Updated May 25, 2001

Tivoli® SecureWay®

PDOS Release Notes

Version 3 Release 7

PDOS Release Notes (May 2001)

Copyright Notice

Trademarks

Notices

Contents

1

PDOS Release Notes

Tivoli SecureWay Policy Director for Operating Systems (PDOS) functions within a Tivoli SecureWay Policy Director environment in order to provide an additional layer of security on top of the native system's security. PDOS enhances security by enforcing authorization policy beyond the native system's security capability. PDOS runs on AIX®, HP-UX, and Solaris.

Tivoli SecureWay Policy Director for Operating Systems (PDOS), Version 3.7 is available as part of the Tivoli SecureWay Security Manager, Version 3.7.1 release. The Tivoli SecureWay Security Manager 3.7.1-SEC-0002 patch contains enhancements and updates for PDOS Version 3.7.

The *PDOS Release Notes* contain important information about PDOS Version 3.7 and describe the enhancements contained in the 3.7.1-SEC-0002 patch. The PDOS enhancements and updates contained in the 3.7.1-SEC-0002 patch are collectively referred to as Fixpack 1 throughout these notes. These notes are also available at the following site:
http://www.tivoli.com/support/Prodman/html/AB.html#Security.

About These Release Notes

These notes have been updated as of May 25, 2001. Some PDOS Version 3.7 information has been revised, and new information about the PDOS 3.7 Fixpack 1 has been added. For a summary of the PDOS 3.7 Fixpack 1 release, see "PDOS 3.7 Fixpack 1" on page 5. For detailed information about individual new features or procedures:

- See "Installing PDOS 3.7 Fixpack 1 Using Native Install" on page 41.
- See "Login Activity Policy for PDOS" on page 5.
- See "Revised Reference Page for pdoslpadm Command" on page 7.
- See "PDOS Auditing" on page 12.
- "Internationalization" on page 53

Contents of These Release Notes

These release notes include the following sections:

Additional Information

The following sections describe how to access publications online, order publications, provide feedback about publications and contact customer support.

Accessing Publications Online

The Tivoli Customer Support Web site (http://www.tivoli.com/support/) offers a guide to support services (the *Customer Support Handbook*); frequently asked questions (FAQs); and technical information, including release notes, user's guides, redbooks, and white papers. You can access Tivoli publications online at http://www.tivoli.com/support/documents/. The documentation for some products is available in PDF and HTML formats. Translated documents are also available for some products.

To access most of the documentation, you need an ID and a password. To obtain an ID for use on the support Web site, go to http://www.tivoli.com/support/getting/.

Resellers should refer to http://www.tivoli.com/support/smb/index.html for more information about obtaining Tivoli technical documentation and support.

Business Partners should refer to "Ordering Publications" for more information about obtaining Tivoli technical documentation.

Ordering Publications

Order Tivoli publications online at http://www.tivoli.com/support/Prodman/html/pub_order.html or by calling one of the following telephone numbers:

- U.S. customers: **(800) 879-2755**
- Canadian customers: **(800) 426-4968**

Providing Feedback about Publications

We are very interested in hearing about your experience with Tivoli products and documentation, and we welcome your suggestions for

improvements. If you have comments or suggestions about our products and documentation, contact us in one of the following ways:

- Send e-mail to **pubs@tivoli.com**.
- Fill out our customer feedback survey at http://www.tivoli.com/support/survey/.

Contacting Customer Support

If you need support for this or any Tivoli product, contact Tivoli Customer Support in one of the following ways:

- Submit a problem management record (PMR) electronically from our Web site at http://www.tivoli.com/support/reporting/. For information about obtaining support through the Tivoli Customer Support Web site, go to http://www.tivoli.com/support/getting/.
- Submit a PMR electronically through the IBMLink™ system. For information about IBMLink registration and access, refer to the IBM Web page at http://www.ibmlink.ibm.com.
- Send e-mail to support@tivoli.com.
- Customers in the U.S. can call **1-800-TIVOLI8** (**1-800-848-6548**).
- Customers outside the U.S. should refer to the Tivoli Customer Support Web site at http://www.tivoli.com/support/locations.html for customer support telephone numbers.

When you contact Tivoli Customer Support, be prepared to provide the customer number for your company so that support personnel can assist you more readily.

PDOS Features

PDOS provides a layer of authorization policy enforcement in addition to that provided by the native operating system. An administrator defines additional authorization policy by applying fine-grained access controls that restrict or permit access to key system resources. Controls are based on user identity, group membership, the type of operation, time of the day or day of the

week, and the accessing application. An administrator can control access to specific file resources, login and network services, and changes of identity. These controls can also be used to manage the execution of administrative procedures and to limit administrative capabilities on a per user basis. In addition to authorization policy enforcement, PDOS provides mechanisms to verify defined policy and audit authorization decisions.

Access controls are stored in a policy database that is centrally maintained in the Policy Director environment. The accessing user definitions are stored in a user registry that is also centrally maintained in the environment. When protected resources are accessed, PDOS performs an authorization check based on the accessing user's identity, the action, and the resource's access controls to determine if access is permitted or denied.

PDOS 3.7 Fixpack 1

The following sections describe changes and new features available in the PDOS 3.7 Fixpack 1 release. For installation instructions, see "Installing PDOS 3.7 Fixpack 1 Using Native Install" on page 41. For information about language packages, see "Internationalization" on page 53.

Login Activity Policy for PDOS

PDOS now supports the ability to define and enforce policy related to login activity using **pdoslpadm** and the login_policy option of the **pdoscfg** configuration utility. For detailed information about login activity policy, refer to the Login Policy section of the PDOS Policy chapter in the *Tivoli SecureWay Policy Director for Operating Systems Administration Guide*. These release notes document the following new features:

- Login-MaxConcurrent Attribute
- User Exception Policy

Login-Max Concurrent Attribute

A new attribute called Login-MaxConcurrent has been added to the list of extended attributes that can be set for **/OSSEAL/policy-branch/Login** to control login activity policy.

The Login-MaxConcurrent attribute specifies the maximum number of terminals that can be logged in from concurrently by a specific user. A terminal is defined as a remote IP address or the local host. Multiple logins from the same terminal count as one login. If a value is specified for the default user, then the policy is applied to all the users on the system. If no value is specified, the default value of zero is assumed and the number of concurrent logins is not tracked. The Login-MaxConcurrent attribute type is a non-negative integer.

User Exception Policy

PDOS now provides the ability to define user exceptions to the default login activity policy. It is important to note that this is strictly provided as a mechanism to define exceptions to the default policy and is not encouraged for a large set of users.

The policy is defined by setting the login activity extended attributes on the **/OSSEAL/policy-branch/Login/UserExceptions/user-name** object, and only the attributes explicitly set for this object apply to the user.

Any login activity extended attribute value not explicitly set for the user-name object is set to a value of **0**. Unspecified attributes do not inherit the value from the default login activity extended attribute values.

UserExceptions policy cannot be specified as a task from Tivoli SecureWay Security Manager. It can only be done via the **pdadmin** command as shown below.

Examples of User Exception Policy for PDOS

The following are examples of setting user exception login policy for the policy-branch **Default**.

1. To set the default login activity policy to have user accounts set to inactive after **30** days of inactivity and to override this default policy for user **bob** to have all the login policy attributes set to **0** (disabling policy enforcement), use the following **pdadmin** commands:

```
pdadmin> object modify /OSSEAL/Default/Login set attribute \
 Login-MaxInactiveDays 30

pdadmin > object create /OSSEAL/Default/Login/UserExceptions/bob \
 "" 2 i yes
```

2. Extending the above example, to set bob's account to inactive state after **90** days of inactivity, you could use the following **pdadmin** command:

```
pdadmin > object modify /OSSEAL/Default/Login/UserExceptions/bob \
set attribute Login-MaxInactiveDays 90
```

3. All the login attribute values are single valued, so to reset the inactivity period for **bob** in the above example to **70**, use the following **pdadmin** commands:

```
pdadmin > object modify /OSSEAL/Default/Login/UserExceptions/bob \
 delete attribute Login-MaxInactiveDays

pdadmin > object modify /OSSEAL/Default/Login/UserExceptions/bob \
 set attribute Login-MaxInactiveDays 70
```

Revised Reference Page for pdoslpadm Command

The **pdoslpadm** command reference documentation on page 108 of the *Tivoli SecureWay Policy Director for Operating Systems Administration Guide* should be replaced by the following text. Please note that the format of this revised text may not exactly match the format of the book.

pdoslpadm

Purpose

Perform administrative commands pertaining to the PDOS Login Activity Database.

Syntax

pdoslpadm [-hvq?]

-c {on|off}

-r [-f] [-e|-d] [user [user ...]]

-m user [password-change-date]

-p [user [user ...]]

-x user [user [user ...]]

-l user [user [user ...]]

-u [-z] user [user [user ...]]

Description

The **pdoslpadm** command aids in the administration of PDOS Login and Password Activity Policy local to a native UNIX system. After login policy has been configured on a PDOS system, login and password policy records will be recorded for each user. Records are generated for each individual user account as each user logs into each PDOS system.

Use the **-c** option to enable or disable enforcement of PDOS Login Activity Policy on the local UNIX system.

Use the **-r** option to generate a report detailing the status of the native UNIX user accounts that are recorded in the PDOS Login Activity Database. If one or more users is specified along with the **-r** option, only the specified users' accounts are included in the report. If no users are specified with the **-r** option, all user accounts are included in the report. The **-e** option may be combined with the **-r** option to generate a report of only those user accounts that are enabled (unlocked). The **-d** option may be combined with the **-r** option to generate a report of only those user accounts that are

disabled (locked). The **-f** option may be combined with the **-r** option to generate a full or more detailed report.

Use the **-m** option to modify the time of the Password Change Date recorded in the PDOS Login Activity Database for the specified user. If no password-change-date is specified, the current time is used. If a password-change-date is specified, it must be in the following format:

```
format: mmddHHMM[[cc]yy].
  mm - 2 digits for the month (01-12)
  dd - 2 digits for a day of the month (01-31)
  HH - 2 digits for the hour of the day (00-23)
  MM - 2 digits for the minute of the hour (00-59)
  cc - 2 optional digits for the century (20,21)
  yy - 2 optional digits for year of century (00-99)
```

When the Password Change Date is set in a user record using the **-m** option, the date stored in the user record is used until the password is reset, even if the change date is available in local system files. Once the password is reset (using **passwd**) the Password Change Date in the record stored in the PDOS Login Activity Database is used only if the native UNIX password change date cannot be retrieved. When **pdoslpadm** generates a report, the password change date that is currently in effect is displayed. If the date is the value stored in the PDOS Login Activity Database, a string is displayed to indicate this. If no date is specified in the user account record from the PDOS Login Activity Database and no value is found in the system files, a string is displayed that indicates that there is no valid password change data available.

Use the **-p** option to display the login and password policy. If no users are specified, the default policy is displayed. If one or more users is specified, the policy associated with each user is displayed. If there is no policy for a specified user, this will be indicated and the default policy that is in effect for the user is displayed.

Use the **-x** option to delete the records for one or more users from the PDOS Login Activity Database.

Use the **-l** option to lock (disable) one or more native UNIX user accounts. Locking a user account will prevent the user from logging into the system.

Use the **-u** option to unlock (enable) one or more native UNIX user accounts. Unlocking a locked account will allow the user to log into the system, changing any appropriate state for the user. Specify the **-z** option along with the **-u** option to zero all fields in the PDOS Login Activity Database record for the specified user account.

Options

The following options are available with the **pdoslpadm** command:

```
-v   Displays the version information.
-h   Displays the usage message.
-?   Displays the usage message.
-q   Run quietly, return only an exit status code.
-c   Sets the configuration to on or off.
-r   Reports the state of user accounts.
-f   Specifies a full report.
-e   Specifies a report of only unlocked (enabled) user
     accounts.
-d   Specifies a report of only locked (disabled) user
     accounts.
-m   Modifies the password change date for a user account.
-p   Displays the policy for a specified exception.
-x   Deletes a user record from the database.
-l   Lock one or more user accounts.
-u   Unlock one or more user accounts.
-z   zeroes all fields in the database when unlocking the
     user account.
Exit Status
 <0  An error occurred.
 >=0 The number of records processed.
```

Examples

The following are usage examples of the options:

1. To generate a report of all users in the PDOS Login Activity Database, enter:

```
pdoslpadm -r
```

The output displays the User (uid), the state, and the time locked:

```
User(uid)   State<:time locked>
------------------------------
root(0)     Unlocked
anne(202)   Unlocked
riley(204)  Unlocked
```

2. To lock **anne's** user account, enter:

```
pdoslpadm -l anne
```

3. To generate a report of all users in the PDOS Login Activity Database whose accounts are locked, enter:

```
pdoslpadm -r -d
```

The output displays the User (uid), the state, and the time locked:

```
User(uid)   State<:time locked>
------------------------------
anne(202)  Locked(administrator): Tue Mar 27 14:38:58 CST 2001
```

4. To unlock **anne's** user account, enter:

```
pdoslpadm -u anne
```

5. To display the login policy for the root user, enter:

```
pdoslpadm -p root
```

The output is as follows:

```
Policy for root is:
  MinPasswordDays = 0
  MaxPasswordDays = 0
  MaxInactiveDays = 0
  MaxFailedLogins = 5
  MaxGraceLogins = 3
  LoginMinutes = 0
  LockMinutes = 0
  MaxConcurrent = 5
  PolicyDisabled = 0
```

6. To delete a record for user **anne** from the PDOS Login Activity Database, enter:

```
pdoslpadm -x anne
```

PDOS Auditing

The PDOS 3.7 Fixpack 1 Release introduces several changes to PDOS auditing. These changes are summarized here and described in more detail in the following sections, which describe changes to the PDOS documentation related to these changes.

New Global Audit Levels

Four new global audit levels are introduced with this release: loginpermit, logindeny, trace_exec, and trace_file. These new global audit levels are supported by both **pdoscfg** and **pdosctl**.

The new global audit levels, logindeny and loginpermit, allow control of login related audit events independent of permit and deny audit events for other PDOS resource accesses. Enabling logindeny will result in audit records being generated for all login authorization decisions that deny the login. Enabling loginpermit will result in all login authorization decisions that permit the login being audited.

The new global audit levels, trace_exec and trace_file, allow the generation of trace type audit events. Enabling trace_exec will cause the generation of audit events for the exec() system call, which is how new programs (commands) are invoked on the system. These events will be generated regardless of whether or not the program being executed is protected in PDOS. In addition, if the target of the exec() is protected by PDOS policy, then the protected object name and an indication of whether the exec() was permitted or denied will be included.

Enabling the trace_file global audit level will result in the generation of audit events on accesses to file system resources protected with PDOS policy. Trace_exec and trace_file events will be generated for a process where a login occurred and for all descendants of that login origin. These audit event types will not be generated for processes that did not descend from a login event. As a result, processes spawned from the UNIX init process during system boot

and processes that are started prior to the start of PDOS will not produce trace_exec and trace_file audit events.

Programs registered as Immune programs in the PDOS Trusted Computing Base (TCB) are also exempt from the trace type audit events.

Changes to the pdosaudview Utility

Two new command options have been added to the pdosaudview utility: **-F** and **-M**.

The **-F** option allows the user to specify how the audit records are formatted. The possible option values are verbose, concise, or keyvalue. The verbose format is similar to the format displayed by **pdosaudview** in the PDOS 3.7 product prior to Fixpack 1. In the concise format, each audit record is displayed on one line, the fields are positional with the value for each field shown in order, separated by commas. If an audit record field does not apply to a particular audit event, then just a comma is displayed to delimit the field. In the keyvalue format, each audit record is displayed on one line, each field is identified by a unique keyword, the contents of the record are displayed as keyword=value pairs separated by commas. If an audit record field does not apply to a particular audit event, it is not shown in the output. The **-F** option allows the user to specify how the output is formatted independent of where the output is written.

To reduce the amount of data displayed in the concise and keyvalue formatted output, integer values or abbreviations are defined for several of the audit record field values that are displayed as text strings in the verbose ouput. This applies to the audit event identifier, the audit view, the audit permissions, the audit qualifier, and the audit outcome fields. The **-M** option allows the user to display the mappings of these integer and abbreviated values as well as the mapping for the keywords to their descriptive text string. The possible **-M** option values are keyword, event, view, permission, qualifier, outcome, and all.

Reduction in Size of PDOS Audit Records

Several modifications were made to the PDOS binary audit record to reduce the size of each audit record. Due to these changes, any existing PDOS audit.log files created by PDOS 3.7 gold level will be renamed when the PDOS 3.7 Fixpack 1 is installed and started on the system. The **pdosaudview** utility shipped with Fixpack 1 does not support processing audit.log files created prior to Fixpack 1.

Auditing Documentation Changes

The following sections describe revisions to the PDOS documentation to support these auditing changes. Note that the format of these revisions may not exactly match that of the referenced book, which will be updated for the next major release.

Changes to the *Tivoli SecureWay Policy Director for Operating Systems Installation Guide* that apply to the **pdoscfg** command:

- Chapter 4, Configuring PDOS. Under Usage of PDOS Configuration Command Options on page 14, the -audit_level options should read:

  -audit_level (all | none | permit | deny | loginpermit | logindeny | admin | verbose | info | trace_exec | trace_file)

- Chapter 4, Configuring PDOS. Under PDOS Configuration Options on page 15, the -audit_level section should read:

  -audit_level

  A comma-separated list of audit levels. The levels are all, none, permit, deny, loginpermit, logindeny, admin, verbose, info, trace_exec, and trace_file.

  Default: none

- Appendix A, Configuration Options, page 31. The values listed for the -audit_level option in the table should read:

  all, none, permit, deny, loginpermit, logindeny, admin, verbose, info, trace_exec, trace_file.

Changes to the *Tivoli SecureWay Policy Director for Operating Systems Administration Guide*:

- Chapter 4, PDOS Administrative Tasks. Under Using Auditing to Verify Policy on page 72, the first paragraph contains a sentence listing the supported audit levels. That sentence should read:

  ″The supported global audit levels are all, none, permit, deny, loginpermit, logindeny, admin, verbose, info, trace_exec, and trace_file. The supported resource audit levels are permit, deny, and all.″

- Chapter 4, PDOS Administrative Tasks. Under Setting and Querying the Global Audit Level on page 72, the third paragraph lists the global audit levels. That sentence should read:

  ″Valid values for audit level are: all, none, permit, deny, loginpermit, logindeny, admin, verbose, info, trace_exec, and trace_file.″

- Chapter 5, PDOS Auditing. On page 81, the following should be added to the list of audit levels:

  loginpermit Tracks all login authorization decisions that permit the login.

  logindeny Tracks all login authorization decisions that deny the login.

  trace_exec Tracks process invocations.

  trace_file Tracks accesses to protected files regardless of whether or not permit or deny global or per-resource auditing is enabled.

- Chapter 5, PDOS Auditing. On page 81, the all and verbose audit levels should read as follows:

  all enables the permit, deny, admin, loginpermit, and logindeny levels.

  verbose enables the permit, deny, admin, loginpermit, logindeny, and info levels.

- Chapter 5, PDOS Auditing. On page 82, a new section called Auditing Login Authorization Decisions should be added before the Auditing Administrative Activity section.

  Auditing Login Authorization Decisions

You can audit authorization decisions that are specific to login by setting the global loginpermit and logindeny audit levels. Setting the loginpermit global audit level will result in the generation of audit records for all login authorization decisions that permit the login action. Setting the logindeny global audit level will result in the generation of audit records for all login authorization decisions that deny the login action.

Authorization decisions that are specific to login are also audited if the global permit and deny audit levels are set. The loginpermit and logindeny audit levels allow you to globally audit login separate from other authorization decisions.

- Chapter 5, PDOS Auditing. On page 82, another new section called Auditing Trace Events should be added following the Auditing Login Authorization Decisions section.

  Auditing Trace Events

  PDOS supports auditing of the trace_exec and trace_file audit events. Trace style audit events are generated by setting the trace_exec and trace_file levels in the global audit level. Setting the trace_exec global audit level will result in the generation of an audit record for each exec() system call. These records will be generated regardless of whether the program being executed is protected by PDOS policy or not. Setting the trace_file global audit level will result in the generation of an audit record for each access to a file system resource that is protected by PDOS policy.

  In general, trace_exec and trace_file audit records are generated for processes in which a login occurred and for all descendants of that login. Conversely, trace_exec and trace_file audit records are generally not generated for processes that did not descend from a login event. Processes that are started or descend from the UNIX init process during system boot do not generate trace_exec or trace_file audit records. In addition, processes that are started prior to PDOS and processes that are running programs that are registered as Immune-Programs in the PDOS TCB do not generate trace_exec or trace_file audit records.

- Chapter 5, PDOS Auditing. On page 82, the following sentence should be added to the section Auditing Administrative Activity:

″The admin audit level also causes PDOS to generate audit records for events related to a user login account being enabled or disabled when Login Activity Policy is being enforced.″

- Chapter 5, PDOS Auditing. Under Audit Log Record Format on page 82, the following information replaces the current information.

  The PDOS audit records can be divided into three distinct types:

  - **general audit records** -- These include login related events, authorization decision events, admin events, and informational events.
  - **trace audit records** -- These include trace_exec and trace_file events.
  - **logout audit records** -- These will be used for logout events.

  Within each type, records may contain different information depending on the type of resource being audited. For the same raw audit record, there will be differences in how the record is displayed by the **pdosaudview** utility depending on the format specified: verbose, keyvalue, or concise.

  Differences in Output Between verbose, concise, and keyvalue Formats

  Audit record output field headings will differ between the three formats. In the verbose output, each relevant field will have a heading in the form of a text message that describes the field. For the keyvalue format, each relevant field is identified by a unique keyword. For the concise format, there are no field headings. The field values are printed positionally and separated by commas.

  Some audit record field values will be written differently depending upon the specified format. In the concise and keyvalue formatted output, integer values are defined for several of the audit record format field values. In the verbose formatted

output, these integer values are mapped to their corresponding descriptive text strings. This mapping is documented in the tables in the following section.

Audit Record Format Field Descriptions

Tables 1, 2, and 3 describe the fields for the new PDOS audit record output formats. This information replaces the Audit Log Record Format contained on page 82 (Chapter 5) of the *PDOS Administration Guide*.

The Fixed Position column shows the fixed position for that field for the concise format. The Field Text Heading column shows the text string heading used for that field in the verbose format. The Possible Values column describes the possible values for that field. The keyword column shows the keyword value for that field for the keyvalue format.

Table 1. General Audit Events

Fixed Position	Field Text Heading	Possible Values	Keyword
1	Timestamp	Date and time event was generated.	TS
2	Audit Event Identifier	A message indicating the event that was added. (Following this table is a list of Audit Event Identifier values.)	E
3	Audit view	Audit view associated with the event: D deny P permit A admin I info T trace W warning	V

Table 1. General Audit Events (continued)

Fixed Position	Field Text Heading	Possible Values	Keyword
4	Audit reason	Reason why audit record was generated: 1 global audit 2 resource audit 3 global warning 4 resource warning	R
5	Audit resource type	Resource type: Process TCB Cred Policy Login File NetIncoming NetOutgoing Surrogate Sudo	RT
6	Accessor name	Accessing user's name.	AN
7	Accessor effective name	Accessing user's effective name.	AEN

Table 1. General Audit Events (continued)

Fixed Position	Field Text Heading	Possible Values	Keyword
8	Audit action	The action for the audit event: check_access add delete change retrieve apply trust untrust start stop register trace isolated not_isolated login logout enable disable	A

Table 1. General Audit Events (continued)

Fixed Position	Field Text Heading	Possible Values	Keyword
9	Audit permissions	If the audit action field value is Check_access, then this field will contain the specific action(s) associated with the access request: C connect D chdir G surrogate K kill L login N create R rename U utime d delete l readdir o chown p chmod r read w write x execute	P
10	Audit qualifier	Provides additional information for the audit event. (Following this table is a list of Audit qualifier values.)	Q
11	Policy Branch Name	The Policy Branch Name field will only be filled in if there is a value in the Protected Object Name field.	PBN

Table 1. General Audit Events (continued)

Fixed Position	Field Text Heading	Possible Values	Keyword
12	Protected Object Name	For audit events where the audit action is check_access, this will be the tail of the protected object name used to determine if access is allowed. For audit events where the resource type is Policy and the audit action is apply, this will be the Protected Object Name that policy was applied to.	PON
13	System Resource Name	If the resource type is File, this will be the system name of the file being accessed. For audit events where the resource type is TCB and the audit action is trust or untrust, this will be the name of the TCB resource that was marked trusted or untrusted. For audit events where the resource type is Login, and the view is Admin, and the action is disable or enable, this will be the name of the user account that was enabled or disabled for login.	SRN

Table 1. General Audit Events (continued)

Fixed Position	Field Text Heading	Possible Values	Keyword
14	Surrogate Name	If the resource type is Surrogate, this will be the user name or ID of the target user or the group name or ID of the target group.	SN
15	Network Remote Host Identifier	If the resource type is NetIncoming, this is the remote host where access originated. If the resource type is NetOutgoing, this is the remote host being accessed. The identifier will be a hostname if the address can be converted; otherwise, it will be an IP address.	NRH
16	Network Protocol	If the resource type is NetIncoming or NetOutgoing, this will be the protocol being used in the access.	NP
17	Network Service	If the resource type is NetIncoming, this will be the service name or port number for the local service being accessed. If the resource type is NetOutgoing, this will be the service name or port number of the remote network service being accessed.	NS

Table 1. General Audit Events (continued)

Fixed Position	Field Text Heading	Possible Values	Keyword
18	Login Location identifier	If the resource type is Login, and the login occurred from a local terminal, this is the local terminal name. If the login occurred from a remote system, this will be either the hostname or the IP address.	LL
19	Accessor Processor ID	Process ID.	APID
20	Running Program Protected Name	If the running program is registered in the TCB, the name it is registered as will appear here.	RPPN
21	Running Program System Resource Name	Name of the running program as executed.	RPSN
22	Sudo Command and Arguments	If the resource type is Sudo, this will be the target command name and the command arguments if they are relevant to the Sudo policy.	SC
23	Sudo User Name	If the resource type is Sudo, this will be the target user name that the Sudo command will be executed as, if relevant to the Sudo policy.	SU

Table 1. General Audit Events (continued)

Fixed Position	Field Text Heading	Possible Values	Keyword
24	Sudo flags	If the resource type is Sudo, this will indicate that the policy dictated that the invoker password and/or target user password was required before the target command could be executed. If neither is specified in the Sudo policy, this field will not contain a value.	SF
25	Additional parameters	Additional information related to the particular audit event.	AP
26	TCB Changed Data Attr flags	Additional information related to TCB resources.	CDAF
27	Policy epoch	Additional information related to Policy resources.	PE
28	Policy version number	Additional information related to Policy resources.	PVN
29	Audit outcome	If the audit record was generated as a result of action taken due to an error condition, the outcome will be Failure (F); otherwise, the outcome will be Success (S).	O
30	Audit fail status	If the audit event outcome is Failure, this field will contain an error code indicating what error occurred; otherwise, this field will be zero.	FS

Table 1. General Audit Events (continued)

Fixed Position	Field Text Heading	Possible Values	Keyword
31	Audit Uniqifier	Integer field to uniquely identify audit records that occur within the same second. The value starts with 0 for the first audit record in a second and will increase sequentially for subsequent records within the same second.	UQ

Audit Event Identifier Values

1 Login related authorization decision was made.

2 User account disabled (locked) for login.

3 User account disabled (suspended) for login.

4 User account enabled for login.

5 Password change time was modified by admin.

6 Logout occurred.

7 An authorization decision was made.

8 An authorization decision API failure has occurred.

9 Access granted to a file marked untrusted in the TCB database.

10 PDOS kernel lost contact with PDOSD.

11 PDOS kernel has regained contact with PDOSD.

12 Policy Director user registry is unavailable (isolation mode).

13 Policy Director user registry is available.

14 Credential acquired.

15	Policy not applied for an invalid protected object name.
16	Policy applied for a protected object name.
17	Policy version set in Kernel Policy Cache.
18	Kernel Policy Cache epoch updated.
19	A new file has been added to the TCB database.
20	A file has been removed from the TCB database.
21	A file has been marked untrusted.
22	A file has been marked trusted.
23	A PDOS process has started.
24	A PDOS process has stopped.
25	A PDOS process has been adopted into the watchdog set.
26	A kosseal_register call was made to acquire privileged access.
27	TRACE Exec program
28	TRACE File access.
29	Password successfully changed.

Audit Qualifier Values

Login related:

1	User account is locked.
2	No grace logins remain and user's password has expired.
3	Maximum concurrent logins reached.
4	Lock time interval has not elapsed.
5	Minimum time interval required between password changes has not elapsed.

6	User account unlocked because lock time interval has elapsed.
7	Maximum number of failed logins for user reached.
8	Maximum inactive days has elapsed.
9	Maximum time interval since last password change has elapsed.
10	Checking login location access control policy.
11	Checking login location via-program access restrictions.
12	Checking login holiday access control policy.
13	Checking login holiday via-program access restrictions.
14	Checking time of day login access control policy.
15	Unknown user attempted to log in.
16	Login denied by native authentication method.
17	User account modified by administrative action.
18	All login policy checks permitted access.

Audit Qualifier Values

General resource related:

30	Checking resource access control policy.
31	Checking resource via-program access restrictions.
32	Checking trust state for TCB resource.
33	Error occurred reading the request message data.
34	All resource policy checks permitted access.

Note: More qualifiers may be defined as needed.

Table 2. Trace Audit Events

Fixed Position	Field Text Heading	Possible Values	Keyword
1	Timestamp	Date and time event was generated.	TS
2	Audit Event Identifier	27 TRACE Exec program. 29 TRACE File access.	E
3	Audit view	Audit view associated with the event: D deny P permit T trace	V
4	Audit reason	Reason why audit record was generated: 1 global audit	R
5	Audit resource type	Resource type: TraceExec TraceFile	RT
6	Accessor name	Accessing user's name.	AN
7	Accessor effective name	Accessing user's effective name.	AEN
8	Audit action	Trace	A
9	Audit permissions	This field will contain the specific action(s) associated with the access request: D chdir K kill N create R rename U utime d delete l readdir o chown p chmod r read w write x execute	P

Table 2. Trace Audit Events (continued)

Fixed Position	Field Text Heading	Possible Values	Keyword
10	Audit qualifier	Provides additional information for the audit event. Currently None. Note: trace audit related qualifiers might be added in the future.	Q
11	Protected resource specification	If the resource type is TraceExec and the subject of the exec() operation is a PDOS protected file resource, then the name of the file system resource with relevant PDOS protections is logged. For TraceFile events, this information is always logged.	PRS

Table 2. Trace Audit Events (continued)

Fixed Position	Field Text Heading	Possible Values	Keyword

12	Accessed resource specification	If the resource type is TraceExec, this will be the file resource name as it was specified in the exec () operation. If the file is a setuid program, then an [SU] token will follow the file name. If the file is a setgid program, then an [SF] token will follow. If the program is both setuid and setgid, then an [SUG] token will follow. Finally, the argv string provided in the exec() call which normally represents command line arguments will follow enclosed within parentheses. An example might look as follows:
		`/usr/bin/ps [SG] \`
		`(ps -elf | grep pdos)`
		
		If the resource type is TraceFile, this will be the name of the file resource used in the access.
			ARS

13	Accessor pid	Process ID.	APID
14	Running program System Resource Name	Name of the running program as executed.	RPSN

Table 2. Trace Audit Events (continued)

Fixed Position	Field Text Heading	Possible Values	Keyword
15	Audit uniqifier	Integer field to uniquely identify audit records that occur within the same second. The value starts with 0 for the first audit record in a second and will increase sequentially for subsequent records within the same second.	UQ

Table 3. Logout Audit Events

Fixed Position	Field Text Heading	Possible Values	Keyword
1	Timestamp	Date and time event was generated.	TS
2	Audit Event Identifier	6 Logout occurred.	E
3	Audit view	P Permit.	V
4	Audit reason	Reason why audit record was generated: 1 global audit	R
5	Audit resource type	Resource type: Logout	RT
6	Accessor name	Logout user name.	AN
7	Accessor effective name	Accessing user's effective name.	AEN
8	Audit action	Logout.	A
9	Accessor pid	Process ID under which the logout is occurring. Typically, this will be the same process ID where the login occurred.	APID

Table 3. Logout Audit Events (continued)

Fixed Position	Field Text Heading	Possible Values	Keyword
10	Login location identifier	If the login terminal location from the original login is available, it is provided as either the local terminal device name (for example, **/dev/tty0**) or as remote host information in the form of a hostname (for example, **host1.eng.com**) or a dotted IP address notation such as **209.41.18.22**.	LL
11	Audit uniqifier	Integer field to uniquely identify audit records that occur within the same second. The value starts with 0 for the first audit record in a second and will increase sequentially for subsequent records within the same second.	UQ

Additional Documentation Changes

The following sections describe additional changes to the *PDOS Administration Guide*.

- Chapter 5, PDOS Auditing. Under Viewing Audit Logs on page 88, the following information should be added.

  A new command option has been added to **pdosaudview**, the PDOS audit viewing utility, to allow the user to specify how the audit records should be formatted. The new command argument is **-F** and the possible argument values are verbose, concise, or keyvalue.

  verbose -- Each field has a text heading that describes the field, and the field's value is fully expanded when applicable. For example, the audit event field value will be a text string describing the event instead of an integer number; the audit

qualifier field value will be a text string instead of an integer number. The start of each record is indicated by the text string ***START OF NEW RECORD*** and the field headings and values are displayed linearly in the output. If an audit record format field doesn't apply to a particular event, it is not shown in the output. The position of the fields is shown in Tables 1, 2, and 3.

concise -- Each audit record is displayed on one line, and the fields are positional with the value for each field shown in order and separated by commas. If an audit record format field does not apply to a particular event, then just a comma will be displayed to delimit that field. The position of the fields is shown in Tables 1, 2 and 3.

keyvalue -- Each audit record is displayed on one line, and each field is identified by a unique keyword; the contents of the record are displayed as keyword=value pairs separated by commas. If an audit record format field does not apply to a particular event, it is not shown in the output. The keyword values are shown in Tables 1, 2, and 3.

The **-F** option allows the user to specify how the output is formatted independent of where the output is written.

By default, the **pdosaudview** utility writes the audit record output to the /var/pdos/audit/text.log file. The default format for this output is the keyvalue format. The **-F** option may be specified to write concise or verbose formatted output to the text.log file.

Specifying the **-l** option indicates that output should be written to STDOUT. The default format for this output is verbose. The **-F** option may be combined with the **-l** argument to write concise or keyvalue formatted output to STDOUT.

Specifying the **-f** filename option indicates that output should be written to the specified filename. The default format for this output is the keyvalue format.

The **-F** option may be combined with **-f** to write concise or verbose formatted output to the specified filename.

The following are examples of the verbose, keyvalue, and concise formats.

For the verbose format, each record is separated by the text string ***START OF NEW RECORD***. Each relevant field is displayed on a single line with a left-justified heading followed by the field value. If an audit record field doesn't apply to a particular event, it is not shown in the output. The following is an example. Note that the output has been formatted to fit the page.

START OF NEW RECORD

Timestamp	Mon May 7 13:14:20 CDT 2001
Audit Event	An authorization decision was made.
Audit View	Deny
Audit Reason	Global Audit
Audit Resource Type	File
Accessor Name	riley
Accessor Effective Name	riley
Audit Action	Check Access
Audit Permissions	readdir
Audit Qualifier	Checking resource access control policy.
Policy Branch Name	carlb
Protected Object Name	File/u/anne
System Resource Name	.
Accessor Process ID	11512
Running Program System Resource Name	/usr/bin/ls
Audit Outcome	Success
Audit Uniqifier	0

For the keyvalue format, each audit record is displayed on one line. Each relevant field is printed as a keyword=value pair. The fields are separated by commas. If an audit record field does not apply to a particular event, it is not shown in the output. The following is an example. Note that the display would be contained on one line:

TS=Mon May 7 13:14:20 CDT 2001,
E=7,V=D,R=1,RT=File,AN=riley,AEN=riley,A=Check
Access,P=l,Q=30,PBN=carlb,PON=File/u/anne,SRN=.,
APID=11512,RPSN=/usr/bin/ls,O=S,UQ=0

For the concise format, each audit record is displayed on one line. Each field has a defined position within the audit record output. The fields are separated by commas. If an audit record field does not apply to the audit record being processed, only the delimiting comma is written. The following is an example:

Mon May 7 13:14:20 CDT 2001,7,D,1,File,riley,riley,Check
Access,1,30,carlb,File/u/anne,.,,,,,,11512,,/usr/bin/ls,,,,,,,,S,,0

- Appendix A, PDOS Commands. Under **pdosaudview** on page 92, the **Syntax** should include the following new options:

  -F verbose | keyvalue | concise

  -M keyword | event | view | permission | qualifier | outcome | all

  The **Options** are changed as follows:

  -g Resource type (azn, daemon, tcb, cred, policy, login, logout, trace_exec, trace_file)

  -p Originating PID (KERNEL, PDOSD, WATCHDOG, AUDITD, TCB, GENERAL)

  -w Audit view (permit, deny, admin, info, trace, warning)

  -a Action (check_access, add, delete, change,

retrieve, apply, trust, untrust, start, stop, register, trace, isolated, not_isolated, unknown, login, logout, enable, disable)

-o Outcome (success, failure, trace_event, trace_permit, trace_deny)

- Appendix A, PDOS Commands. On page 93 of the *PDOS Administration Guide*, the following examples replace the examples for the **pdosaudview** command.

  The following record is an example of a General Audit Event Record when **pdosaudview** is invoked with the **-F** verbose parameter. Note that the output has been formatted to fit the page.

  START OF NEW RECORD

Timestamp	Tue May 8 08:44:55 CDT 2001
Audit Event	An authorization decision was made.
Audit View	Deny
Audit Reason	Global Audit
Audit Resource Type	File
Accessor Name	riley
Accessor Effective Name	riley
Audit Action	Check Access
Audit Permissions	readdir
Audit Qualifier	Checking resource access control policy.
Policy Branch Name	carlb
Protected Object Name	File/u/anne
System Resource Name	.
Accessor Process ID	11910

Running Program System Resource Name	/usr/bin/ls
Audit Outcome	Success
Audit Uniqifier	0

The following record is an example of a General Audit Event Record when **pdosaudview** is invoked with the **-F** keyvalue parameter.

TS=Tue May 8 08:44:55 CDT 2001,
E=7,V=D,R=1,RT=File,AN=riley,AEN=riley,A=Check Access,P=1,Q=30,PBN=carlb,PON=File/u/anne,SRN=.,
APID=11910,RPSN=/usr/bin/ls,O=S,UQ=0

The following record is an example of a General Audit Event Record when **pdosaudview** is invoked with the **-F** concise parameter:

Tue May 8 08:44:55 CDT 2001,7,D,1,File,riley,riley,Check Access,1,30,carlb,File/u/anne,.,,,,,,11910,,/usr/bin/ls,,,,,,,,S,,0

The following record is an example of a Trace Audit Event Record when **pdosaudview** is invoked with the **-F** verbose parameter:

START OF NEW RECORD

Timestamp	Tue May 8 08:44:55 CDT 2001
Audit Event	TRACE File access.
Audit View	Deny
Audit Reason	Global Audit
Audit Resource Type	TraceFile
Accessor Name	riley
Accessor Effective Name	riley

Audit Action	Trace
Audit Permissions	readdir
Protected Resource Specification	/u/anne
Accessed Resource Specification	.
Accessor Process ID	11910
Running Program System Resource Name	/usr/bin/ls
Audit Uniqifier	0

The following record is an example of a Trace Audit Event Record when **pdosaudview** is invoked with the **-F** keyvalue parameter:

TS=Tue May 8 08:44:55 CDT 2001,
E=28,V=D,R=1,RT=TraceFile,AN=riley,AEN=riley,
A=Trace,P=1,PRS=/u/anne,ARS=.,APID=11910,RPSN=/usr/bin/ls,UQ=0

The following record is an example of a Trace Audit Event Record when **pdosaudview** is invoked with the **-F** concise parameter:

Tue May 8 08:44:55 CDT 2001,
28,D,1,TraceFile,riley,riley,Trace,1,,/u/anne,.,11910,/usr/bin/ls,0

The following record is an example of a Logout Audit Event Record when **pdosaudview** is invoked with the **-F** verbose parameter:

START OF NEW RECORD

Timestamp	Tue May 8 08:44:55 CDT 2001
Audit Event	Logout occurred.
Audit View	Permit

Audit Reason	Global Audit
Audit Resource Type	Logout
Accessor Name	riley
Audit Action	Logout
Accessor Process ID	10924
Login Location Identifier	riley.tivoli.com
Audit Uniqifier	0

The following record is an example of a Logout Audit Event Record when **pdosaudview** is invoked with the **-F** keyvalue parameter:

TS=Tue May 8 08:44:55 CDT 2001,
E=6,V=P,R=1,RT=Logout,AN=riley,A=Logout,
APID=10924,LL=riley.tivoli.com,UQ=0

The following record is an example of a Logout Audit Event Record when **pdosaudview** is invoked with the **-F** concise parameter:

Tue May 8 08:44:55 CDT 2001,6,P,1,Logout,riley,,Logout,
10924,riley.tivoli.com,0

- Appendix A, PDOS Commands. Under the Syntax section of **pdoscfg** on page 96, the -audit_level should read as follows:

  -audit_level (all | none | permit | deny | loginpermit | logindeny | admin | verbose | info | trace_exec | trace_file)

  Under the Options section on page 97, the -audit_level should read as follows:

  -audit_level

  A comma-separated list of audit levels. The levels are all, none, permit, deny, loginpermit, logindeny, admin, verbose, info, trace_exec, and trace_file.

  Default: none

- Appendix A, PDOS Commands. Under **pdosctl** on page 100, the Description section lists the valid values for the audit level. The sentence should read:

  ″Valid values for audit level are: all, none, permit, deny, loginpermit, logindeny, admin, verbose, info, trace_exec, and trace_file.″

Installing PDOS 3.7 Fixpack 1 Using Native Install

Follow these instructions if the Tivoli SecureWay Policy Director for Operating Systems 3.7.0.0 product was installed from the Native Installation CD.

Prior to installing the patch, PDOS must be stopped. In addition, it is recommended that you get the latest operating system installation patches.

Note: If you have installed the PDOS 3.7.0.0 English catalogs, you need to install the PDOS 3.7.0.1 English catalogs.

Tivoli SecureWay Policy Director for Operating Systems 3.7 Fixpack 1 is available as part of the Tivoli SecureWay Security Manager 3.7.1-SEC-0002 patch and can be downloaded from the Tivoli support website:

http://www.tivoli.com/patches

1. Select Security Management.
2. Select 3.7.1-SEC-0002.
3. Download the native tar image, untar it, and follow the instructions in the following sections.

Installing PDOS on AIX

PDOS can be installed on AIX using SMIT, or it can be installed from the command line.

Installing on AIX Using SMIT

Use these steps to install PDOS on AIX using SMIT:

1. Download PDOS 3.7 Fixpack 1.
2. Log in as root.
3. At the command line, type:

   ```
   smit
   ```

   Press Enter. The **System Management Interface Tool** window is displayed.
4. From the System Management menu, click **Software Installation and Maintenance**.
5. From the Software Installation and Maintenance menu, click **Install and Update Software**.
6. From the Install and Update Software menu, click **Install and Update from LATEST Available Software**. The **Install and Update from LATEST Available Software** pop-up panel is displayed.
7. Specify the INPUT device / directory for software by typing the name of the directory where the PDOS 3.7 Fixpack 1 package is located. Click **OK**.
8. The **Install and Update from LATEST Available Software** pop-up panel is displayed.
9. By the SOFTWARE to install selection, click **List**. The **Multi-select List** pop-up panel is displayed. Highlight 3.7.0.1 Policy Director for Operating Systems Runtime. Click **OK**.
10. The **Install and Update from LATEST Available Software** window is redisplayed. For the **COMMIT software updates?** field, select **no**.
11. Click **OK**.
12. You are asked to confirm your installation choices. Click **OK**.
13. During installation, the **Install and Update from LATEST Available Software** window displays a split screen that shows the install command and the output log for the installation.

14. When installation is complete, click **Done**.
15. Close the **Install and Update from LATEST Available Software** pop-up panel. The **System Management Interface Tool** window is displayed.
16. Close the **System Management Interface Tool** window.
17. Reboot the system in order to activate the kernel update.

Installing on AIX Using the Command Line

To install PDOS on AIX from the command line, use these steps:

1. Download PDOS 3.7 Fixpack 1.
2. Log on as root.
3. At the command line, type:

   ```
   installp -a -g -X -d /directory PDOS.rte
   ```

   where *directory* specifies the directory where Fixpack 1 was downloaded.
4. Reboot the system in order to activate the kernel update.

Installing PDOS on HP-UX

PDOS can be installed on HP-UX using SWinstall, or it can be installed from the command line. The files must be installed in the **/opt/pdos** and **/var/pdos** directories. Do not change target from **/**.

Installing on HP-UX Using SWinstall

To install PDOS on HP-UX, complete the following steps:

1. Download PDOS 3.7 Fixpack 1.
2. Log on as root.
3. At the command line, type:

   ```
   swinstall
   ```

   Press Enter.
4. The **SD Install – Software Selection** window and **Specify Source** pop-up panel are displayed. Select **Local Directory** from the Source Depot Type list.

5. For the Source Depot path, enter
   `/directory/PDOSrte.depot`

   where *directory* specifies the directory where Fixpack 1 was downloaded.

   Click **OK**. The **SD Install - Software Selection** window is displayed.
6. From the **SD Install – Software Selection window**, mark the software you want to install by selecting the PDOS package **PDOSrte**.
7. Click the Actions menu and select **Mark for Install**.
8. Click the Actions menu and select **Install (analysis)**. The **Install Analysis** pop-up panel is displayed. When status is Ready, click **OK**.
9. The **Confirmation** pop-up window is displayed. Click **Yes**.
10. The Install Window pop-up panel displays the status of the installation process. When status is Completed, click **Done**.
11. Close the **SD Install – Software Selection** window.
12. Reboot the system in order to activate the kernel update.

Installing on HP-UX Using the Command Line

To install PDOS on HP-UX from the command line, use these steps:

1. Download PDOS 3.7 Fixpack 1.
2. Log on as root.
3. At the command line, type:
   `swinstall -s /directory/PDOSrte.depot PDOSrte`

   where *directory* specifies the directory where Fixpack 1 was downloaded.
4. Reboot the system in order to activate the kernel update.

Installing PDOS on Solaris

PDOS can be installed on Solaris from the command line.

Installing on Solaris Using the Command Line

This installation requires that you have loaded the patches for Solaris 2.6 and 2.7. For Solaris 2.6, the patch needed is 106125-10. For Solaris 2.7, the patch needed is 107171-05.

To install PDOS on Solaris from the command line, use these steps:

1. Download PDOS 3.7 Fixpack 1.
2. Log on as root.
3. At the command line, type:
   ```
   pdos_fix_solaris_arch
   ```
   Press Return.
4. At the command line, type:
   ```
   patchadd PDOS000370-01
   ```
   Press Return.
5. Reboot the system in order to activate the kernel update.

Removing PDOS 3.7 Fixpack 1 Using Native Install

Prior to uninstalling PDOS 3.7 Fixpack 1, ensure that Login Activity Policy enforcement is not enabled. To do so, run **pdoscfg** and set the login_policy option to off.

If you have applied and then removed PDOS 3.7 Fixpack 1, complete the following steps.

1. Run **pdosobjsig** to retrust the PDOS default objects.
2. Reboot the system in order to activate the PDOS 3.7.0.0 level of the kernel.

PDOS System Requirements

This section describes the hardware and software requirements for PDOS.

Hardware Requirements

This section describes hardware requirements needed to install PDOS.

Hardware Requirements for Installing PDOS on AIX, HP-UX, and Solaris

The hardware requirements for a PDOS machine are given in the following tables:

Table 4. PDOS Hardware Requirements

Minimum RAM	64 MB
Recommended RAM	128 MB or greater

Table 5. Disk Space Required for Installing PDOS

Platform	Approximate Space Needed
AIX	10 MB in **/opt** for PDOS
	90 MB in **/usr** for GSKit, LDAP and PD
	20 MB in **/var** for PDOS runtime files
HP-UX	100 MB in **/opt** for PDOS, GSKit, LDAP, and PD
	20 MB in **/var** for PDOS runtime files
Solaris	100 MB in **/opt** for PDOS, GSKit, LDAP, and PD
	20 MB in **/var** for PDOS runtime files

Note: For all platforms, space required under /var/pdos is dependent on your policy and audit settings; space required can increase over time.

Software Requirements

This section describes the software requirements needed to install PDOS.

Software Requirements for Installing PDOS on AIX

The minimum software requirements for installing PDOS on AIX depend on what version of AIX your system uses. Most of the software required is available on the PDOS CD.

AIX 4.3.3 or Higher

If your system uses AIX 4.3.3 or higher, the minimum software requirements for installing PDOS depend on what version of IBM SecureWay Directory client you are running.

IBM SecureWay Directory 3.1.1.5 Client

- Tivoli SecureWay Policy Director 3.7.0 Runtime Environment
- IBM SecureWay Directory 3.1.1.5 Max Crypto Client
- IBM Global Security Toolkit 3.0.1.120 and 4.0.3.61
- bos.rte.libpthreads 4.3.3.11 available with patch u470050 (not on CD)

IBM SecureWay Directory 3.2 Client

- Tivoli SecureWay Policy Director 3.7.0 Runtime Environment
- IBM SecureWay Directory 3.2 Max Crypto Client (not on CD)
- IBM Global Security Toolkit 4.0.3.61
- bos.rte.libpthreads 4.3.3.11 available with patch u470050 (not on CD)

AIX 4.3.1 and AIX 4.3.2

The software requirements for installing PDOS on AIX 4.3.1 and 4.3.2 are:

- Tivoli SecureWay Policy Director 3.7.0 Runtime Environment
- IBM SecureWay Directory 3.1.1.5 Client
- IBM SecureWay Directory 3.1.1.5 Max Crypto Client
- IBM Global Security Toolkit 3.0.1.120 and 4.0.3.61

Note: IBM SecureWay Directory 3.2 does not support AIX 4.3.1 and AIX 4.3.2.

Software Requirements for Installing PDOS on HP-UX

The minimum software required for installing PDOS on HP-UX, most of which is on the PDOS CD, includes:

- HP-UX 11.00.47 (not on CD)
- Tivoli SecureWay Policy Director 3.7.0 Runtime Environment
- IBM SecureWay Directory 3.2 Client
- IBM Global Security Toolkit 4.0.3.65

Software Requirements for Installing PDOS on Solaris

The minimum software required for installing PDOS on Solaris, most of which is on the PDOS CD, includes:

- Solaris 2.6 with patch 105181–23 (not on CD)
- Solaris 2.7 with patch 106980-13 (not on CD)
- Solaris 2.8 (not on CD)
- Tivoli SecureWay Policy Director 3.7.0 Runtime Environment
- IBM SecureWay Directory 3.2 Client
- IBM Global Security Toolkit 4.0.3.57

Installation Notes Using Native Install

You should be familiar with the native software installation utility for the platform where you plan to install PDOS. In addition, you must have the required patches.

At runtime, PDOS stores authorization policy information, audit logs, and error logs in the various directories under /var/pdos. It is strongly recommended that /var/pdos be created as a separate file system in order to ensure that user activity that might cause /var to become full does not impact PDOS's ability to enforce authorization policy. It is also advisable to make /var/pdos/log and /var/pdos/audit separate file systems. You should carefully monitor the space usage of the /var/pdos, /var/pdos/log, and /var/pdos/audit directories.

At runtime, PDOS relies on an osseal user and group existence on a system. If an osseal group entry does not exist, the installation of PDOS creates an osseal group entry. If an osseal user entry does not exist, the installation of PDOS creates an osseal user entry. The osseal user is created with the primary group of osseal.

Note: If you are currently using TACF for enforcing policy, whether in a TSSM environment or a non-TSSM environment, you should also read the information in the migration appendix in the *PDOS Installation Guide*.

Supported Levels of Tivoli SecureWay Policy Director 3.7

The minimum supported level for the Tivoli SecureWay Policy Director Management server running in Policy Director for Operating Systems (PDOS) 3.7 environments is Tivoli SecureWay Policy Director 3.7 Fixpack 1 (3.7-POL-0001) or Tivoli SecureWay Policy Director 3.7.1.

The supported level of the Tivoli SecureWay Policy Director Runtime Environment (PDRTE) installed on a PDOS 3.7 machine varies depending on the version of the Tivoli SecureWay Policy Director Management Server.

If the Tivoli SecureWay Policy Director Management Server is running Version 3.7.0 Fixpack 1 (3.7-POL-0001), then PDOS 3.7 machines may have the PDRTE Version 3.7.0 or 3.7.0 with Fixpack 1 installed; but not PDRTE Version 3.7.0 Fixpack 2 (3.7-POL-0004) or 3.7.1.

If the Tivoli SecureWay Policy Director Management Server is running Version 3.7.1, then PDOS 3.7 machines may have the PDRTE 3.7.0, 3.7.0 with Fixpacks, or PDRTE Version 3.7.1 installed.

The current *Tivoli SecureWay Policy Director, Version 3.7/3.7.1 Release Notes* can be accessed at the following URL:

http://www.tivoli.com/support/Prodman/html/AB.html#Security

Tivoli SecureWay Policy Director 3.7 Fixpacks are available at the following URL:

http://www.tivoli.com/patches

Patch for IBM SecureWay Directory 3.2 Client

In order for PDOS to function properly, a patch is needed for IBM SecureWay Directory 3.2 Client. The patch for each platform is available on the Tivoli SecureWay Policy Director for Operating Systems Version 3.7 (128-BIT) CD. If the Quick Install Feature installs IBM SecureWay Directory 3.2 on the system, the patch is applied automatically. Otherwise, you need to apply the patch.

Installing on AIX

To apply the patch on an AIX system that has IBM SecureWay Directory 3.2 installed:

Note: Do not apply this patch to IBM SecureWay Directory 3.1.1.5 systems.

1. Insert the PDOS CD-ROM.
2. Log on as root.
3. Mount the CD.
4. Type the following command on the command line:

   ```
   cp /cdrom/usr/sys/inst.images/ldap32_patch/libldap.a \
    /usr/ldap/lib/libldap.a
   ```

   where /cdrom is the CD mount point. Press Enter.

Installing on HP-UX

To apply the patch on an HP-UX system that has IBM SecureWay Directory 3.2 installed:

1. Insert the PDOS CD-ROM.
2. Log on as root.
3. Start pfs_mountd and then pfsd, if they are not running and mount the CD with the pfs_mount command. For example, at the command line type:

   ```
   pfs_mount /dev/dsk/c0t0d0 /cd-rom
   ```

   where /dev/dsk/c0t0d0 is the CDROM device and /cd-rom is the mount point. Press Enter.

4. Type the following command on the command line:

   ```
   cp /cd-rom/hp/libldap.sl  /opt/ldap/adt/lib/libldap .sl
   ```

   where /cd-rom is the cd mount point. Press Enter.

Installing on Solaris

To apply the patch on a Solaris system that has IBM SecureWay Directory 3.2 installed:

1. Insert the PDOS CD-ROM.
2. Log on as root.
3. Type the following command on the command line:

   ```
   cp /cdrom/solaris/libibmldap.so  /opt/IBMldapc/lib/libibmldap.so
   ```

   where /cd-rom is the cd mount point. Press Enter.

Quick Install Feature of PDOS

PDOS can be installed using the **install_pdos_client.***platform* script. The **install_pdos_client.***platform* script takes you through the necessary installation and configuration steps. The script identifies what components are already installed, locates the needed uninstalled components on the CD-ROM, and installs them. After the components are installed, those requiring configuration can be configured from the script as well.

The *platform* suffix refers to the platform where you plan to install PDOS. The available platform suffixes include:

Table 6. Platform Suffixes for PDOS Quick Install Script

Platform	Platform Suffix
AIX	aix
HP-UX	hpux
Solaris	sol

Installing Using the Quick Install Script

Use these steps to install PDOS using the **install_pdos_client.***platform* script:

1. Insert the PDOS CD-ROM.
2. Log in as root.
3. Mount the CD-ROM drive based on mounting procedure for your platform.

   Note: On HP-UX, use the pfs_mount command which requires pfs-mountd and pfsd to be running.
4. Change to the CD-ROM directory. This directory contains the **install_pdos_client.***platform* script.
5. To run the script, type this command on the command line:

   `./install_pdos_client.`*`platform`*

   Press Enter.
6. Before each installation, the process informs you of what is about to happen. Press Enter to continue.
7. If language files are located on the CD-ROM for the various components, the process displays all of the available language files, allowing you to specify which ones to install on the client machine. A number is displayed beside the language files. Enter the number of the language you wish to install. All of the languages selected are displayed on the screen. If you make a mistake, press X to start over. Press Y when you are ready to install the language files.

   Note: If no language files need to be installed, press Y to continue.

Configuring Using the Quick Install Script

After you have successfully completed the installations, the configuration screens are displayed. Each screen contains various numbered options. To modify the value of an option, enter the corresponding number beside the option. The screen prompts you for the value. If you make a mistake, enter the number again to correct the value.

Once all of the configuration values have been entered correctly, press Y to begin the configuration.

During a successful installation and configuration of each component, you might notice that the status of each component changes from **Not Installed** to **Not Configured** to **Configured**. When all of the components have a status of **Configured**, the installation and configuration process is complete. To start PDOS, enter the following command at the command line:

```
rc.osseal start
```

Log File for the Quick Install Script

Every event which occurs during the install and configuration process is logged in a file named **/var/install_pdos_client.***platform***.log**. If an error occurs during the process, refer to this log for more details.

Internationalization

With the PDOS 3.7 Fixpack 1 release, PDOS is an internationalized product that supports English and other languages. It derives its language behavior from the installed localization features and from the user's language preference. The localization features consist primarily of translated message catalogs and codeset tables for text processing and interoperability.

Installing PDOS 3.7 Fixpack 1 Language Packages Using Native Install

For language package installation, refer to Chapter 3, Installing PDOS in the *PDOS Installation Guide*.

Notes:

1. Since language packages have been downloaded, you can skip CD-specific steps.
2. If you have installed the PDOS 3.7.0.0 English catalogs, you need to install the PDOS 3.7.0.1 English catalogs.

Enabling Language Support

PDOS is translated into the following languages:

- Brazilian Portuguese
- Chinese (simplified)
- Chinese (traditional)
- U.S. English
- French
- German
- Italian
- Japanese
- Korean
- Spanish

To enable these languages, install the appropriate language support package. Be sure to set your locale based on your operating system procedures. You can also install multiple language support packages for a single product.

The following tables show the package name for the PDOS message package as it relates to code page and language for each operating system platform.

Table 7. AIX

Language	Package Name
Brazilian Portuguese	PDOS.msg.pt_BR
Simplified Chinese (EUC)	PDOS.msg.zh_CN
Simplified Chinese (GBK)	PDOS.msg.Zh_CN
Traditional Chinese	PDOS.msg.zh_TW
T-Chinese (big5)	PDOS.msg.Zh_TW
U.S. English	PDOS.msg.en_US
French	PDOS.msg.fr_FR
French (IBM-850)	PDOS.msg.Fr_FR

Table 7. AIX (continued)

Language	Package Name
German	PDOS.msg.de_DE
German (IBM-850)	PDOS.msg.De_DE
Italian	PDOS.msg.it_IT
Italian (IBM-850)	PDOS.msg.It_IT
Japanese (IBM-eucJP)	PDOS.msg.ja_JP
Japanese	PDOS.msg.Ja_JP
Korean	PDOS.msg.ko_KR
Spanish	PDOS.msg.es_ES
Spanish (IBM-850)	PDOS.msg.Es_ES

Table 8. HP-UX

Language	Package Name
Brazilian Portuguese	PDOSmsgpt_BR
Simplified Chinese (EUC)	PDOSmsgzh_CN
Traditional Chinese	PDOSmsgzh_TW
T-Chinese (big5)	PDOSmsgZh_TW
U.S. English	PDOSmsgen_US
French	PDOSmsfr_FR
German	PDOSmsgde_DE
Italian	PDOSmsgit_IT
Japanese (IBM-eucJP)	PDOSmsgja_JP
Japanese	PDOSmsgJa_JP
Korean	PDOSmsgko_KR
Spanish	PDOSmsges_ES

Table 9. Solaris

Language	Package Name
Brazilian Portuguese	PDOSptBR
Simplified Chinese (EUC)	PDOSzhCN

Table 9. Solaris (continued)

Language	Package Name
Traditional Chinese	PDOSzhTW
T-Chinese (big5)	PDOSZhTW
U.S. English	PDOSenUS
French	PDOSfrFR
German	PDOSdeDE
Italian	PDOSitIT
Japanese (IBM-eucJP)	PDOSjaJP
Japanese	PDOSJaJP
Korean	PDOSkoKR
Spanish	PDOSesES

Product Notes

This section contains important information that you should consider when using PDOS.

Vulnerability of /var Running Out of Space

PDOS stores authorization policy information, audit logs, and error logs in the various directories under /var/pdos. It is strongly recommended that /var/pdos be created as a separate file system in order to ensure that user activity that might cause /var to become full does not impact PDOS's ability to enforce authorization policy. It is advisable to make /var/pdos/log and /var/pdos/audit separate file systems.

Problem with the Policy Director Runtime Library libpdsvcutl

When applications that invoke the PDOS LPM functionality exit, the Policy Director runtime library libpdsvcutl may core dump. This problem has only been reproduced on Solaris 2.6 machines at certain patch levels, but potentially it could occur at other OS levels and on AIX. The problem can be identified by core files with a stack that ends with a SEGV on the exit() of a process:

```
t@1 (l@1) terminated by signal SEGV (no mapping at the fault address)
(dbx) where
current thread: t@1
=>[1]0xef3babd8(0x2, 0x0, 0xef7f108c, 0xef5b89dc, 0xef623680, 0xef598d48),
 at 0xef3babd7
[2]_exithandle(0xef625af0, 0xef6294a4, 0x0, 0x0, 0x0, 0x0), at 0xef598d70
[3]exit(0x1, 0x0, 0xefffd680, 0x0, 0x0, 0x0), at 0xef608824
```

This problem is addressed by APAR IY18564, a fix to the Policy Director runtime.

Problem with the Policy Director Runtime Library libivadminapi.sl

The **pdoscfg** and **pdadmin** commands may fail to execute on some levels of HP-UX machines due to a problem with the Policy Director runtime library libivadminapi.sl. The problem can be identified by the occurrence of these error messages when the commands are executed:

```
# pdadmin
/usr/lib/dld.sl: Bad system id for shared library: /lib/libivadminapi.sl
/usr/lib/dld.sl: Exec format error
Abort(coredump)
```

The problem was introduced in the Tivoli SecureWay Policy Director 3.7 Fixpack 2 (patch 3.7-POL-0004) and in the Tivoli SecureWay Policy Director 3.7.1 release. The problem is addressed by APAR IY19537, a fix to the Policy Director runtime.

Solaris Patch Installation Failure

If during the installation of the patch on Solaris, the following error is displayed

```
patchadd PDOS000370-01
Checking installed patches...
One or more patch packages included in
PDOS000370-01 are not installed on this system.
Patchadd is terminating.
```

First check that PDOS has been installed on the system. If PDOS has been installed, then an operating system patch is needed.

For Solaris 2.6, the patch needed is 106125-10.

For Solaris 2.7, the patch needed is 107171-05.

rhost Field in pdoslpadm -r -f Report Sometimes Truncated

The ″rhost name″ field displayed by a full report of a user (using **pdoslpadm -r -f** <user>) may be truncated. The value of this field is dependent on support from the login applications being used and the OS platform. This field is for informational purposes only, and a truncated hostname will not affect the enforcement of Login Activity policy. (CMVC 7405)

Not Storing osseal UNIX User and Group in NIS Registry

PDOS defines a UNIX® user and a UNIX group (both named osseal). If PDOS is unable to resolve these names to their equivalent numeric ID when starting, PDOS will not start successfully. On installation PDOS defines these users and groups in the local system user and group registries. If you later enable NIS, make sure that the osseal user and group are left in the local system user and group registries.

When installing on a system configured to use NIS, the standard user creation mechanisms used during the PDOS installation process to create the osseal UNIX user and group might create the user and group after the + entry in the /etc/passwd and /etc/group files. If the osseal UNIX user and group are created after the + entry in the /etc/passwd and /etc/group files, you need to reorder the files to ensure that the osseal UNIX user and group entries appear before the +. Failure to reorder the files can result in PDOS failing to start if the NIS server is unavailable.

Policy Database Polling Interval and Registration for Policy Update Notification Defaults

The *PDOS Installation Guide* and the *PDOS Administration Guide* contain incorrect information about the PDOS policy database polling interval and the registration for policy update notification defaults.

The *PDOS Installation Guide* and the *PDOS Administration Guide* specify the default policy database polling interval as 10 minutes. This is incorrect. The default configuration is for PDOSD not to poll for policy database updates. The default value for the refresh-interval parameter of [pdosd] stanza in the PDOSD configuration file, /opt/pdos/etc/pdosd.conf is 0, not 10. The default value for the refresh_interval option of pdoscfg is 0.

The *PDOS Installation Guide* and the *PDOS Administration Guide* specify that by default PDOSD does not register for update notification. This is incorrect. The default configuration is for PDOS to register for policy update notifications and to listen for them on TCP port 7134. The default value for the ssl_listening_port option of the **pdoscfg** command is 7134, not 0.

Limiting the Number of Concurrent Policy Database Update Notifications

The number of concurrent policy database update notifications should be limited.

The Policy Director Management Server allows the configuration of the maximum number of concurrent policy update notifications that can be transmitted to database replicas. If registered for policy update notifications (the default), each configured and running PDOS machine receives policy updates by notification. Each notification consumes memory proportional to the size of the policy database. For large policy databases, it might be necessary to reduce the number of concurrent notifications from the default of 10 to ensure that the Policy Directory Management Server does not exhaust system resources on the machine on which it is running.

The maximum number of concurrent notifications is controlled by the **max-notifier-threads** configuration option in the [ivmgrd] stanza of the Policy Director Management Server's configuration file ivmgrd.conf. This file is located in the /opt/PolicyDirector/ivmgrd/lib directory on UNIX systems and in the ivmgrd/lib subdirectory of the Policy Director installation directory on Windows NT® machines.

Limiting the Number of Polling Policy Database Replicas

Polling policy database replicas should be limited.

The Policy Director Management Server can respond to up to 50 polls for policy updates concurrently. This Policy Director Management Server operational parameter is not configurable. For large policy databases, servicing this many policy updates concurrently might cause the Policy Director Management server to exhaust virtual memory resources on the machine on which it is running.

To avoid the Policy Director Management server exhausting virtual memory resources on the machine on which it is running, do not configure PDOS to poll for policy database updates. The default configuration is to not poll for policy database updates. Setting the polling interval to a large value does not eliminate the possibility of overloading the Policy Director Management server but reduces the likelihood of this situation arising. See "Documentation Additions and Changes" on page 69 for additional information.

Limiting the Set of Audit Logs Processed by pdosaudview

Depending on the configuration of the PDOS audit subsystem, the audit daemon (**pdosauditd**) can create many binary audit.log files in /var/pdos/audit. The normal operation of **pdosaudview** is to process all the audit.log files in /var/pdos/audit while searching for the particular records of interest. The more logs that are present, the longer **pdosaudview** takes to process them. Use the **–i** option to give the name of the actual audit.log to be processed.

For example, this command tells **pdosaudview** to search only the audit.log file, ignoring other rollover audit logs:

```
pdosaudview -i audit.log
```

PDOSD Space Errors on Overloaded HP-UX Systems

On overloaded HP-UX systems, you might see the following error message generated in the PDOSD log file /var/pdos/log/pdosd.log:

```
2000-12-01-17:48:32.863+00:00I----- 0x35A62686 \
 pdosd ERROR oss db hla_db_hash.c 924 0x00000015
An error occurred while fetching the entry
from the database: key  : status =  10.210.3.36 :
Not enough space : 12
```

This error message indicates that all of the system-wide address space available for shared data has been consumed. This situation arises when an excessive number of processes are running on the system. PDOS continues to operate normally in this situation.

PDOS Login Activity Policy with $HOME/.rhosts and /etc/hosts.equiv

The usage of the system file **$HOME/.rhosts** and **/etc/hosts.equiv** is discouraged when PDOS Login Activity Policy is configured. The behavior of this configuration depends on the platform.

On AIX systems, the **$HOME/.rhosts** and **/etc/hosts.equiv** result in the complete circumvention of PDOS Login Activity Policy, with programs that can use these files for authentication (**rlogin**, **rsh**, etc.). Other login policy (terminal, time of day, holiday) will still be enforced.

On PAM platforms, programs using these files for login authentication will fail to establish a login shell if PDOS Login Activity Policy is configured. These files cause the login program to not use the PDOS code for the authentication phase of the login, which does require initialization of the login session. This results in a PDOS denial of the login session in the Login Activity code. If PDOS auditing is configured, an audit event will be generated with an audit outcome of ″Failure″ and an audit view of ″Deny.″

PDOS Login Activity Policy on HP-UX 10x/11x with rexec/remsh

The PDOS Login Activity policy does not work with the HP-UX login programs **rexecd** and **remshd**. This is a limitation of the HP-UX 10 and 11 platforms, because these programs are not PAM enabled. Other login policy (terminal, time of day, holiday) will still

be applied. Login using **rexec** or **remsh** on an HP-UX machine should be disabled if there is a need to have Login Activity policy enforced.

These programs are PAM enabled in HP-UX release 11i, as described by the ″HP-UX 11i non-critical enhancement impacts″ web page (http://devresource.hp.com/STK/impactlist.html), in the ″rexecd, remshd - use PAM for authentication″ document. (CMVC 7341)

Creation of Local User Accounts with Minimum Password Age Policy

The specification of minimum password age policy can complicate the creation of new user accounts for locally defined users. New accounts are created with no password, and an administrator will set the password using the **passwd** command.

On AIX, when **passwd** is run by the administrator to change the password for a user account, the PDOS modules are not loaded and no enforcement of PDOS policy for password age of the passwords is performed. However, the password change time is set in the system files, and a flag is set in the local user database that requires the user to change their password on the next login. So, when a user attempts to log in, the system prompts for a new password, but the attempt to change the password fails because of the PDOS policy on minimum password age.

On Solaris and HP-UX, the password change date is also set when the administrator sets the password for an account. The user will be able to log in with the password set by the administrator but will be unable to change the password due to minimum password age policy.

The solution to both of these scenarios is to run the **pdoslpadm** tool with the **-m** option to explicitly set the password change date in effect to a date that allows the user to change their password without violating policy defined in PDOS. The administrator should perform the following steps to create a new local user account with a password that can be changed immediately by the user:

1. Create an account using system tools (for instance, **mkuser** on AIX, **useradd** on Solaris and HP-UX).
2. Set the password change date using **pdoslpadm -m** so that the age allows the change of the password without violating the PDOS minimum password age policy.

The user can then log in with the initial password and immediately change it without violating PDOS policy.

Protection Against System Crash During Startup

When PDOS is started, it will create a temporary file kosseal_starting___load in /tmp on AIX and HP-UX and in /var/tmp on Solaris. After PDOS's kernel extension is successfully loaded, this file is removed.

If this file is present when rc.osseal is run, PDOS will not start. This protects your system against the possibility of repeated crashes when the system loads the PDOS kernel extension when PDOS is configured to automatically start.

If this situation ever arises, PDOS will not start again until the file is removed. Before removing the file, however, ensure you save all necessary data about the system crash and report the crash to Tivoli Support so that it may be investigated by a support person.

pdosuidprog Can Fail on Circular Linked Directories

When executing the **pdosuidprog** utility without the **-s** flag, the utility will continue to follow a circularly linked directory structure until the operating system detects that there are too many levels of symbolic links. In certain cases, this can result in a large number of returned setuid/setgid programs and cause the utility to run for an extended period of time. In the case that such circular links exist, these links should be listed as being excluded from the search, and should be searched separately.

Known Product Limitations and Workarounds

This section describes known limitations and workarounds in the PDOS 3.7 Release and in the PDOS 3.7 Fixpack 1 Release. Please note that this might not be a complete list of limitations and workarounds.

AIX Message Catalogue Installation

On AIX, to ensure that the PDOS.msg package gets installed when you are installing the PDOS.rte package and the PDOS.msg.*language* package at the same time, it is recommended that APAR IY08023 (bos.rte.install fileset level 4.3.3.14 or higher) be installed on the system before installing the PDOS packages.

AIX NIS Client and PDOS Startup Order

On AIX systems, if the system is a NIS client, then the NIS client must be started prior to PDOS starting. This is the default when PDOS is configured for automatic start at system boot time. If you manually modify the **/etc/inittab** file after PDOS configuration, you must ensure the entry for PDOS comes after the entry for the NIS client.

Configuration During Policy Updates

The **pdoscfg** command might fail if policy updates are performed during the configuration process. This situation might arise if any of the following activities are occurring within the Policy Director domain at the same time as the configuration of a new PDOS system. They are listed in decreasing order of likelihood of causing the PDOS configuration to fail:

- Performing policy administration while configuring a PDOS system
- Configuring PDOS on the first system to subscribe to a new policy branch
- Unconfiguring a PDOS on a system specifying the ″-remove_per_policy yes″ option to the **pdosucfg** command
- Configuring PDOS as the second or later machine subscribing to an existing policy branch

- Unconfiguring PDOS on a system

If the PDOS configuration process fails because of concurrent policy updates, the **pdoscfg** command will fail, an error will be indicated in the **pdoscfg** error log /var/pdos/log/pdoscfg.log and you will need to restart the configuration by reissuing the **pdoscfg** command.

Server Connections Lost When Configuring

If the connection to the Policy Director Management Server or LDAP Server is lost during the configuration of a PDOS system, the **pdoscfg** command might fail with one of the following errors:

```
Policy Director command name_of_Policy_Director_command failed.
```

or

```
Registering with Policy Director failed with error code 1.
```

The **pdoscfg** command might not have been able to roll back some of the committed changes on these servers. If this happens, subsequent configurations fail because of this partial configuration. The following commands need to be issued when connections to the servers are restored:

1. Issue the following command on the system where the configuration failed:

   ```
   /opt/PolicyDirector/bin/svrsslcfg /dev/null –unconfig –n pdosd \
   –P sec_master_password
   ```

   where *sec_master_password* is your Policy Director Security Master password.

2. If this is the first PDOS system to specify this **branch** value, then issue:

   ```
   pdadmin> objectspace delete /OSSEAL/policy_branch
   ```

   where *policy_branch* is the name specified for the **pdoscfg –branch** value.

3. If this is the first PDOS system to be configured to this Policy Director Server, then issue:

   ```
   pdadmin> objectspace delete /OSSEAL
   ```

4. Reissue the configuration command.

pdoscfg May Affect Permissions

On a Solaris platform, the file permissions on /etc/name_to_sysnum may be affected after PDOS is configured. It should be verified that read permission for ″others″ is turned on.

pdosucfg Completes with Errors

The **pdosucfg** command completes PDOS unconfiguration even if errors are encountered during some of the unconfiguration steps. Some manual cleanup might need to be performed to complete the PDOS unconfiguration.

If **pdosucfg** reports that it completed with errors, check the /var/pdos/log/pdoscfg.log file for more information about the specific errors.

If errors were encountered when running the **svrsslcfg** command to unregister with Policy Director, on the system where unconfiguration failed, type the following **srvsslcfg** command on the command line:

```
/opt/PolicyDirector/bin/svrsslcfg  /dev/null –unconfig –n \
 pdosd –P sec_master_password
```

where *sec_master_password* is your Policy Director Security Master password. Ensure that the Policy Director Management server is operating normally before issuing the command.

If the **pdosucfg** option, remove_per_policy on, was specified and errors were encountered while unregistering the policy-specific policy information, type the following **pdadmin** command on the command line to complete the policy branch removal:

```
pdadmin> objectspace delete /OSSEAL/policy_branch
```

where *policy_branch* is the name that was specified for the **branch** value of the configuration. Ensure that the Policy Director Management server is operating normally before issuing the command.

If the **pdosucfg** option, remove_once_only on, was specified and errors were encountered when unregistering the Policy Director for Operating Systems product policy, type the following **pdadmin** command on the command line:

```
pdadmin> objectspace delete /OSSEAL
```

Ensure that the Policy Director Management server is operating normally before issuing the command.

HP-UX swremove Command Fails with Memory Allocation Error

The **swremove** command fails while removing PDOS from a system that has PDOS 3.7 Fixpack 1 applied. The following memory allocation error is displayed during the analysis phase of the installation.

```
Could not allocate memory for the agent, daemon or PC controller
serving this operation.
```

To remove PDOS, perform the following steps:

1. Install PDOS 3.7.0.0 with the force option.

   At the command line, type:

   ```
   swinstall -s /cd-rom/hp -x allow_downdate=true PDOSrte
   ```

2. At the command line, type:

   ```
   swremove PDOSrte
   ```

Limitations of Grace Login Enforcement

Grace login functionality is limited in an NIS environment. NIS does not provide a means of acquiring the password change time on an NIS client. The **pdoslpadm** tool allows the password change time to be explicitly set for a user activity record, but this will have to be done on every NIS client that is a PDOS node when the password is changed, in order to enforce grace login policy correctly.

The behavior when a maximum password age is specified with a grace logins value of 0 is different on AIX than on machines that support PAM (Solaris and HP-UX). When the password is expired and the grace logins value is 0, a user will be prompted to change

their password on all platforms, if the password is stored locally (not an NIS client or other security system that does not update shadow password entries).

If the machine is an NIS client and supports PAM, the user will be prompted for a new password, and if configured correctly, the password update will occur on the NIS server, but no other PDOS nodes that are NIS clients will be aware of the new password change date unless notified, as mentioned above. On AIX machines that are NIS clients, a login with an expired password when grace logins is set to 0 will fail. Logins will fail until a new password change time is set for the user.

Auditing of Native System Failed Logins

The PDOS LPM code attempts to generate audit events when a login failure occurs due to native authentication failures. This is done by means of a global state of the login process and by routines that are invoked when the shared modules that check the global state are unloaded. These routines are NOT invoked if the library is not unloaded when the login is terminated. Unfortunately, this is the case when a login attempt is terminated by a user entering ^C at the login prompt. For example, the following sequence will not generate an audit event for the login failure from the PDOS LPM:

1. User starts a login attempt, and receives ″login:″ prompt.
2. User enters invalid ID or password; login is denied.
3. User receives a login prompt.
4. User enters ^C, login process is terminated.

The net result is that the last failed system login attempt will not be audited if the login session is terminated with a ^C.

Auditing of Native System Failed Password Changes

For the current release of PDOS, failed attempts to change a password due to system restrictions (no matching old password, etc.) will NOT be audited by PDOS on the AIX platform.

Documentation Additions and Changes

Known defects in the documentation for this release of PDOS are listed below. The revised or corrected information is listed below the description of each documentation defect.

1. The *PDOS Administration Guide* contains incorrect information in Table 3, Wildcard Matching Examples. In the Pattern column, the entry /use/local/*.log is incorrect. The correct entry is /usr/local/*.log.

2. The *PDOS Installation Guide* and the *PDOS Administration Guide* contain incorrect information about the PDOS policy database polling interval and the registration for policy update notification defaults.

   The *PDOS Installation Guide* and the *PDOS Administration Guide* specify the default policy database polling interval as 10 minutes. This is incorrect. The default configuration is for PDOSD not to poll for policy database updates. The default value for the refresh-interval parameter of [pdosd] stanza in the PDOSD configuration file, /opt/pdos/etc/pdosd.conf is 0, not 10. The default value for the refresh_interval option of **pdosucfg** is 0.

   The *PDOS Installation Guide* and the *PDOS Administration Guide* specify that by default PDOSD does not register for update notification. This is incorrect. The default configuration is for PDOS to register for policy update notifications and to listen for them on TCP port 7134. The default value for the ssl_listening_port option of the **pdoscfg** command is 7134, not 0.

3. In Chapter 3 of the *PDOS Administration Guide*, two headers under **PDOS Initial Policy** need to be changed. On the bottom of page 59, the **osseal-audit** header should say **osseal-credentials**. At the top of page 60, the **osseal-credentials** header should say **osseal-audit** (CMVC-6259).

4. A sample usage of the **-a** option should be added to the syntax listing for the **pdosaudview** command on page 92 of the *PDOS Administration Guide*. Place the following after the **-w** syntax option and before the **-r** syntax option:

   [-a action]

Also on page 92, the syntax listing for the **pdosaudview** command contains a duplicate line [-s YYYY-MM-DD{-hh:mm:ss}]. This duplicate line should be removed. (CMVC-6259)

5. There is an error in the example under **Local and Remote Terminals** on page 34 of the *PDOS Administration Guide*. (CMVC-7253)

   In the second line, ″hostspec″ should be used instead of ″device.″

   ```
   /OSSEAL/policy-branch \
   /Login/Teminal/Remote/termgroup/hostspec.
   ```

6. A description of the **-s** option is missing from the **pdosobjsig** command on page 111 of the *PDOS Administration Guide*. (CMVC-7548)

   There should be a line just prior to the -S that reads:

   ```
   -s Updates the state of a single object in the database
   ```

7. A paragraph separator is missing from the description of the **pdosrgyimp** command in the *PDOS Administration Guide*. (CMVC-7594)

   In the fourth paragraph on page 115, there should be a new paragraph after the following sentence:

   ″The -E option eliminates a specific set of users and groups found in the UNIX registry.″

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.