.so
   - **HP-UX**
     # ls -l /usr/lib/libivauthzn.sl
     # rm -f /usr/lib/libivauthzn.sl

5. Create a symbolic link with the new Policy Director 3.7 authorization library:
   - **AIX**
     # ln -s /opt/PolicyDirector/lib/libivauthzn.a /usr/lib/libivauthzn.a
   - **Solaris**
     # ln -s /opt/PolicyDirector/lib/libivauthzn.so /usr/lib/libivauthzn.so
   - **HP-UX**
     # ln -s /opt/PolicyDirector/lib/libivauthzn.sl /usr/lib/libivauthzn.sl

6. Restart the Policy Director servers (and any Authorization API clients):
   - **AIX**
     # /etc/iv/iv start
   - **Solaris**
     # /etc/init.d/iv start
7. Start the Policy Director configuration utility:
   # pdconfig
8. Select **Policy Director Configuration**.
9. Select **Policy Director WebSEAL (PDWeb) Configuration**.
10. Complete the WebSEAL configuration, as prompted.

**Solution:**
To prevent this problem from occurring, manually stop the Policy Director 3.6 WebSEAL server when preparing the Policy Director 3.6 system for an upgrade to Policy Director 3.7.

Perform this action *after* backing up the Policy Director 3.6 ACL database and WebSEAL junction database.

**Note:** If the Policy Director 3.6 system has a NetSEAL server, remove the NetSEAL server before stopping the other Policy Director 3.6 servers.

To stop the WebSEAL server on AIX systems, enter the following command at a shell prompt:

# /etc/iv/iv stop

To stop the WebSEAL server on Solaris systems, enter the following command at a shell prompt:

# /etc/init.d/iv stop

To stop the WebSEAL server on HP-UX systems, enter the following command at a shell prompt:

# /sbin/init.d/iv stop
6.2 IBM SecureWay Directory 3.2 Requires AIX 4.3.3 Patches

Problem:
On AIX systems only, IBM SecureWay Directory 3.2 installation fails because prerequisite AIX operating system software is not installed.

Explanation:
Policy Director 3.7 supports LDAP user registries. Policy Director users can choose to install IBM SecureWay Directory Version 3.2 to provide LDAP user registry support. SecureWay Directory Version 3.2 is included on the Policy Director Base CDs.

On AIX only, SecureWay Directory Version 3.2 is dependent on a number of AIX operating system patches that are not part of the file sets installed by default during AIX 4.3.3 installation. If any of these dependencies are missing, the SecureWay Directory Version 3.2 installation fails.

Solution:
1. Before installing SecureWay Directory Version 3.2, use the `smit` utility to verify that the following patches are installed:
   - X11.Dt.lib 4.3.3.2
   - X11.Dt.rte 4.3.3.3
   - X11.adt.motif 4.3.3.1
   - X11.base.lib 4.3.3.2
   - X11.base.rte 4.3.3.2
   - X11.compat.lib.X11R5 4.3.3.2
   - X11.motif.lib 4.3.3.2
   - X11.motif.mwm 4.3.3.1
   - bos.adt.include 4.3.3.1
   - bos.adt.prof 4.3.3.3
   - bos.net.tcp.client 4.3.3.3
   - bos.rte.libpthread 4.3.3.3
   - bos.sysmgmt.serv_aid 4.3.3.2
   - bos.mp 4.3.3.3
   - bos.up 4.3.3.3
2. Use `smit` to install any missing patches.

### 6.3 IBM SecureWay Directory DMT Utility Fails to Start

**Problem:**

**Platform:** AIX only

The first time a user configures IBM SecureWay Directory Version 3.2, the Directory Management Tool (DMT) might fail to start. This failure prevents the update of LDAP ACLs that control the user registry. This configuration step is described in Section 4.4.1 and Section A.7.3 of the *Tivoli SecureWay Policy Director Base for AIX Installation Guide*.

**Explanation:**

The DMT utility is part of IBM SecureWay Directory Version 3.2. IBM SecureWay Directory is included on the Policy Director 3.7 Base for AIX CD. Policy Director users who want to use an LDAP user registry often install IBM SecureWay Directory as prerequisite software for Policy Director.

The DMT utility depends on the AIX 4.3.3 operating system file set `X11.adt.lib`. The `X11.adt.lib` file set is not included in the SecureWay Directory .TOC file that specifies the required software dependencies (file sets). Thus, the IBM SecureWay Directory Version 3.2 installation completes despite missing a software dependency.

**Solution:**

1. Use the `smit` utility to install the AIX 4.3.3 file set `X11.adt.lib`.

2. Restart the DMT utility.

### 6.4 NetSEAT Installation Requires GSKit 4.0 (IY22179)

IBM GSKit version 4.0 must be installed prior to installing Policy Director 3.7.1 NetSEAT client. This information was not included in the *Tivoli SecureWay Policy Director 3.7 NetSEAL Installation Guide*.
Base Defects and Workarounds

- 6.5 - Configuring the Management Server on Solaris
- 6.6 - LDAP 3.1.x to LDAP 3.2 Migration Procedure Revisions
- 6.7 - IBM DCE 3.1 Patch 3 Solves Management Server Memory Leak
- 6.8 - Correction to set min-password-alphas Help Message (IY18408)

6.5 Configuring the Management Server on Solaris

Problem:
This problem is Solaris-specific. The Policy Director Management Server (ivmgrd), configured for SSL, fails to start when the LDAP server is on the same host.

To properly authenticate over SSL, the Management Server must be able to read the /opt/ibm/gsk4/bin/ldapsslclient.kdb key database file. This file has read/write permissions only for the root user, who initially created the file. When the Management Server starts, it runs as user ivmgr. The ivmgr user does not have read permission on the file.

Workaround:
Change the ownership of the ldapsslclient.kdb file to user ivmgr.

6.6 LDAP 3.1.x to LDAP 3.2 Migration Procedure Revisions

This information discusses problems with existing IBM SecureWay Directory (LDAP) documentation as it pertains to the process of upgrading from Policy Director 3.6 to Policy Director 3.7. The primary issue discussed here is preserving the LDAP schema.

Note: This discussion is based on the Windows NT platform. However the issues and corrections described are also appropriate for UNIX platforms.

1. The LDAP Server Version 3.2 Readme document specifies a document that describes LDAP 3.1.1.5 migration to LDAP 3.2.
2. This document is entitled *Directory version 3.2 Installation and Configuration Guide for Windows NT* and is located on the IBM support site at:


3. Click on the section entitled “Installation, Configuration, and Migration”. The full link is now:


4. Expand the table of contents for this section and click on “Migration”.

5. Scroll down to the sub-section entitled “Migrating with the Existing Schema and Database Preserved”. This procedure is required when migrating from Policy Director 3.6 to 3.7.

6. Steps 1 and 2 are correct. Stop LDAP and the DB2 instance.

7. Step 5 suffers from no information about stopping replicas in the correct order.

   It should also say that LDAP 3.2 is installed directly over 3.1.1.5.

8. The paragraph following step 6 suggests that “the schema content is updated”.

   This conclusion is in conflict with the title of the section, “Migrating with the Existing Schema and Database Preserved”. In fact, Policy Director does not work after the schema is altered. Therefore the following additional step is required (based on the copy commands in step 3 of the following section, “Migrating from V3.1 to V3.2”):

9. Reinstate the schema, with the following command:

   ```
   MSDOS> copy <install_directory>\etc\ldapV31\V3.modifiedschema <install_directory>\etc
   ```

10. Verify with the DMT tool that the data is still available in the upgraded LDAP.

**Comments:**

- This discussion was Windows-specific. However, the problem is probably the same for UNIX.
- Data for the Solaris platform must be manually saved.
6.7 IBM DCE 3.1 Patch 3 Solves Management Server Memory Leak

**Problem:**

The following problem applies to Policy Director 3.7 on Solaris, when used with IBM DCE 3.1.

Modifying policy using an administration tool such as `pdadmin` or the Management Console can cause a memory leak in the Management Server (`ivmgrd`).

**Solution:**

The memory leak can be fixed by installing a patch to IBM DCE 3.1. Obtain and install Patch 3 (IDCE31-03) for IBM DCE 3.1.

IBM DCE software home page:


Patch Set 3:


6.8 Correction to set min-password-alphas Help Message (IY18408)

The Help message for `pdadmin policy set min-password-alphas` states:

“Set the minimum number of alphanumeric characters in a user’s password.”

The word “alphanumeric” should be “alphabetic” (letters only).

The same problem and correction exists for `pdadmin policy set min-password-non-alphas`. 
Known Software Defects and Workarounds

WebSEAL Defects and Workarounds

- 6.9 - Additional WAP Gateway Support
- 6.10 - Deleted User Credentials Remain in WebSEAL Cache
- 6.11 - Certificate Authentication for CDSSO Causes WebSEAL Failure
- 6.12 - Forms Re-login Can Result Loss of POST Data (IY21348)

6.9 Additional WAP Gateway Support

When you use WebSEAL to communicate exclusively with another proxy or gateway server, you can take advantage of the HTTP over SSL authentication methods supported by WebSEAL.

This approach can be useful, for example, when you want to provide authorization services in the WAP environment.

1. Enter the following configuration parameter in the [wand] stanza of the iv.conf configuration file:
   
   use-http-auth-for-ssl = yes

2. Configure the enable-http-auth-forms parameter to specify whether to use Basic Authentication or Forms-based login.

   Use the [http-auth-headers] stanza in the iv.conf configuration file to specify any special HTTP headers to use as authentication data.

   When you set up WebSEAL in this mode, WebSEAL will ignore the SSL session ID and instead use the standard HTTP session management mechanisms. Refer to the Tivoli SecureWay Policy Director WebSEAL Administration Guide for detailed information about these authentication mechanisms.

6.10 Deleted User Credentials Remain in WebSEAL Cache

Problem:

When you delete a user from the user registry (DCE or LDAP), the user’s credentials in the WebSEAL credentials cache (if there are any) do not get removed.
Note: The purpose of the cache is to limit calls to the user registry.

If the user has a browser session active at the time the account is deleted, the user can continue to browse, based on the undeleted credentials.

Only the registry is affected when a user is deleted. In an active browser session, the registry is not queried if there is a legitimate credential available for that user. A registry look-up (to reveal the deleted account) only occurs with a new login or when the current credentials expire.

Workaround:

Once the user logs out of a browser session, the credentials in the cache are cleared.

If you, as the security administrator, require an immediate halting of user activity in the secure domain, you can add an entry to the default WebSEAL ACL policy for the specific user, with the traverse (T) permission removed.

6.11 Certificate Authentication for CDSSO Causes WebSEAL Failure

Problem:

In a CDSSO environment, if a client authenticates to domain A via a client-side certificate and then activates a link to domain B, excessive growth of the secmgrd (WebSEAL) process occurs due to a memory leak.

Workaround:

Clients who want to utilize CDSSO functionality should not authenticate to the initial domain via client-side certificates. For example, Basic Authentication and Forms-based login are acceptable authentication methods.

Please check with Tivoli Support for a fix pack that will allow authentication via client-side certificates.
6.12 Forms Re-login Can Result Loss of POST Data (IY21348)

Background:
When an unauthenticated client browser makes an HTTP request to a WebSEAL server (configured for Forms login), WebSEAL receives the request, generates a session ID, creates a cache entry using the session ID, stores the requested URL in the cache entry, and sends back an HTML login form.

The user supplies the login information and submits the data to WebSEAL. In the current implementation of Forms login, WebSEAL only caches the URL of the request that triggered the authentication process.

Problem:
The following example illustrates the inconvenience caused to a user when a forced Forms re-login causes the loss of POST data. In this example, the user is researching the information required to complete a lengthy form submitted by an application. The session inactivity timeout value is exceeded.

When the user finally submits the form, WebSEAL determines that reauthentication is required (due to the session inactivity timeout) and sends a Forms login prompt. Because WebSEAL only caches the URL of the request that triggered the authentication process, the Message body (that includes all the form data) is lost.

If the browser has caching enabled, it might be possible to recover the form data when the Back button is used. Otherwise, the user must re-enter the form data.

Workaround:
In general, application servers should not send data forms until after the authentication process is complete.

The only workaround for the session inactivity timeout scenario is to enable browser caching.
NetSEAL Defects and Workarounds

- 6.13 - AIX Trap Defect
- 6.14 - Solaris Patch Requirements

6.13 AIX Trap Defect

There is an outstanding defect with the AIX kernel trap. You cannot configure NetSEAL to trap ephemeral ports (for example, ports in the range 1025-5000).

If you configure NetSEAL to trap an ephemeral port, all outgoing network connections fail, rendering the server useless.

6.14 Solaris Patch Requirements

The NetSEAL trap requires the latest O/S patches on Solaris.

The O/S patches can be located at:

http://sunsolve.Sun.COM

Look under Sunsolve contents, “Recommended and Security patches”.
6.15 Management Console Defects and Workarounds

The following limitations and conditions apply when you run the Policy Director Management Console for Windows:

- For an LDAP user registry, the Account Manager cannot copy and paste users from either the Users container or a group to another group. The workaround is to drag and drop users.

- For an LDAP registry, the Account Manager view—when in the Create GSO Resource Group or GSO Resource Group Properties views and clicking on the “...” button—should bring up the GSO Resources view. However, the GSO Resource view does not list any resources. The workaround for this problem is to drag and drop resources from the GSO Resource container.

- For a DCE registry, the DCE SecRgy view causes the Console to abort when bringing up the Permissions view. Selecting either Group or Principals, right-clicking, and clicking on Add can also cause the Console to abort.

In addition, some of the help documents are either missing or not updated (not re-branded).

- The Refresh button requires that a container object be selected for it to have an effect. Otherwise, no refresh action will be performed.

- For a DCE registry, the Entry and Object tabs are the same in the Edit Principal view.

- The Object pull-down menu in the Account Manager view should be disabled. It does not provided any menu selection items for this view. Previously, it only listed the Custom Commands option which is not supported and has been removed.

- The Console may hang while attaching an ACL or a POP to an object or detaching an ACL from an object in the Object Space view. The action appears to be completed successfully. The workaround for the hang is to restart the Console.

- The Console sometimes aborts immediately when started. The workaround is to log out and log in again.
Known Software Defects and Workarounds

- The Console must be restarted to see action group changes (such as adding or removing permission bits).
- If PDRTE is reconfigured to use a different user registry type (for example, switching from a DCE user registry to an LDAP user registry), the Console must be reinstalled.
6.16 WebSEAL Can Become Unstable with LDAP Configuration

Background:
For IBM LDAP, Policy Director supports an option for improved authentication performance through the auth-using-compare parameter located in the [ldap] stanza of the iv.conf configuration file.

This option does not work with Netscape LDAP and is therefore ignored by WebSEAL. Documentation of this parameter appears in Section 4.2 of the Tivoli SecureWay Policy Director Performance Tuning Guide.

The default value for auth-using-compare is “yes”. With IBM LDAP, WebSEAL can use this parameter and perform as expected.

Problem:
However, when auth-using-compare is set to “no” with IBM LDAP, WebSEAL can become unstable under heavy authentication loads.

In addition, the same defect causes WebSEAL to become unstable under heavy authentication loads when Policy Director is configured with Netscape LDAP, even though the auth-using-compare parameter is ignored.

The common problem involves the IBM LDAP 3.2 client used by Policy Director 3.7.

Workaround:
This problem is fixed by installing the IBM LDAP 3.2.1 client on the WebSEAL machine. You can download the IBM LDAP 3.2.1 client from the IBM SecureWay Directory Web site:

http://www.software.ibm.com/enetwork/directory/

From the links listed on the left side of the page, click Download.