Contents

Tables................................................................................... xi

Preface ........................................................................... xiii
   Who Should Read This Guide ............................................... xiii
   What This Guide Contains .................................................... xiii
   Publications ...................................................................... xiv
      Tivoli Policy Director for Operating Systems Library .............. xiv
      Prerequisite Publications ................................................... xv
      Accessing Publications Online .......................................... xv
      Ordering Publications ........................................................ xv
      Providing Feedback about Publications .............................. xv
   Contacting Customer Support ............................................. xv
   Conventions Used in This Book ............................................. xvi
      Typeface Conventions ...................................................... xvi
      Operating System-dependent Variables and Paths .................. xvi

Chapter 1. Introduction .......................................................... 1
   Understanding Tivoli Policy Director for Operating Systems .......... 1
   Environment ..................................................................... 2
      Databases ................................................................... 2
   Authorization Model ......................................................... 3
      The UNIX Identity and Its Relationship to the Tivoli Policy Director User Identity 3
   Authorization Policy ........................................................... 4

Chapter 2. Policy ................................................................. 5
   Protected Object Name Structure ........................................... 5
      Namespace Root ............................................................ 5
      Policy Branch ................................................................ 6
      Resource Types ............................................................ 6
      Object Name .................................................................. 6
      Wildcarding .................................................................... 6
   Access Controls .................................................................. 8
      Access Control Lists ........................................................ 9
      Inheritance and Traversal ............................................... 12
   Protected Object Policies .................................................. 13
      POP Attributes Used for Access Control ......................... 13
   Access Restrictions ........................................................... 15
Chapter 4. Administrative Tasks

Defining Runtime Administrators and Auditors

Establishing a Consistent Username Space

Identifying Users and Groups

Identifying Duplicate User Names

Using pdosrgyimp

Tuning the Configuration

Managing Tivoli Policy Director for Operating Systems Processes

Starting Tivoli Policy Director for Operating Systems

Stopping Tivoli Policy Director for Operating Systems

Checking Daemon Status

Daemon Log Files

Verifying Policy

Using Warning Mode to Verify Policy

Using Auditing to Verify Policy

Managing the Trusted Computing Base

Tuning the PDOSD Daemon’s TCB Monitoring

Managing the Object Signature Database

Managing Login Activity Policy

Viewing Account Records

Locking and Unlocking Accounts

Password Change Date for User Accounts

Creation of Local User Accounts with Minimum Password Age Policy
Chapter 5. Tasks Available from Tivoli Desktop .......................... 89

Task Overview ................................................................ 89

General Information Regarding wrunjob and wruntask ..................... 91

Add/Remove PDOS Auditors/Administrators .................................... 91
    Syntax for wrunjob and wruntask ........................................ 92

Backup PDOS Database ......................................................... 93
    Syntax for wrunjob and wruntask ........................................ 94

Certificate Transfer Utility ........................................................ 94
    Syntax for wrunjob and wruntask ........................................ 95

Configure PDOS Auditing ........................................................ 96
    Syntax for wrunjob and wruntask ........................................ 96

Configure PDOS Caching ........................................................ 97
    Syntax for wrunjob and wruntask ........................................ 97

Configure PDOS Logging ........................................................ 98
    Syntax for wrunjob and wruntask ........................................ 99

Configure PDOS Login and Password Policy ...................................... 100
    Syntax for wrunjob and wruntask ....................................... 101

Configure PDOS Server ........................................................... 101
    Syntax for wrunjob and wruntask ...................................... 102

Configure PDOS TCB ............................................................. 103
    Syntax for wrunjob and wruntask ...................................... 104

Display PDOS Hostname Cache .................................................. 105
    Syntax for wrunjob and wruntask ...................................... 105

Import UNIX TCB .................................................................. 106
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax for wrunjob and wruntask</td>
<td>106</td>
</tr>
<tr>
<td>Import UNIX Users and Groups</td>
<td>107</td>
</tr>
<tr>
<td>Syntax for wrunjob and wruntask</td>
<td>108</td>
</tr>
<tr>
<td>Manage PDOS Credential Cache</td>
<td>109</td>
</tr>
<tr>
<td>Syntax for wrunjob and wruntask</td>
<td>110</td>
</tr>
<tr>
<td>Manage PDOS Server State</td>
<td>110</td>
</tr>
<tr>
<td>Syntax for wrunjob and wruntask</td>
<td>111</td>
</tr>
<tr>
<td>Manage PDOS TCB</td>
<td>111</td>
</tr>
<tr>
<td>Syntax for wrunjob and wruntask</td>
<td>112</td>
</tr>
<tr>
<td>Migrate TACF to PDOS</td>
<td>112</td>
</tr>
<tr>
<td>Syntax for wrunjob and wruntask</td>
<td>113</td>
</tr>
<tr>
<td>Purge PDOS Hostname Cache</td>
<td>114</td>
</tr>
<tr>
<td>Syntax for wrunjob and wruntask</td>
<td>114</td>
</tr>
<tr>
<td>Query PDOS Login and Password Policy</td>
<td>115</td>
</tr>
<tr>
<td>Syntax for wrunjob and wruntask</td>
<td>116</td>
</tr>
<tr>
<td>Query PDOS Server State</td>
<td>117</td>
</tr>
<tr>
<td>Syntax for wrunjob and wruntask</td>
<td>117</td>
</tr>
<tr>
<td>Query PDOS TCB</td>
<td>117</td>
</tr>
<tr>
<td>Syntax for wrunjob and wruntask</td>
<td>118</td>
</tr>
<tr>
<td>Restore PDOS Database</td>
<td>118</td>
</tr>
<tr>
<td>Syntax for wrunjob and wruntask</td>
<td>119</td>
</tr>
<tr>
<td>Set PDOS Server Audit Level</td>
<td>119</td>
</tr>
<tr>
<td>Syntax for wrunjob and wruntask</td>
<td>120</td>
</tr>
<tr>
<td>Set PDOS Server Trace Level</td>
<td>121</td>
</tr>
<tr>
<td>Syntax for wrunjob and wruntask</td>
<td>121</td>
</tr>
<tr>
<td>Setup TEC Event Server for PDOS</td>
<td>122</td>
</tr>
<tr>
<td>Syntax for wrunjob and wruntask</td>
<td>123</td>
</tr>
<tr>
<td>Show PDOS Auditing Configuration</td>
<td>124</td>
</tr>
<tr>
<td>Syntax for wrunjob and wruntask</td>
<td>124</td>
</tr>
<tr>
<td>Show PDOS Auditors/Administrators</td>
<td>125</td>
</tr>
<tr>
<td>Syntax for wrunjob and wruntask</td>
<td>125</td>
</tr>
<tr>
<td>Show PDOS Caching Configuration</td>
<td>126</td>
</tr>
<tr>
<td>Syntax for wrunjob and wruntask</td>
<td>126</td>
</tr>
<tr>
<td>Show PDOS Logging Configuration</td>
<td>126</td>
</tr>
<tr>
<td>Syntax for wrunjob and wruntask</td>
<td>126</td>
</tr>
<tr>
<td>Show PDOS Server Audit Level</td>
<td>127</td>
</tr>
<tr>
<td>Syntax for wrunjob and wruntask</td>
<td>127</td>
</tr>
</tbody>
</table>
## Tables

1. Wildcard Elements ............................................................... 6
2. Wildcard Matching Examples ....................................................... 7
3. Wildcard Element Precedence Rules .................................................. 7
4. Wildcard Pattern Precedence Examples ................................................ 8
5. Permissions Defined in the OSSEAL Action Group ...................................... 11
6. Tivoli Policy Director Primary Actions Used for Policy Management ................. 11
7. Policy Director Primary Actions Used for Policy Decisions ................................ 11
8. File System Objects ................................................................ 17
9. File Permissions .................................................................... 18
10. Login Programs Certified for Tivoli Policy Director for Operating Systems .......... 24
11. System Programs Defined as Immune-Programs in Default Policy ..................... 27
12. Network Resource Naming ........................................................ 28
13. Valid Permission for Incoming or Outgoing Connection to a Network Resource .... 29
14. Definitions of Terms about Terminals ................................................ 34
15. Valid Permission to Log In ........................................................ 35
16. Login Activity Policy Attributes .................................................... 36
17. Surrogate Object Naming ......................................................... 40
18. Surrogate Operation Permission .................................................... 40
19. Sudo Objects .................................................................. 42
20. Sudo Command Attributes ........................................................ 42
21. Permission Required for Sudo ....................................................... 43
22. Extended Sudo Attributes for Fine-grained Control ...................................... 44
23. Environment Variables Stripped by Sudo ............................................. 46
24. Environment Variables Set by Sudo ................................................. 47
25. PDOS Credential Configuration Attributes ............................................ 51
26. Configuration Attributes Controlling PDOSD’s Communications with the User Registry 52
27. Authorization Configuration Attributes ............................................... 53
28. Authorization Policy-branch Configuration Attribute ................................... 54
29. PDOSD TCB File Monitoring Resource Configuration Attributes .................... 55
30. PDOSD Log Configuration Attributes ................................................ 56
31. Global Audit Level Configuration Attribute .......................................... 56
32. PDOSAUDITD Configuration Attributes ............................................ 57
33. PDOSWDD Configuration Attributes ................................................ 58
34. PDOSTECD Configuration Attributes ................................................. 59
35. Attribute Equivalents of `pdoscf` Options in osseal.conf ................. 74
36. Attribute Equivalents of `pdoscf` Options for pdosd.conf ........... 74
37. Attribute Equivalents of `pdoscf` Options in pdosauditd.conf ........... 75
38. Attribute Equivalents of `pdoscf` Options in pdoswdd.conf ........... 75
39. `pdoscf` Options that Control the Daemon Log Files .................................... 77
40. Authorization for Tivoli Policy Director for Operating Systems Tasks ................ 90
41. Global Audit Levels ............................................................... 132
42. General Audit Event Record Type ................................................... 137
43. Description of Audit Event Identifiers ................................................ 141
44. Description of Audit Qualifiers ....................................................... 142
45. Trace Audit Event Record Type ....................................................... 142
46. Logout Audit Event Record Type ..................................................... 144
47. System Resources and Corresponding Tivoli Policy Director for Operating Systems Resource Types .......................................................... 205
49. Policy Director Primary Actions Used for Policy Management ............................ 206
50. Policy Director Primary Actions Used for Policy Decisions ............................ 206
51. Special Elements of Wildcard Character Set .......................................... 207
52. Wildcard Character Set Character Classes Valid for all Locales ....................... 208
53. Process Related Tivoli Enterprise Console Events ...................................... 211
54. File Related Tivoli Enterprise Console Events ......................................... 213
55. Network Related Tivoli Enterprise Console Events ....................................... 214
56. Sudo Related Tivoli Enterprise Console Events ........................................ 215
57. Set(User) Related Tivoli Enterprise Console Events .................................... 216
58. Set(Group) Related Tivoli Enterprise Console Events ................................... 217
59. TCB Related Tivoli Enterprise Console Events ........................................ 217
60. Policy Related Tivoli Enterprise Console Events ....................................... 219
61. Login Related Tivoli Enterprise Console Events ....................................... 219
62. Credential Related Tivoli Enterprise Console Events .................................... 220
Preface

The *Tivoli Policy Director for Operating Systems Administration Guide* describes how to use Tivoli Policy Director for Operating Systems and provides a reference of the available commands.

**Who Should Read This Guide**

This guide is intended for systems administrators who have some knowledge of these topics:

- UNIX® operating system
- Internet protocols, including HTTP, TCP/IP, FTP, TELNET, SSL
- Security management
- Directory services
- Authentication
- Authorization
- Tivoli Policy Director

Supplementary information that systems administrators may find useful includes knowledge of the following topics:

- Tivoli Management Environment framework
- Tivoli Distributed Monitoring
- Tivoli Enterprise Console®
- Tivoli Risk Manager
- Tivoli Security Manager
- Tivoli User Administration

**What This Guide Contains**

The *Tivoli Policy Director for Operating Systems Administration Guide* contains the following sections:

- **Chapter 1, “Introduction” on page 1**
  Introduces Tivoli Policy Director for Operating Systems and its functions.

- **Chapter 2, “Policy” on page 5**
  Describes the resources Tivoli Policy Director for Operating Systems provides protection for, and helps you plan your protection requirements.

- **Chapter 3, “Runtime” on page 49**
  Describes the Tivoli Policy Director for Operating Systems runtime components and their environment. This chapter describes the Tivoli Policy Director for Operating Systems daemons.

- **Chapter 4, “Administrative Tasks” on page 71**
  Explains the administrative tasks required to manage Tivoli Policy Director for Operating Systems.
What This Guide Contains

- **Chapter 5, “Tasks Available from Tivoli Desktop” on page 89**
  Describes the management tasks provided to allow Tivoli Policy Director for Operating Systems to be managed with the Tivoli desktop.

- **Chapter 6, “Auditing” on page 131**
  Explains how to use the auditing functions to track access to protected functions and monitor activity.

- **Chapter 7, “Commands” on page 147**
  Provides a reference of all the Tivoli Policy Director for Operating Systems commands. It lists each command and its syntax, options, and usage.

- **Chapter 8, “Integrating with Tivoli Enterprise Console” on page 197**
  Describes how Tivoli Policy Director for Operating Systems can be integrated with Tivoli Enterprise Console.

- **Chapter 9, “Integrating with Tivoli Risk Manager” on page 201**
  Describes how Tivoli Policy Director for Operating Systems can be integrated with Tivoli Risk Manager.

- **Appendix A, “Policy Quick Reference” on page 205**
  Provides a quick reference of the policy resources and permissions.

- **Appendix B, “Wildcard Character Set Expressions” on page 207**
  Lists and defines the wildcard character set expressions.

- **Appendix C, “Tivoli Enterprise Console Events” on page 209**
  Describes the events sent to Tivoli Enterprise Console.

- **Appendix D, “Messages” on page 221**
  Provides a list of the messages in Tivoli Policy Director for Operating Systems along with a detailed explanation and a suggested action to be taken.

Publications

This section lists publications in the *Tivoli Policy Director for Operating Systems* library and any other related documents. It also describes how to access Tivoli publications online, how to order Tivoli publications, and how to make comments on Tivoli publications.

**Tivoli Policy Director for Operating Systems Library**

The following documents are available in the *Tivoli Policy Director for Operating Systems* library:

- *Tivoli Policy Director for Operating Systems Installation Guide*
  Provides information about installing Tivoli Policy Director for Operating Systems.

- *Tivoli Policy Director for Operating Systems Administration Guide*
  Provides information on using Tivoli Policy Director for Operating Systems and includes a reference of the commands available.

- *Tivoli Policy Director for Operating Systems Release Notes*
  Provides late-breaking information about Tivoli Policy Director for Operating Systems.
Prerequisite Publications

To be able to use the information in this guide effectively, you must have some prerequisite knowledge, which you can get from the following books:

- Tivoli SecureWay® Policy Director Base Administration Guide, Version 3.8
- Tivoli SecureWay Policy Director Base Installation Guide, Version 3.8
- Tivoli SecureWay Policy Director Release Notes, Version 3.8

Accessing Publications Online

You can access many Tivoli publications online at the Tivoli Customer Support Web site:
http://www.tivoli.com/support/documents/

These publications are available in PDF or HTML format, or both. Translated documents are also available for some products.

Ordering Publications

You can order many Tivoli publications online at the following Web site:
http://www.ibm.com/shop/publications/order

You can also order by telephone by calling one of these numbers:

- In the United States: 800-879-2755
- In Canada: 800-426-4968
- In other countries, for a list of telephone numbers, see the following Web site:
  http://www.tivoli.com/inside/store/lit_order.html

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 an e-mail to pubs@tivoli.com.
- Complete our customer feedback survey at the following Web site:
  http://www.tivoli.com/support/survey/

Contacting Customer Support

If you have a problem with any Tivoli product, you can contact Tivoli Customer Support. See the Tivoli Customer Support Handbook at the following Web site:

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

The handbook provides information about how to contact Tivoli Customer Support, depending on the severity of your problem, and the following information:

- Registration and eligibility
- Telephone numbers and e-mail addresses, depending on the country you are in
- What information you should gather before contacting support
Conventions Used in This Book

This book uses several conventions for special terms and actions, operating system-dependent commands and paths, and margin graphics.

Typeface Conventions

The following typeface conventions are used in this book:

**Bold**

Lowercase and mixed-case commands, command options, and flags that appear within text appear like this, in bold type.

Graphical user interface elements (except for titles of windows and dialogs) and names of keys also appear like this, in **bold** type.

*Italic*

Variables, values you must provide, new terms, and words and phrases that are emphasized appear like *this*, in *italic* type.

**Monospace**

Commands, command options, and flags that appear on a separate line, code examples, output, and message text appear like this, in monospace type.

Names of files and directories, text strings you must type, when they appear within text, names of Java methods and classes, and HTML and XML tags also appear like this, in monospace type.

Operating System-dependent Variables and Paths

This book uses the UNIX convention for specifying environment variables and for directory notation.

When using the Windows command line, replace `$variable` with `%variable%` for environment variables and replace each forward slash (`/`) with a backslash (`\`) in directory paths.

**Note:** If you are using the bash shell on a Windows system, you can use the UNIX conventions.
Introduction

Welcome to the Tivoli Policy Director for Operating Systems Administration Guide. This book contains detailed information about Tivoli Policy Director for Operating Systems and describes the environment, authorization model, and the commands provided.

This chapter provides an overview of the product and describes the environment so that you are better equipped to plan for and enforce authorization policy on your systems.

Understanding Tivoli Policy Director for Operating Systems

Tivoli Policy Director for Operating Systems 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, mechanisms are provided to verify defined policy and audit authorization decisions.

Access controls are stored in a policy database that is centrally maintained in the Tivoli 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, Tivoli Policy Director for Operating Systems performs an authorization check based on the accessing user’s identity, the action, and the resource’s access controls to determine if access should be permitted or denied.
Environment

Tivoli Policy Director for Operating Systems functions in a Tivoli Policy Director environment, as shown in Figure 1.

Tivoli Policy Director is a network-based authorization framework that provides a backbone for defining, managing, and enforcing authorization policy. Multiple resource managers can use this framework. Tivoli Policy Director for Operating Systems is one of the resource managers that use the authorization service provided by Tivoli Policy Director. Other resource managers include WebSEAL and Tivoli Policy Director for MQSeries. Tivoli Policy Director is administered through a central server that all resource managers can access. This lets an administrator control policy for a large number of similar machines from one central location. Tivoli Policy Director for Operating Systems is installed on each machine that you want to protect.

Databases

The Tivoli Policy Director environment includes two main databases used by the resource managers. The first database, the Tivoli Policy Director user registry, stores the user and group definitions and is used for managing and identifying users in the Tivoli Policy Director environment. For Tivoli Policy Director for Operating Systems, the Tivoli Policy Director environment must be set up to use an LDAP user registry. The second database, the Tivoli Policy Database, stores all of the policy defined for each of the resource managers to enforce security. The policy database is where the access controls are stored. Resource managers access these two databases over a network using TCP, secured by Secure Socket
Layers (SSL). In addition to the databases, Tivoli Policy Director provides a standardized authorization API by which all authorization decisions are made.

Although Tivoli Policy Director for Operating Systems relies on the information stored in the centrally maintained Tivoli Policy Director databases, the information required to make authorization decisions is replicated and cached to enable authorization policy to continue to be enforced even if the Tivoli Policy Director server or the Tivoli Policy Director user registry server becomes inaccessible. See Chapter 3, “Runtime” on page 49 for a discussion of these topics.

Authorization Model

Tivoli Policy Director for Operating Systems components operate in the user level application space and also within the UNIX kernel. The Tivoli Policy Director for Operating Systems kernel extension and user level components interact in a tightly integrated secure manner to provide an extended layer of authorization enforcement. Applications access system resources through system provided APIs, which eventually arrive in the UNIX kernel through a variety of mechanisms.

On a system not protected by Tivoli Policy Director for Operating Systems, the native system’s security verifies whether the accessing user’s native identity has authorization to perform the requested action and either carries out the operation or denies it.

The primary function of the kernel extension is to intervene in accesses to resources that are subject to the authorization policy. The kernel extension uses the authorization daemon process, PDOSD, to obtain an authorization decision and then enforces that decision. If the policy permits access to the resource, the operation continues and is then subject to the native system’s security. Otherwise the resource access is denied.

The PDOSD daemon maps UNIX user identities to Tivoli Policy Director credentials that describe users and their group memberships from a Tivoli Policy Director point of view. The PDOSD daemon then utilizes the Tivoli Policy Director Authorization API to obtain authorization decisions based on the credentials, the operation being performed, the resource being accessed, and its associated access controls defined in the policy database.

The UNIX Identity and Its Relationship to the Tivoli Policy Director User Identity

To acquire the credentials needed to make an authorization decision, the accessing user’s native numerical UNIX ID must be mapped to a Tivoli Policy Director user. The user’s UNIX username is obtained from the system’s native User Registry using the numerical ID. This username is mapped one-to-one to a Tivoli Policy Director user of the same name to retrieve credentials from the Tivoli Policy Director user registry. These credentials define the user’s identity and group membership. If there is no Tivoli Policy Director user corresponding to the user’s native username, then the user is treated as unauthenticated when making authorization decisions. Users with disabled accounts are also treated as unauthenticated.

All systems sharing the same Tivoli Policy Director environment should use a consistent and distinct native username for each real user in the environment.

For example, assume Sally Smith has a username of sally on Machine A and a username of ssmith on Machine B. She will be mapped to two different Tivoli Policy Director users depending on which machine she logs into; this might affect the resources she can access.
Conversely, assume Sally Smith has the UNIX username sally on machine A. User Sally Doe has the UNIX username of sally on machine C. Both Sally Smith and Sally Doe will get mapped to the same Tivoli Policy Director user. Either of these situations might compromise your security policy.

Credentials are initially retrieved or refreshed from the Tivoli Policy Director user registry when a user logs into a UNIX system using a Tivoli Policy Director for Operating Systems supported and defined login program while Tivoli Policy Director for Operating Systems is running. All authorization decisions made for operations performed by processes subsequently run by this user are made using these credentials. This is true even for processes that change their effective user ID, for example, programs that perform setuid() calls or programs run after successfully performing an su command.

Authorization Policy

Setting up authorization policy involves identifying the system resources that require protection and the degree of protection needed. A security policy is successfully implemented when the appropriate access controls are applied on the resources requiring protection.

The term access controls is used consistently throughout this document to refer to the various kinds of authorization policy that can be used to protect system resources. Access controls include:

Access Control List (ACL)
  Identifies specific users, groups of users, and types of users who can be considered for access and specifies the operations permitted on the resource.

Protected Object Policies (POP)
  Specifies conditions on access to the protected objects, such as auditing, warning mode, and time-of-day access.

Extended Attributes
  Additional values placed on an object, ACL, or POP that further restrict the access such as limiting what programs can be used to access a resource.

Examples of establishing policy in this book are illustrated using the Tivoli Policy Director pdadmin command. These examples are always prefaced with the prompt pdadmin>. For additional information about establishing policy in Tivoli Policy Director and the pdadmin command, see Tivoli SecureWay Policy Director Base Administration Guide.

In order to establish an effective authorization policy, you should do the following:

- Understand your systems resources
- Identify the key resources that need to be protected
- Identify the types of users requiring access to these resources
- Understand the available Tivoli Policy Director for Operating Systems options for securing the resources
Policy

Tivoli Policy Director for Operating Systems protects system resources by enforcing authorization policy defined in terms of Tivoli Policy Director access controls. Access to the following types of system resources can be controlled:

- File system resources
- Remote network services
- Local network services
- Login services
- Changes of user and group identity
- Sudo commands

These resources are identified by Tivoli Policy Director object names. They are protected by associating Tivoli Policy Director access controls with the object name.

The following sections discuss how Tivoli Policy Director object names and access controls are used to define authorization policy for the system resources Tivoli Policy Director for Operating Systems protects.

Protected Object Name Structure

Every resource has a protected object name that identifies the resource to Tivoli Policy Director. After a protected object name has been defined in Tivoli Policy Director, you can assign an access control to it. Protected object names are comprised of the following main parts:

- Namespace root
- Policy branch
- Resource type
- Object name

Each of the parts of a protected object name are described below.

Namespace Root

Every resource manager under Tivoli Policy Director has a namespace where all resource definitions are rooted. The namespace for Tivoli Policy Director for Operating Systems is OSSEAL. All protected machines or nodes use OSSEAL. The OSSEAL namespace is /OSSEAL.
Policy Branch

Your environment probably has several machines that require the same or similar authorization policy because they are used for the same or similar purposes. Tivoli Policy Director for Operating Systems lets you group the policy for similar machines under user-defined policy branches. Machines are configured to subscribe to a particular policy branch. All machines subscribing to the same policy branch are subject to the same authorization policy. The policy branch is specified by the element of the object name immediately following the /OSSEAL root. The administrator determines the name of the policy branches. When referred to generically in the remainder of this document, the policy branch is referred to as /OSSEAL/policy-branch.

Assume you have three classes of systems: servers, workstations and test machines, each with different security requirements. You could define a policy branch for each class:

/OSSEAL/Servers
/OSSEAL/Workstations
/OSSEAL/Test

Resource Types

Beneath a policy branch lie all the resource types that can be protected. Resource types include system resources such as files and directories or other resources such as Sudo commands, Surrogate actions, and Network resources. The resource type specifies what kind of resource is being protected. For example, the protected object name for all protected file system resources could start as follows: /OSSEAL/policy-branch/File.

Similarly, the protected object name for all Trusted Computing Base (TCB) secure files could start as follows:

/OSSEAL/policy-branch/TCB/Secure-Files

Object Name

Beneath the resource type are the actual resources themselves. Each resource type has specific objects that can be protected. For example, File resources protect files and directories. This is the lowest level of a protected object name because it defines a single resource.

For file system resources the object name is the file or directory name. For network resources the object name is the specified host and service information. Each of the resource types specifies the information that identifies specific instances of that resource in this part of the object name.

Many of the object names can represent system resources with names matching a wildcard pattern. The basic elements of the wildcard patterns are described in Table 1. Each resource that makes use of wildcard patterns does so in different ways. "Protected System Resources" on page 16 describes how each specific resource makes use of wildcarding.

Wildcarding

You can use wildcards to protect resources collectively that are not contained in a hierarchy. For example, all files ending in .log or all host names beginning with www. Table 1 describes the basic elements that make up a wildcard pattern.

Table 1. Wildcard Elements

<table>
<thead>
<tr>
<th>Wildcard Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Matches a string of any length of characters, including slash (/) characters.</td>
</tr>
<tr>
<td>?</td>
<td>Matches any single character.</td>
</tr>
</tbody>
</table>
Table 1. Wildcard Elements (continued)

<table>
<thead>
<tr>
<th>Wildcard Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>Matches one or more occurrences of the previous element.</td>
</tr>
<tr>
<td>[set of characters]</td>
<td>Matches a single character that is one of the set of characters. The set of characters is specified according to the POSIX wildcard expansion rules. For example, [a-z] matches any ASCII character in the range from a to z.</td>
</tr>
<tr>
<td>a character</td>
<td>Matches the exact character specified.</td>
</tr>
</tbody>
</table>

Use a backslash (\) to inhibit the special significance of the following character. You can use two backslashes (\\) when you need to match a single backslash. Table 2 shows some wildcard patterns that match and some that do not match.

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Matching strings</th>
<th>Non-matching strings</th>
</tr>
</thead>
<tbody>
<tr>
<td>a*</td>
<td>a</td>
<td>ba</td>
</tr>
<tr>
<td></td>
<td>aa</td>
<td>q a over the dog</td>
</tr>
<tr>
<td></td>
<td>a quick brown fox</td>
<td></td>
</tr>
<tr>
<td>a*</td>
<td>a*</td>
<td>ab</td>
</tr>
<tr>
<td></td>
<td>a</td>
<td>ab</td>
</tr>
<tr>
<td>a?</td>
<td>aa</td>
<td>a</td>
</tr>
<tr>
<td></td>
<td>al</td>
<td>aaa</td>
</tr>
<tr>
<td>/usr/local/*.log</td>
<td>/usr/local/x.log</td>
<td>/usr/local/x.log.1</td>
</tr>
<tr>
<td></td>
<td>/usr/local/app/x.log</td>
<td></td>
</tr>
<tr>
<td>*.charity.org</td>
<td><a href="http://www.charity.org">www.charity.org</a></td>
<td><a href="http://www.charity.org.com">www.charity.org.com</a></td>
</tr>
<tr>
<td></td>
<td>ftp.charity.org</td>
<td></td>
</tr>
<tr>
<td>[:alpha:]+</td>
<td>abcd</td>
<td>/abcd</td>
</tr>
<tr>
<td></td>
<td>ABCD</td>
<td>tty0</td>
</tr>
<tr>
<td>* *</td>
<td>(There is a space between the asterisks)</td>
<td>a b</td>
</tr>
</tbody>
</table>

Wildcard precedence

For each kind of resource that makes use of wildcard patterns, Tivoli Policy Director for Operating Systems needs to determine which wildcard pattern to apply. For example, assume that there are two patterns:

/usr/local/*.log

and

/usr/local/user1/*.log

The string /usr/local/user1/x.log matches both of these patterns.

To resolve this ambiguity, precedence rules are applied. The more specific a pattern the higher its precedence. According to this principal /usr/local/user1/x.log is matched against the /usr/local/user1/*.log pattern before the /usr/local/*.log pattern. Because a match is found, any policy applicable to objects matching this pattern will apply. Table 3 on page 8 shows the precedence of wildcard elements. Elements higher in the table have precedence over elements lower in the table.
Table 3. Wildcard Element Precedence Rules

<table>
<thead>
<tr>
<th>Precedence</th>
<th>Element</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Exact character</td>
<td>a, *, \</td>
</tr>
<tr>
<td>2</td>
<td>Character range</td>
<td>[Aa], [:digit:]</td>
</tr>
<tr>
<td>3</td>
<td>Arbitrary character</td>
<td>?</td>
</tr>
<tr>
<td>4</td>
<td>Repeated exact characters</td>
<td>a+</td>
</tr>
<tr>
<td>5</td>
<td>Repeated character range</td>
<td>[Aa]+, [:digit:]+</td>
</tr>
<tr>
<td>6</td>
<td>Repeated arbitrary character</td>
<td>?+</td>
</tr>
<tr>
<td>7</td>
<td>Arbitrary string</td>
<td>*</td>
</tr>
</tbody>
</table>

Depending on the kind of resource, the precedence is determined by comparing the patterns, element by element, from beginning to end or in reverse. Patterns for matching file names are compared from beginning to end. Patterns for matching host names are compared from end to beginning.

For two patterns otherwise considered equal, the longer pattern is considered more specific than the shorter pattern unless the longer string is longer because of an asterisk (*).

Examples of Wildcard Precedence

Table 4 shows file name and host name wildcard patterns arranged from highest precedence to lowest.

Table 4. Wildcard Pattern Precedence Examples

<table>
<thead>
<tr>
<th>Precedence</th>
<th>File name pattern</th>
<th>Host name pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>log/0[0-9]/error</td>
<td><a href="http://www.%5Ba-z%5Dtv.com">www.[a-z]tv.com</a></td>
</tr>
<tr>
<td>2</td>
<td>log/0?/error</td>
<td><a href="http://www.?tv.com">www.?tv.com</a></td>
</tr>
<tr>
<td>3</td>
<td>log/0*/error</td>
<td><a href="http://www.*tv.com">www.*tv.com</a></td>
</tr>
<tr>
<td>4</td>
<td>log/[0-9]+/error.1</td>
<td>www-help.[a-z]+v.com</td>
</tr>
<tr>
<td>5</td>
<td>log*/error.1</td>
<td>www-help.*v.com</td>
</tr>
<tr>
<td>6</td>
<td>log*/error.1</td>
<td>www-help.*.com</td>
</tr>
<tr>
<td>7</td>
<td>log*/error</td>
<td><a href="http://www.*.com">www.*.com</a></td>
</tr>
<tr>
<td>8</td>
<td>log*/error*</td>
<td>*<a href="http://www.*.com">www.*.com</a></td>
</tr>
<tr>
<td>9</td>
<td>log*</td>
<td>*.com</td>
</tr>
<tr>
<td>10</td>
<td>*</td>
<td>*</td>
</tr>
</tbody>
</table>

When the only difference between two patterns is the characters specified in a character set, precedence is determined by lexically comparing the two strings containing the patterns. This needs to be taken into account only if the character sets to be matched have some of the same characters. If there are no common characters between the two sets, any given string can match at most one of the patterns.

Access Controls

Policy Director provides two basic kinds of access controls:

Access Control Lists

Access Control Lists (ACLs) define access controls based on a user’s identity and action performed or attempted.
Protected Object Policies

Protected Object Policies (POPs) define access controls based on other information (such as the time an access is occurring) and control aspects of an authorization decision such as whether or not the decision should be audited.

Access controls are applied by defining ACLs and POPs and then attaching them to objects. The name of the object (the Protected Object Name) represents the resource being protected.

Tivoli Policy Director provides two ways of defining the set of objects that may be protected: dynamically by a resource discovery mechanism, and statically by explicitly creating the objects in the policy database. Tivoli Policy Director for Operating Systems uses the static mode. Every object to be protected, that is, every object that is to have an ACL or POP attached, must be explicitly created. For example, the pdadmin command:

```
padmin> object create /OSSEAL/Servers/File/etc/passwd "Password file" 
3 ispolicyattachable yes
```

creates a Tivoli Policy Director for Operating Systems File resource representing the /etc/passwd file with a description of "Password file", type 3 (meaning file) and indicating that authorization policy might be attached to this object. Refer to Tivoli Policy Director documentation for details about the object create command and other pdadmin commands.

Tivoli Policy Director provides resource managers with the capability to extend, in an application specific way, the information contained in the policy database. Application specific extended attributes are used to extend the meaning of the objects, ACLs, and POPs defined in the policy database. Tivoli Policy Director for Operating Systems defines an extended ACL attribute to implement access control based on the program being used to perform an action. Tivoli Policy Director for Operating Systems also defines extended object attributes to implement the Holidays and Sudo resources. [Login Policy” on page 31 and “Sudo Policy” on page 42] describe these extended attributes. The remainder of this section describes each type of access controls and how Tivoli Policy Director for Operating Systems uses them.

Access Control Lists

An Access Control List (ACL) in the Policy Director environment follows the discretionary access control model. Access to resources is controlled based on the identity of the user and the action that they are performing.

ACLs consist of a list of ACL entries. Each ACL entry has an accessor and a permission set. These components will be denoted by the following notation in the examples below:

```
accessor : permission-set
```

A permission is represented by a single character that represents actions that may be performed on objects to which an ACL is attached. For example the x permission might represent permission to execute a program. The full set of permissions used by Tivoli Policy Director for Operating Systems is described in the Table 5 on page 11. The accessor describes the users that the ACL entry is to apply to. The types of accessors are:

**user**

This accessor type defines an ACL entry that controls access to a resource for a particular user. The user’s name is also specified in an accessor of this type. This user name must identify an existing Policy Director user. The following ACL entry grants the x permission to the root user.

```
user root : x
```

This kind of ACL entry has the highest precedence. If user root were a member of a group that was denied the x permission, this ACL entry would override that. Conversely, if user root were a member of a group that granted y permission, this...
ACL entry would have precedence and deny root y permission on resources protected by this ACL. The username component of a user accessor in an ACL entry must be unique so that each user has only one user entry in an ACL.

**group**  
This accessor type defines an ACL entry that controls access to a resource based on group membership. The group’s name is also specified in an accessor of this type. This group name must identify an existing Tivoli Policy Director group. The following ACL entry grants the y permission to the users group:

```
group users : y
```

Users are granted permissions based on group membership by taking the union of all the permissions in group ACL entries for groups in which they are a member. For example, if the user kevin is a member of the groups users and sys-admin, but not net-admin, then the following ACL entries grant kevin a and b permission but not c:

```
group users : a
group sys-admin : b
```

The group name component of a group accessor in an ACL entry must be unique so that each group has only one group entry in an ACL.

**any-other**  
The any-other ACL entry grants permissions to any authenticated user that is not explicitly listed in a user entry within the ACL and is not a member of any groups listed in group entries within the ACL. An entry of this type allows definition of default permissions for authenticated users. The following entry grants q permission to any authenticated user not covered by a user or group entry in the ACL:

```
any-other : q
```

Only one any-other ACL entry may appear in an ACL.

**unauthenticated**  
The unauthenticated ACL entry grants permissions to unauthenticated users. [The UNIX Identity and Its Relationship to the Tivoli Policy Director User Identity” on page 3](#) explains the meaning of unauthenticated users in Tivoli Policy Director for Operating Systems. Unauthenticated users, by definition, have no Tivoli Policy Director user name nor can they be members of Tivoli Policy Director groups. The following entry grants p permission to unauthenticated users:

```
unauthenticated : p
```

Only one unauthenticated ACL entry may appear in an ACL. Unauthenticated users cannot be granted permissions that authenticated users do not have. This means that any permissions granted by an unauthenticated ACL entry that are not granted by the any-other ACL entry are ignored. In the above example unauthenticated users would only be granted p permission if the ACL also has an any-other entry that grants the p permission.

Permissions describe actions that can be performed on resources protected by Tivoli Policy Director. The set of permissions specified in an ACL entry is the full set of permissions granted to users that match the accessor of that ACL entry. A user trying to perform an action not present in the permission set will be denied access to any resources the ACL is protecting.

Permissions are defined by Tivoli Policy Director actions. An action defines a single letter mnemonic representing the permission, the name of the permission, the kind of the resource it applies to and the action group of which it is a part. An action group is a collection of
related actions. All Tivoli Policy Director for Operating Systems actions are defined as members of the OSSEAL action group. Actions in the OSSEAL action group represent operations that may be performed on the resources that Tivoli Policy Director for Operating Systems protects. Table 5 defines all of the actions used by Tivoli Policy Director for Operating Systems. Each permission is defined when it appears in this book.

**Table 5. Permissions Defined in the OSSEAL Action Group**

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>Resource Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>Connect</td>
<td>NetIncoming and NetOutgoing</td>
</tr>
<tr>
<td>D</td>
<td>Change directory</td>
<td>File</td>
</tr>
<tr>
<td>G</td>
<td>Surrogate</td>
<td>Surrogate</td>
</tr>
<tr>
<td>K</td>
<td>Kill program</td>
<td>File</td>
</tr>
<tr>
<td>L</td>
<td>Login</td>
<td>Login</td>
</tr>
<tr>
<td>N</td>
<td>Create</td>
<td>File</td>
</tr>
<tr>
<td>R</td>
<td>Rename</td>
<td>File</td>
</tr>
<tr>
<td>U</td>
<td>Update timestamp</td>
<td>File</td>
</tr>
<tr>
<td>d</td>
<td>Delete</td>
<td>File</td>
</tr>
<tr>
<td>l</td>
<td>List directory</td>
<td>File</td>
</tr>
<tr>
<td>o</td>
<td>Change ownership</td>
<td>File</td>
</tr>
<tr>
<td>p</td>
<td>Change permission</td>
<td>File</td>
</tr>
<tr>
<td>r</td>
<td>Read</td>
<td>File</td>
</tr>
<tr>
<td>w</td>
<td>Write</td>
<td>File</td>
</tr>
<tr>
<td>x</td>
<td>Execute</td>
<td>File and Sudo</td>
</tr>
</tbody>
</table>

Tivoli Policy Director defines actions that control access to policy management functions. Tivoli Policy Director for Operating Systems uses these actions to control who can modify the policy. These actions are all members of the primary action group. Policy management uses the primary actions in Table 6.

**Table 6. Tivoli Policy Director Primary Actions Used for Policy Management**

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>Attach an ACL or POP</td>
</tr>
<tr>
<td>b</td>
<td>Browse object space and see object names</td>
</tr>
<tr>
<td>c</td>
<td>Control or modify an ACL</td>
</tr>
<tr>
<td>d</td>
<td>Delete an object</td>
</tr>
<tr>
<td>m</td>
<td>Modify an object’s attributes</td>
</tr>
<tr>
<td>v</td>
<td>View the attributes of an object</td>
</tr>
</tbody>
</table>

The full meaning of these permissions is explained in the Policy Director documentation. Table 7 lists the two other primary Policy Director actions that affect the way authorization decisions are made.

**Table 7. Policy Director Primary Actions Used for Policy Decisions**

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>Bypass time-of-day restriction</td>
</tr>
<tr>
<td>T</td>
<td>Traverse</td>
</tr>
</tbody>
</table>
If a user has the **B** permission, then any time-of-day restriction applicable is not applied to that user. Policy administrators need this permission in order to administer policy on objects subject to time-of-day access restrictions. See "Protected Object Policies" on page 13 for an explanation of time-of-day restrictions.

The **T**, or Traverse, permission lets you control access to whole branches of resources efficiently. See "Inheritance and Traversal" for details.

When included in a permission set, all actions are prefixed by their action group name. For actions in the primary action group this is optional. An ACL entry for Tivoli Policy Director for Operating Systems typically looks like:

```
user root: T[OSSEAL]rwx
```

This indicates that the user root has the Tivoli Policy Director for Operating Systems read, write, and execute permissions plus the Traverse permission. Other resource managers may define actions with mnemonic names similar to those used by Tivoli Policy Director for Operating Systems. For example the Policy Director WebSEAL uses 'r' to grant permission to read a web page protected by WebSEAL. These permissions, despite having the same mnemonic, are entirely separate and should not be confused. An ACL entry with the permission set Br[OSSEAL]wx does not grant Tivoli Policy Director for Operating Systems users read access to files that this entry’s ACL may be protecting.

### Inheritance and Traversal

In the Tivoli Policy Director environment resources can inherit ACLs from other resources. Examining the protections of file resources is an example of inheritance. For example, if you have a directory named project01 on your system, the protected object name of this directory might be /OSSEAL/default/File/project01. By placing an ACL on the protected object name for the /project01 directory which contains all of the files for a project, all the sub-directories and files in this directory inherit that ACL from project01.

Inheritance lets you easily apply policy to a number of resources by placing ACL high up in the protected object name hierarchy.

Inheritance applies to all resources. If a resource does not have an ACL attached to it, Tivoli Policy Director for Operating Systems moves up the protected object name until it finds an ACL. For example,

1. Assume a user is trying to access a network resource with a protected object name of /OSSEAL/default/NetIncoming/tcp/telnet/www.company.com.

2. If that protected object name does not have an ACL assigned to it, Tivoli Policy Director for Operating Systems looks to see if /OSSEAL/default/NetIncoming/tcp/telnet has an ACL assigned to it.

3. If this next level up does not have an ACL attached to it, Tivoli Policy Director for Operating Systems looks to see if /OSSEAL/default/NetIncoming/tcp has an ACL assigned to it.

4. Tivoli Policy Director for Operating Systems continues up the hierarchy like this until it finds an ACL it can use to make a policy decision.

There is one exception to this rule. Tivoli Policy Director for Operating Systems, when protecting file system resources, always assumes that a permissive ACL, that is an ACL that will grant all accesses, is attached to the root of the file system. This ensures that a system remains functional when Tivoli Policy Director for Operating Systems is protecting it and
also ensures that Tivoli Policy Director for Operating Systems can make efficient authorization decisions when file system resources are accessed.

When making a policy decision, Tivoli Policy Director for Operating Systems uses the ACL lowest in the hierarchy. This lower-level ACL completely overrides any higher level ACL. For example, assume the following:

1. Assume you have a file resource with a protected object name of /OSSEAL/servers/File/usr/games/solitaire. The solitaire game is a file, and usr and games are directories.
2. You have one ACL on the directory usr that gives everyone full access and another ACL on solitaire that gives only the administrator full access.
3. By inheritance, the games directory under usr is accessible to everyone, but solitaire is accessible only by the administrator, no matter what ACL entries are present in the ACL at the usr directory.

The only exception to the rule that an ACL lower in the hierarchy entirely overrides a higher one is the behavior of the primary Tivoli Policy Director Traverse permission ("T"). In order for a user to access a resource, that user must be granted Traverse permission in every ACL higher in the hierarchy than the object being accessed. Traverse permission is not required to access the object itself. In the above example the administrator needs Traverse permission in the ACL attached at usr but not in the ACL attached at solitaire. If an ACL were placed at games, then the administrator would also require Traverse permission be granted by that ACL.

Protected Object Policies

Tivoli Policy Director provides a form of access control called a Protected Object Policy (POP). POps define access controls that are not based on user identity or the action the user is performing and also to control other details about how an authorization decision is made. POps, like ACLs, are defined by the administrator and are attached to objects in the Tivoli Policy Director database that represent the resources being protected. POps obey the same inheritance rules as ACLs.

POPS and ACLs are inherited independently, you do not need to attach them at the same point in the object hierarchy. Any given object might inherit access controls from an ACL attached at one point in the hierarchy and from a POP at another. In the solitaire example above assume a POP restricting time-of-day access at the games directory is defined. Access is controlled to solitaire by the ACL attached directly to it and, by inheritance, the POP attached above it at games.

You can define various attributes within a POP. Tivoli Policy Director for Operating Systems uses the warning mode, audit level, and time-of-day attributes. It does not use the quality of protection or IP endpoint authentication attributes.

POP Attributes Used for Access Control

POPs provide several attributes you can use to implement specific policies.

The Warning Mode Attribute

This access control lets you implement trial policy. A protected object protected by a POP with warning set to yes has warning mode enabled. When an ACL denies access to an object with warning mode enabled, instead of the access being denied, it is granted and an audit record is generated. You can try policy by applying ACLs where you believe they should go and then examining the audit trail to verify that accesses that should be denied are
denied and accesses that should be granted are granted. Audit records are generated regardless of the audit level setting in the POP. See "Enabling, Disabling, and Querying Resource Warning Mode" on page 78 for examples of the warning mode attribute.

By default warning mode is disabled.

The Audit Level Attribute
The audit level access control specifies under what circumstances an access to an object generates an audit record. The audit level is set to one or more of the following levels:

- **permit**
  If enabled, an audit event is generated when access to the resource is granted

- **deny**
  If enabled, an audit event is generated when access to the resources is denied

- **admin**
  Does not apply to Tivoli Policy Director for Operating Systems resources

- **error**
  Does not apply to Tivoli Policy Director for Operating Systems resources

- **all**
  All of the defined audit levels are enabled

- **none**
  None of the defined audit levels are enabled. This is the default.

See "Setting and Querying the Resource Audit Level" on page 79 for examples of setting the resource audit level. Further details about the audit levels are in the Tivoli Policy Director documentation.

The Time-of-day Attribute
The time of day access control specifies times of the days of the week and the times of the day that a resource can be accessed. The time of day access control specification is of the form:

```
day-range : time-range [ : utc | local ]
```

where

- **day-range**
  Either anyday, weekday, or a comma-separated list of sun, mon, tue, wed, thu, fri, or sat. The anyday option indicates that the user is permitted access on any day of the week. The weekday option specifies that the user is permitted access on any day except for Saturday and Sunday. A list of days indicates that the user is permitted to access the resource only on the specified days.

- **time-range**
  Either anytime or a start time and end time. The anytime option indicates that the user is permitted to access the resource at any time on the days of the specified by the day-range. If time is specified in the form start_hhmm-end_hhmm, the start_hhmm specifies an hour followed by minutes past the hour, and the end_hhmm specifies the end time. Specify the hour in 24-hour format.

- **utc**
  Specifies that the time-of-day restriction should be applied according to Universal Coordinated Time (UTC).

- **local**
  Specifies that the time-of-day restriction should be applied according to the local time on the machine the user is logging in on. This is the default.

By default, access is permitted on all days at all times.
Access Restrictions

Tivoli Policy Director for Operating Systems defines an extended attribute on an ACL that lets you control what programs users can use to perform particular actions. This restriction is in addition to the access control enforced by the ACL. Before an access restriction is applied the user must first have been granted access by the ACL entries. The name of the attribute is Access-Restrictions and its format is:

accessor : permission-set : program-set

The accessor is an accessor defined in the same way as the accessor component of an ACL entry. The permission set is also defined in the same as in an ACL entry except that, because this extended attribute applies only to Tivoli Policy Director for Operating Systems actions, you can omit the [OSSEAL] action group qualifier.

The program set is a space-separated list of programs that the accessor is allowed to use to perform the actions specified in the permission set to resources protected by the ACL extended with the access restriction. Programs listed in a program set are trusted to access the resource protected by the ACL. These programs are therefore included in the Trusted Computing Base. See “Trusted Computing Base Resources” on page 23 for information about the Trusted Computing Base.

The special program set * means that any program may be used to perform the action.

Example of Access Restrictions

For example, to allow any user to access the /etc/passwd file but to restrict non-administrators to using the /usr/bin/passwd command to write to the file, the ACL defined by the following pdadmin commands could be used:

```
padmin> acl create passwd
padmin> acl modify passwd set any-other [OSSEAL]rw
padmin> acl modify passwd set unauthenticated [OSSEAL]rw
padmin> acl modify passwd set attribute \
        Access-Restrictions "group sys-admin:w:*"
padmin> acl modify passwd set attribute \
        Access-Restrictions "any-other:w:/usr/bin/passwd"
```

Access restrictions can be applied to any of the following resources: File, NetIncoming, NetOutgoing, Login, or Surrogate. It is meaningless to define an Access-Restriction for Sudo resources because the accessing program is always the pdossudo command. See “Sudo Policy” on page 42 for a description of Sudo policy and the pdossudo command.

Access Restriction Evaluation

When a resource protected by an ACL with Access-Restrictions is accessed the following rules are used to determine which access restriction value applies:

1. Find all of the values whose permission set contains all of the permissions being requested. For example if read and write access is requested then only entries with both the r and w permissions (and possibly others) are considered.

2. If the user is unauthenticated and there is no unauthenticated accessor entry, grant access.

3. If the user is unauthenticated and there is an unauthenticated accessor entry (there may be more than one) listing the user’s program in the program set, then grant access, otherwise deny access.
4. If the user is authenticated, look for entries with a user accessor matching the user requesting access. If any one of these includes the user’s program in its program set, grant access, otherwise deny access.

5. If no matching user accessor was found, look for group accessor entries for all of the groups in which the user requesting access has membership. If any of these entries includes the user’s program in its program set, grant access, otherwise deny access.

6. If no matching user or group accessor entries were found and there are any-other accessor entries and none of them list the user’s program then deny access.

7. Otherwise access is granted (because there are no any-other accessor entries, or there are, and one of them lists the user’s program in its program set).

Example of Access Restriction Evaluation

Assume the following Access-Restrictions attribute values:

- user root:rw:/usr/bin/vi
- group sys-admin:r:/usr/bin/more
- group net-admin:r:/usr/bin/cat

In this case the user root is allowed to use /usr/bin/vi only when reading, writing or both. The root user can not use either the /usr/bin/more or the /usr/bin/cat program to read the file because the root user always matches the first entry, and the group membership will not be taken in to account.

Members of the sys-admin group can use the /usr/bin/more command only to read files.

Members of the net-admin group must use /usr/bin/cat to read files.

Users who are members of both groups (except the root user) can use either /usr/bin/more or /usr/bin/cat to read.

Because the Access-Restrictions attribute values do not further restrict write access for the members of the groups sys-admin and net-admin (except the root user), write access for members of these groups is controlled only by the ACL entries in the ACL to which this Access-Restriction has been applied. To ensure that users who are members of these groups cannot write to the files, the ACL entries should deny write access. If the ACL entries grant write access, then users who are members of these groups (except for root) can use any program to write to the files.

When you define access restrictions you should group actions. In the above example, assume the restriction: user root:rw:/usr/bin/vi had been split into two restrictions:

- user root:r:/usr/bin/vi
- user root:w:/usr/bin/vi

If root opened a file protected by these restrictions for both read and write, then no access restriction would apply because no restriction contains all of the requested permissions.

Protected System Resources

This section describes protected system resources as they are defined in the Tivoli Policy Director for Operating Systems environment. It specifies what resources can be protected, how the resources are defined in the policy namespace, and what actions can be defined for a resource. It also describes how resources are defined in the Trusted Computing Base (TCB) and how TCB resources are treated.
File Policy

Tivoli Policy Director for Operating Systems provides the ability to control access to file system resources. File systems resources consist of:

- Files
- Directories
- Soft links
- Hard links
- Device files

This section describes how access each of these resources are affected when the authorization policy is applied to them. File system resources are protected in two ways:

- Access controls protect file system resources based on the identity of the user attempting the access and the action they are trying to perform. They are applied to resources of type File.
- Membership in the TCB protects file system resources by monitoring the members’ contents and attributes for change. The membership of the TCB is defined by resources of type TCB.

These two mechanisms for protecting are described in the following sections.

File Resources

File system resources are represented in the Tivoli Policy Director namespace by defining an object name with resource type File and specifying the name of the file system resource to be protected:

```
/OSSEAL/policy-branch/File/filespec
```

Table 8 details the file system objects.

<table>
<thead>
<tr>
<th>Object Name</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>filespec</td>
<td>An object name that represents a file system resource. The string specifies the full path name of the file resource being protected. The path name can contain wildcards.</td>
<td>String conforming to the UNIX file naming rules.</td>
</tr>
</tbody>
</table>

Example File System Resources

Some example file system resource specifications are:

```
/OSSEAL/Default/Files/etc/passwd
/OSSEAL/Default/Files/usr/local/*/.*.log
/OSSEAL/Default/Files/usr/sbin/httpd
```

The following restrictions apply when naming File resources:

- Access controls cannot be attached to the root directory, `/`. Tivoli Policy Director for Operating Systems always assumes that permissive access controls are attached at `/OSSEAL/policy-branch/File`.
- The first element of a file specification can not contain wildcard elements (for example, `/*.`.log or `/*/tmp`). Specific resources in the root directory can have access controls.

These restrictions ensure that authorization decisions can be made efficiently.
Access Control on File Resources

The Tivoli Policy Director for Operating Systems actions that apply to File resources are defined in Table 9.

Tivoli Policy Director ACLs can be placed at any point in a file system resource representation in the namespace. Normal Tivoli Policy Director ACL inheritance rules apply to file system resources. This includes namespace traversal (T) permissions.

The single exception to the normal ACL inheritance model is the root of the file system namespace, for example, /OSSEAL/policy-branch/File. Tivoli Policy Director for Operating Systems assumes that there is always an ACL at that point that permits access (and traversal) to everyone. Thus, for the purposes of ACL inheritance, the effective root of the namespace is at this position. In other words, an explicit ACL attached to the File object or higher is ignored for both access to the file system root directory (/) and for the purposes of inheritance.

Table 9 details the valid ACL permissions that can be associated with file system resources.

### Table 9. File Permissions

<table>
<thead>
<tr>
<th>Permission Name</th>
<th>Permission granted</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read (r)</td>
<td>Access a file system resource for reading.</td>
</tr>
<tr>
<td>Write (w)</td>
<td>Access a file system resource for writing.</td>
</tr>
<tr>
<td>Create (N)</td>
<td>Create a particular file system resource.</td>
</tr>
<tr>
<td>Execute (x)</td>
<td>Execute a file system resource.</td>
</tr>
<tr>
<td>Chown (o)</td>
<td>Change the ownership of a file system resource.</td>
</tr>
<tr>
<td>Chmod (p)</td>
<td>Change the native UNIX file system permissions associated with a file system resource. This applies to both operations that modify UNIX mode bits and to operations that alter a resource’s native ACL for applicable platforms.</td>
</tr>
<tr>
<td>Chdir (D)</td>
<td>Change directory into a file system directory resource (directories only).</td>
</tr>
<tr>
<td>Rename (R)</td>
<td>Move (or rename) a file system resource.</td>
</tr>
<tr>
<td>Delete (d)</td>
<td>Remove a file system resource.</td>
</tr>
<tr>
<td>Utime (U)</td>
<td>Modify the file access and modification times associated with a file system resource.</td>
</tr>
<tr>
<td>Kill (K)</td>
<td>Terminate a process that was executed from a file system resource.</td>
</tr>
<tr>
<td>List (l)</td>
<td>List the contents of a directory.</td>
</tr>
</tbody>
</table>

Many of the permissions have special behaviors or, where an equivalent UNIX permission exists, slightly different behavior. These behaviors are as follows:

- The Kill (K) permission can be applied to the special File resource /OSSEAL/policy-branch/unix to control the ability to shutdown or reboot the system.

- The Rename (R) permission interacts with the Create and Delete permissions. When renaming a file, in addition to Rename permission on the source file, the user must have Create permission on the target. If the target exists the user must additionally have permission to delete it. For example, if a directory has the contents:

  log.1  log.bak

  then a user issuing the command:

  `$ mv log.1 log.2`
in the directory must have Rename permission on the file log.1 and Create permission on log.2. If the command
$ mv log.1 log.bak
were issued, the user would need both Create and Delete permission on the file log.bak.

- The Change permission (p) permission also controls the ability to modify UNIX ACLs in addition to file permission. This applies only on systems that support this facility.
- The Execute (x) permission applies only to files. The UNIX 'x' file permission also controls the ability to navigate a directory hierarchy. The Tivoli Policy Director for Operating Systems Change directory permission (D) and primary Traverse (T) permission can be used together to control a user’s ability to navigate file systems directories.

File System Aliases

The file system provides the capability to define alias names for a resource. When a resource is accessed by an alias name, Tivoli Policy Director for Operating Systems makes sure that the underlying resource is still protected. The file system aliases are:

- Symbolic links
- Hard links
- Device files

The following sections describe how Tivoli Policy Director for Operating Systems enforces authorization policy when protected resources are accessed through the different kinds of alias names and when authorization policy is associated with an alias rather than the real resource.

The major principles that define the way Tivoli Policy Director for Operating Systems handles access controls in conjunction with alias names are:

- Access controls applied to an alias should protect the real resource in addition to the alias.
- Creation of a new alias should not allow access controls that already apply to the real resource to be bypassed.

Keep these two principals in mind when reading the following sections.

Symbolic Links

First, consider how symbolic links affect the way policy is evaluated when access controls are not inherited. There are three possibilities:

- The target has access control directly applied to it. In this case, where the target of the symbolic link has an access control applied but the symbolic link does not, accesses to the resource by either name are controlled by the policy attached to the target. A symbolic link can not be used to side step authorization policy.
- The symbolic link has access control applied to it. In this case, where the symbolic link has access control applied but the target does not, accesses to the resource by either name are also controlled by the same policy; that attached to the symbolic link.
- Both the target and the symbolic link have access controls applied. In the case where access controls are applied to both the symbolic link and its target, accesses to the target directly are controlled only by the access control that is directly applied. Accesses via
the symbolic link are controlled by both sets of access controls and access is granted to
the resource only if the accessor is permitted by both sets of access controls.

Examples of Symbolic Link Aliases
The following are examples of the affect of policy on symbolic links.

Example 1
Assume you have this real file with an ACL attached to it:
/usr/bin/vi
The file
/usr/local/bin/vi
is a symbolic link to
/usr/bin/vi
Then, when a user attempts to execute vi by either name an authorization decision is made
using the ACL attached to /usr/bin/vi If, instead, the ACL was attached to
/usr/local/bin/vi, then it would still protect vi no matter which of the names was used to
access it. The protected object would be /usr/local/bin/vi.
If an ACL were attached to both /usr/bin/vi and /usr/local/bin/vi then accesses via
the name /usr/bin/vi are protected by the ACL attached to /usr/bin/vi. Accesses via the
name /usr/local/bin/vi are protected by both ACLs.

Example 2
Suppose
/home/joe/data
is a file with no access controls applied.
/home/joe/data.link
is a symbolic link to data with an ACL attached.
/tmp/data/joe_data
is a symbolic link to
/home/joe/data
also with an ACL attached.

The following conditions affect the access to this resource.

- If the file is accessed directly via the name /home/joe/data both ACLs must be passed
  before access is granted.
- If the file is accessed via either of the symbolic links then both ACLs will also apply.
- If an ACL were to be attached directly to /home/joe/data then when the file is
  accessed directly as /home/joe/data only this ACL would apply.
- If the access were by either of the symbolic links, then this ACL, plus the ACL on the
two symbolic links, would apply.
- If the symbolic link is to a directory name rather than a file name. The same rules
  described above for files apply in this case as well with the resulting policy being
  inherited by the contents of the target directory.

Example 3
The next case to consider is when either the target resource or the symbolic link is protected
by inherited access controls rather than having access controls applied directly. When a
symbolic link has no access control directly applied to it, the target of the symbolic link is protected only by access controls that the symbolic link inherits when the target is accessed via the symbolic link. When the target of a symbolic link has no access control directly applied to it, access controls inherited by the target are always applied whether the target is accessed directly or via the symbolic link. Consider the following examples:

Suppose

/home/joe/data

is a file with ACL attached directly to it.

/tmp/data/joe_data

is a symbolic link to /home/joe/data also with an ACL attached at /tmp/data.

- When the file is accessed directly, only the ACL attached directly is applied.
- When the file is accessed via the name /tmp/data/joe_data both ACLs are applied.

**Example 4**

Suppose: /home/joe/data is a file this time with an ACL attached only at /home.

/tmp/data/joe_data is a symbolic link to /home/joe/data this time with an ACL attached directly to /tmp/data/joe_data.

In this case, both ACLs are applied when the file is accessed by either name.

Having access controls propagate through symbolic links allows platform independent policy to be established more easily, particularly in cases where file layouts differ only by which name for a resource is the real file and which is the symbolic link. Even so, care must be taken to understand the effects of applying Tivoli Policy Director for Operating Systems authorization to a system in order to ensure that the enforcement of the policy you define is as you intend.

When a symbolic link is created or deleted the only access controls that apply are those that apply directly to the symbolic link or that the symbolic link inherits.

### Hard Links

You can define hard links to create multiple directory entries for a file. Each of these directory entries must reside in the same file system. Accesses to files system resources that have multiple hard links are controlled similarly to resources with symbolic links. However, once created, there is no one hard link that can be considered the target or real resource. The following rules summarize the behavior:

- When accessing a hard link that has access controls directly applied, only those access controls are applied.
- When accessing a resource that does not have any access control applied but has other hard links that do have access controls directly applied, all of the other access controls must be passed to gain access to the resource.
- Only if no hard links of the resource have access controls directly applied will access controls inherited by the accessed resource be applied.

**Examples of Hard Link Aliases**

The following are examples of the effect of policy on hard links.
Example 1
Assume /home/joe/data is a file with an ACL attached directly to it.
/home/data/joe_data is a hard link to /home/joe/data with no ACL attached to /home/data

Accesses to /home/joe/data are subject only to the ACL attached directly to /home/joe/data.

Accesses to /home/data/joe_data are also subject only to the ACL attached directly to /home/joe/data.

Example 2
Assume /home/joe/data is a file with no ACL attached to it.

/home/data/joe_data.1 and /home/data/joe_data.2 are both hard links to /home/joe/data each with their own ACL attached.

Accesses to /home/joe/data are subject to both ACLs.

Accesses to either /home/data/joe_data.1 or /home/data/joe_data.2 are each subject only to the ACL directly applied to them.

Because different hard links to a file can have different UNIX file permissions, Tivoli Policy Director for Operating Systems controls the creation of a new hard link in a special way. When creating a new hard link the user needs the following permissions:

N Create permission on the name of the new hard link.
R Rename permission on the target of the new hard link.
r Read permission on the target of the new hard link.
w Write permission on the target of the new hard link.

When a hard link is deleted only those access controls that apply to that hard link are enforced.

Device Files
Device files represent an underlying resource of the system, for example a printer or a disk device. You can create a device file that represents the same device as an existing device file. The creation of new alias files should not be used to bypass access controls applied to a device. The same rules that apply to hard links apply to device files.

- When accessing a device file that has access controls directly applied, only those access controls are applied.
- When accessing a device file that does not have any access control applied and there are other device files representing the same device that do have access controls directly applied, all of the other access controls must be passed to gain access to the resource.
- Only if none of the device files representing the device have access controls directly applied will access controls inherited by the accessed resource be applied.

Files Accessed From NFS Clients
Tivoli Policy Director for Operating Systems policy can be placed on file system resources that are accessed by NFS clients. The access controls are defined based on the path that the NFS client would use to access the file.

For instance, let’s say that there is a directory on an NFS server called /usr/shared/hrtools/bin that is available to NFS clients through a mount point of
Access controls can be applied to the file resource 
/usr/tools/bin/payroll to restrict access to the payroll executable file by the NFS clients. This policy would be applied to any file with an identical access path on any Tivoli Policy Director for Operating Systems system, whether it is an NFS mount point or not. However, these access controls would not apply to the direct access of the file on the NFS server itself. Similarly, access controls on the NFS server path of 
/usr/shared/hrtools/bin/payroll would have no effect on the NFS clients accessing the file through the NFS mount mount.

Because NFS is a stateless file access protocol, operations performed from one NFS client might not be immediately visible at other NFS clients accessing the same file system resources. As a result, Tivoli Policy Director for Operating Systems policy might not be immediately enforced on an NFS client when the file is created, deleted, or renamed by another NFS client or on the NFS server itself. For this reason, it is recommended that access controls on file resources accessed through NFS client-mounted paths be placed only on files that already exist and that are infrequently deleted or renamed. Directories and read-only files, such as executable files, are good candidates for such access controls.

**Trusted Computing Base Resources**

Tivoli Policy Director for Operating Systems provides the ability to define files on a system as being part of a trusted computing base. Files that are members of the trusted computing base are monitored for changes in ownership, UNIX file permissions, creation and modification timestamps, presence or absence on a system, content of the file, and the device on which the file resides. These attributes are collectively referred to as the file’s signature.

Tivoli Policy Director for Operating Systems lets you grant special privileges to programs by defining them in the Trusted Computing Base (TCB). If the integrity of a program defined in the TCB is compromised, it should no longer be trusted with special privileges. Tivoli Policy Director for Operating Systems detects changes that comprise the integrity of a registered program. When a change is detected, Tivoli Policy Director for Operating Systems records that the program is untrusted and does not allow an untrusted program to be executed until an administrator explicitly requests it by using the `pdosobjsig` command.

Special privileges are granted to programs by defining them in one of the following classes of TCB resources:

- Secure-Files
- Secure-Programs
- Login-Programs
- Impersonator-Programs
- Immune-Programs

A file might be classified as more than one type of TCB resource. The special privileges conveyed by these categories are detailed below.

Files are created in the TCB by explicitly creating a Tivoli Policy Director policy object of the appropriate name. Tivoli Policy Director for Operating Systems enforces no authorization policy based on access controls applied on or beneath the `/OSSEAL/policy-branch/TCB` resource tree. Access controls are applied to files that are members of the TCB by attaching access controls to objects in the File resource tree. For example, to add the file `/etc/hosts.equiv` as a Secure-File while permitting access only to root, use the following `pdadmin` commands:
1. Add `hosts.equiv` to the TCB:

   ```
padmin> object create /OSSEAL/Workstations/TCB/Secure-Files/etc/hosts.equiv "Host equivalents" 0 ispolicyattachable yes
   ```

2. Allow only root to access `hosts.equiv`

   ```
padmin> acl create hosts-equiv
padmin> acl modify hosts-equiv set user root T(OSSEAL)NRUdoprw
padmin> object create /OSSEAL/Workstations/File/etc/hosts.equiv "hosts equiv file" 3 ispolicyattachable yes
padmin> acl attach /OSSEAL/Workstations/File/etc/hosts.equiv hosts-equiv
   ```

Programs listed in any ACL’s Access-Restrictions attribute are trusted to access the resource protected by the ACL. These programs are therefore included in the TCB whether or not they are explicitly defined as TCB resources.

All files in the TCB, regardless of the class they are specified in, are monitored for change. When a change is detected, the file becomes untrusted. The trust state of a file is recorded on a per-system basis. Access to untrusted files, in addition to any access controls applied to the file as a File resource, is further controlled as follows:

- When a file is initially added to the TCB by issuing the appropriate `object create` command in `padmin`, it is marked as trusted and its initial signature is recorded.
- An administrative audit event is generated when the file’s signature is detected to have changed.
- An untrusted file cannot be executed, regardless of any access controls.
- Other accesses permitted by access controls, to an untrusted file (such as read), generate an administrative audit event.
- If a file is recorded as a TCB file but does not exist on a system, that file is immediately untrusted on that system if it is created.
- If a file is recorded as a TCB file and is deleted, that file is marked untrusted and remains untrusted if recreated.
- A file, once untrusted, can become trusted again only by an explicit action from the administrator. Use the `pdosobjsig` command to retrust a file. See “pdosobjsig” on page 170.

The different types of TCB resources are defined as follows:

**Login-Programs**

UNIX systems have no specific action that can be classified as a login. Tivoli Policy Director for Operating Systems detects a user’s login from the execution of various Surrogate operations by specific programs. The specific programs are defined by their membership in the Login-Programs class of TCB files. Only certain programs have been certified to work as Login-Programs in the Tivoli Policy Director for Operating Systems environment. These are the programs that are involved in UNIX logins from locally attached terminals, graphical desktop environments, and common network protocols (FTP, RLOGIN, TELNET, REXEC, RSH).

Other programs might work and can be added to the Login-Programs class, but only the programs, as distributed by the operating system vendor, listed in Table 10 on page 25 have been certified to perform logins in a manner that can be detected by Tivoli Policy Director for Operating Systems. None of the programs defined as Login-Programs by default should be removed from the set unless the corresponding files are removed from the systems being protected by Tivoli Policy Director for Operating Systems. Doing so can compromise system security.
Table 10. Login Programs Certified for Tivoli Policy Director for Operating Systems

<table>
<thead>
<tr>
<th>Platform</th>
<th>Login Programs</th>
</tr>
</thead>
</table>
| AIX      | /usr/dt/bin/dtlogin  
           | /usr/sbin/ftpd     
           | /usr/sbin/getty    
           | /usr/sbin/login    
           | /usr/sbin/rexecd   
           | /usr/sbin/rlogind  
           | /usr/sbin/rshd     
           | /usr/sbin/telnetd  
           | /usr/sbin/tsm      |
| HP-UX    | /usr/bin/login     
           | /usr/bin/tsm       
           | /usr/dt/bin/dtlogin 
           | /usr/lbin/ftpd     
           | /usr/lbin/remshd   
           | /usr/lbin/rexecd   
           | /usr/lbin/rlogind  
           | /usr/lbin/telnetd  
           | /usr/sbin/getty    
           | /usr/sbin/tsm      |
| Solaris  | /usr/bin/login     
           | /usr/dt/bin/dtlogin 
           | /usr/lib/saf/ttymon 
           | /usr/sbin/in.ftpd  
           | /usr/sbin/in.rexecd 
           | /usr/sbin/in.rlogind 
           | /usr/sbin/in.rshd  
           | /usr/sbin/in.telnetd 
| Linux    | /bin/login         
           | /sbin/getty        
           | /sbin/mingetty     
           | /usr/bin/gdm       
           | /usr/bin/gdmlogin  
           | /usr/bin/kdm       
           | /usr/sbin/in.ftpd  
           | /usr/sbin/in.rexecd 
           | /usr/sbin/in.rlogind 
           | /usr/sbin/in.rshd  
           | /usr/sbin/in.telnetd 
           | /usr/sbin/in.tftp   
           | /usr/sbin/wu.ftpd  
           | /usr/sbin/wu.ftpd  
           | /usr/X11R6/bin/xdm |

Secure-Files
Secure files are granted no special privileges. They are simply monitored for changes in their signature. Tivoli Policy Director for Operating Systems defines some Tivoli Policy Director for Operating Systems files as Secure-Files when initially configured. No system files are pre-defined as Secure-Files.

Secure-Programs
Many UNIX programs require UNIX privileges which are different from the UNIX
permissions of the users who can run them. Such programs are marked with the set user ID or set group ID permissions and might include such commands as su, mail, or telnet. Without any special action, the change of UNIX identity that occurs when such programs are executed would require the invoking user to have the Tivoli Policy Director for Operating Systems authority to Surrogate to the target user and group indicated by the ownership attributes of the program. On systems where the mail program is set UID root, every user should probably be able to run the mail program. However, every user should likely not be authorized to Surrogate to root. See “Surrogate Policy” on page 39 for more information.

Programs defined in the Secure-Programs class of TCB files are treated as exempt from Surrogate policy when the initial UNIX identity changes are performed as the program is executed. If, while the program is executing, it changes UNIX user or group identity again, this subsequent change is subject to Surrogate policy.

The only system program defined as a Secure-Program by Tivoli Policy Director for Operating Systems when initially configured is the su program. If you want to establish restrictive Surrogate policy you need to determine which set UID and set GID files you need to add to the Secure-Programs class of TCB files to allow them to continue to be used by ordinary users who would otherwise be restricted from performing the required Surrogate operation. The pdosuidprog command described in “pdosuidprog” on page 187 locates set UID and set GID programs on your system.

The following Tivoli Policy Director for Operating Systems programs are defined as Secure-Programs:

/opt/pdos/bin/pdosdestroy
/opt/pdos/bin/pdoslpadm
/opt/pdos/bin/pdosrefresh
/opt/pdos/bin/pdossudo
/opt/pdos/bin/pdosunauth
/opt/pdos/bin/pdoswhoami
/opt/pdos/bin/pdoswhois
/opt/pdos/kernel/kosserrs

Impersonator-Programs
UNIX systems generally provide a mechanism (for example, cron) for users to schedule jobs to be executed as batch operations while they are not logged in to the system. Such programs typically run as the root user and, when executing a task, change identity to the user who scheduled the task. That change of identity is viewed as a Surrogate operation and without special action would run with root’s Tivoli Policy Director for Operating Systems credentials and not the user’s credentials because Surrogate operations do not change the Tivoli Policy Director for Operating Systems accessor ID of a process.

A program’s membership in the Impersonator-Programs class of the TCB instructs Tivoli Policy Director for Operating Systems to change the accessor ID of a process running the program when the process changes its effective UNIX user ID. If you have restrictive Surrogate policy you might need, for example with cron, to permit root to Surrogate to otherwise restricted users. Do this by specifying an Access-Restrictions attribute that allows the Surrogate operation only when using the cron.

The only Impersonator-Program defined by Tivoli Policy Director for Operating Systems when initially configured is the cron program.

Immune-Programs
A program might be integrated so tightly to a system that if a process running that
program was subject to authorization policy as enforced by Tivoli Policy Director for Operating Systems, the system would cease to function. You can mark such programs as immune from all Tivoli Policy Director for Operating Systems policy by making them a member of the Immune-Programs class of the TCB. Execution of immune programs is subject to authorization as for any other program but once running the program is immune to all Tivoli Policy Director for Operating Systems authorization policy. This immunity includes auditing; no operations that a running immune program performs are audited.

A process’s immunity is not inherited by any child programs spawned by that process. Tivoli Policy Director for Operating Systems defines the system programs listed in Table 11 as immune in the default policy. They represent system processes involved in file system operations, user identity mapping, and error logging.

Table 11. System Programs Defined as Immune-Programs in Default Policy

<table>
<thead>
<tr>
<th>Platform</th>
<th>Immune Programs</th>
</tr>
</thead>
</table>
| AIX      | /usr/bin/AIXPowerMgtDaemon  
                       /usr/ccs/bin/shlap  
                       /usr/ccs/bin/shlap64  
                       /usr/lib/errdemon  
                       /usr/lpp/diagnostics/diagd  
                       /usr/sbin/automountd  
                       /usr/sbin/biod  
                       /usr/sbin/nfsd  
                       /usr/sbin/rpc.lockd  
                       /usr/sbin/rpc.statd  
                       /usr/sbin/syncd  
                       /usr/sbin/syslogd |
| HP-UX    | /usr/lib/netsvc/fs/autofs/automountd  
                       /usr/lib/netsvc/fs/autofs/automount  
                       /usr/sbin/biod  
                       /usr/sbin/nfsd  
                       /usr/sbin/pwgrd  
                       /usr/sbin/rpc.lockd  
                       /usr/sbin/rpc.statd  
                       /usr/sbin/syslogd  
                       /usr/sbin/syncer |
| Solaris  | /usr/lib/autofs/automountd  
                       /usr/lib/nfs/lockd  
                       /usr/lib/nfs/nfsd  
                       /usr/lib/nfs/statd  
                       /usr/sbin/syslogd |
| Linux    | /sbin/klogd  
                       /sbin/portmap  
                       /sbin/rpc.lockd  
                       /sbin/rpc.statd  
                       /sbin/syslogd  
                       /sbin/apmd  
                       /sbin/automount  
                       /sbin/rpc.nfsd |

In addition to the system programs listed in Table 11, the following Tivoli Policy Director for Operating Systems programs are defined as Immune-Programs on all platforms:
Network Policy

Tivoli Policy Director for Operating Systems provides the ability to control access to remote network services from a local machine and also to control access to local network services from remote locations. These two types of network access are controlled separately by defined protected resources of type NetOutgoing and NetIncoming respectively. These resources are represented in the Policy Director namespace as:

/OSSEAL/policy-branch/NetIncoming/protocol[/service[/host]]
/OSSEAL/policy-branch/NetOutgoing[/hostspec[/protocol[/service]]]

Table 12 details the elements of the network policy object names.

<table>
<thead>
<tr>
<th>Object Name</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol</td>
<td>A representation of a network protocol name. The only supported protocol is TCP over IP version 4. This protocol is represented by the string tcp.</td>
<td>A case-sensitive string representing the protocol.</td>
</tr>
<tr>
<td>service</td>
<td>A description of the set of services represented by this resource. For NetIncoming resources this service represents the service on the local machine to which an incoming connection has been addressed. For NetOutgoing resources this service represents the service on the remote machine to which a connection attempt is being made.</td>
<td>A comma-separated list of ports and port ranges. Ports can be specified explicitly by number or by name. Port names are mapped to port numbers according to the mapping defined in the /etc/services file on the machine where the network policy is being enforced. The special port range ‘<em>’ is equivalent to the range 1-65535. Only one of ‘</em>’ or ’1-65535’ can be present in your policy.</td>
</tr>
</tbody>
</table>
| host        | A description of the set of hosts represented by this resource. For NetIncoming resources, this represents remote hosts from which an incoming connection is attempted. For NetOutgoing resources, this represents the remote host to which an outgoing connection is being attempted. | The host specification may be in one of two forms:  
  - ip-address[/nbits]  
  - hostname |
| ip-address  | A dotted notation of an IP address, for example, 192.168.1.42 | A string representing an IP version 4 address. |
Table 12. Network Resource Naming (continued)

<table>
<thead>
<tr>
<th>Object Name</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>nbits</td>
<td>The number of bits considered significant in an ip-address. Bits are counted from left to right. 0 indicating that no bits are significant and 32 indicating that all bits are significant. When a host is specified in the ip-address[:nbits] form and no nbits component is specified, 32 is assumed.</td>
<td>A number in the range 0 to 32.</td>
</tr>
<tr>
<td>hostname</td>
<td>A wildcard string matching the names of the hosts represented by this resource.</td>
<td>A case-insensitive string consisting of wildcard elements and legal host name characters.</td>
</tr>
</tbody>
</table>

Example Network Resources

Some example network resource specifications are given below:

/OSSEAL/Default/NetIncoming/tcp/80
/OSSEAL/Default/NetIncoming/tcp/telnet/*.dev.company.com
/OSSEAL/Default/NetOutgoing/10.0.151.0:24/tcp/23
/OSSEAL/Default/NetOutgoing/10.1.34.12

For both NetIncoming and NetOutgoing the only permission used in ACLs to control access is the Connect (C) permission.

Table 13. Valid Permission for Incoming or Outgoing Connection to a Network Resource

<table>
<thead>
<tr>
<th>Permission Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connect (C)</td>
<td>Permission to establish an incoming or outgoing connection to a network resource.</td>
</tr>
</tbody>
</table>

Network Service and Host Pattern Precedence

When a network access is attempted Tivoli Policy Director for Operating Systems must determine which protected object name represents that access. The access probably matches more than one of the configured object names. For example, the host name www.good.times.com matches both www.*.com and www.*.times.com. Similarly, the telnet service (port 23) matches the port range "23,513" and the range "*". By matching against the most specific pattern first Tivoli Policy Director for Operating Systems lets you first establish a broad policy and then define exceptions.

The structure of object names is also important when determining their precedence. For each of NetIncoming and NetOutgoing the higher object name components have higher precedence than the lower components. For example, with the two objects:

NetOutgoing/www.good.times.com/tcp/*
NetOutgoing/www.*.com/tcp/http

an outgoing http connection to www.good.times.com is protected by policy attached to the first object because the host component of the object name has the highest precedence.

In the NetIncoming case with the two objects:

NetIncoming/tcp/*/server.cracker.net
NetIncoming/tcp/ftp/*
An incoming ftp request from server.cracker.net to the protected system is authorized based on policy applied to the second object name, not the first.

The precedence rules for determining which service pattern is chosen are the same for both NetIncoming and NetOutgoing. The precedence rules for determining which host pattern is chosen is also the same. [Host Pattern Precedence](#) describes the precise rules.

### Service Pattern Precedence

Service pattern precedence is determined by the following rules:

- Patterns representing a smaller number of distinct ports have higher precedence than those representing more.
- If two service patterns represent the same number of ports then the one with the lowest port number has higher precedence.
- If two service patterns represent exactly the same ports but are not represented identically in the object space then they are considered ambiguous. One of them will be arbitrarily rejected from policy and the PDOSD daemon generates warnings in its error log and administrative audit events warning that ambiguous policy was rejected.

Consider the following examples:

1. The pattern "telnet" has higher precedence than "20-25" because "telnet" represents just one port while "20-25" represents 6.
2. The pattern "20-25" has higher precedence than "21-26" because although both patterns represent 6 ports, 20 is less than 21.
3. The pattern "20-25,50-60" has higher precedence than "20-25,60-70" because although both patterns represent 17 ports, 50 is less than 60.
4. The patterns "1-10,23-30" and "1,2,3,4-9,10,telnet,24-30" are ambiguous because they represent exactly the same set of ports.

### Host Pattern Precedence

Host pattern precedence is determined by the following rules:

- Host patterns of the form `ip-address[:nbits]` patterns always have higher precedence than patterns specified as host names.
- If two `ip-address[:nbits]` patterns with the same `ip-address` component are present with one specifying an `nbits` component of 32 and the other not specifying an `nbits` component at all, the policy is considered ambiguous. One of the objects will be arbitrarily rejected and the PDOSD daemon generates warnings in its error log and administrative audit events indicating that ambiguous policy was rejected.
- `ip-address[:nbits]` patterns with more significant bits (nbits is a larger number) have higher precedence than those with fewer significant bits.
- Host patterns specified as possibly wildcarded host names have precedence according to the wildcard element precedence and are compared from end to beginning. See [Wildcarding](#) on page 6 for information about wildcard pattern precedence.

Consider the following examples:

1. The pattern 10.1.2.3:32 has higher precedence than the pattern 10.1.2.3:24.
2. If www.good.times.com has IP address 10.1.2.3 then the pattern 10.1.2.3:32 has higher precedence than the pattern www.good.times.com. This policy is not considered ambiguous because the `ip-address[:nbits]` pattern always has higher precedence.
3. If www.good.times.com has IP address 10.1.2.3 then the pattern 10.1.0.0:16 has higher precedence than the pattern www.good.times.com. The \textit{ip-address}[::nbits] pattern always has higher precedence than host name patterns.

4. The pattern www.*.times.com has higher precedence than www.good.*.com because host name patterns are compared from end to beginning.

\textbf{Network Resource Access Control}

Authorization decisions made when an outgoing network connection is attempted answer the question: “Is the accessing user allowed to connect to the requested service on the specified remote host?” Authorization decisions made when an incoming network connection arrives at a host answer a slightly different question. Tivoli Policy Director for Operating Systems has no knowledge of the remote user making the incoming network connection request. The accessor is considered to be the accessor ID of the process accepting the incoming connection. The question being answered when making the authorization decision for NetIncoming resources is: “Is the user allowed to accept incoming connections for the requested service from a particular remote machine?” The user that must be given access by any ACLs placed on NetIncoming resources, therefore, is typically the root user because the processes that run on a machine that accept incoming connections to system services typically run as the root user.

Application services that are accessible over the network will often run as a user other than root. For these services it is that user who must be granted access by any ACLs protecting the NetIncoming resource.

\textbf{Login Policy}

Tivoli Policy Director for Operating Systems lets you control when and from where a user can log in to a system. The basic mechanisms for controlling user access are:

- Defining time-of-day login restrictions for users independent of where they log in from
- Defining access controls on local and remote terminals

Tivoli Policy Director for Operating Systems also provides the ability to enforce login activity related policy such as password expiry, automatically disabling accounts after a number of failed logins, and automatically disabling inactive accounts.

\textbf{Time-of-day Login Restrictions}

Time-of-day login restrictions are defined by specific policy attributes in the Tivoli Policy Director user registry. They can be specified globally, on a per-user basis, or specifically for unauthenticated users.

Time of day restrictions define hours of the day and days of the week during which users are permitted to log in. For users defined in the Tivoli Policy Director user registry, any user-specific policy overrides any global policy. For users not defined in the Tivoli Policy Director user registry, and therefore treated as unauthenticated by Tivoli Policy Director for Operating Systems, the per-user policy associated with the special osseal-unauth user overrides any global policy.

A time-of-day restriction is defined by a string of the following format:

\texttt{day-range:time-range[:utc|local]}

where:

\texttt{day-range}

Either \texttt{anyday}, \texttt{weekday}, or a comma-separated list of \texttt{sun}, \texttt{mon}, \texttt{tue}, \texttt{wed}, \texttt{thu}, \texttt{fri}, or \texttt{sat}. The \texttt{anyday} option indicates that the user is permitted to log in on any day.
of the week. The **weekday** option specifies that the user is permitted to log in on any day except for Saturday and Sunday. A list of days indicates that the user is permitted to log in only on the specified days.

**time-range**

Either **anytime** or a start time and end time. The **anytime** option indicates that the user is permitted to log in at any time on the days of the week that they are permitted to log in. If time is specified in the form `start_hhmm-end_hhmm`, the **start_hhmm** specifies the hour followed by minutes past the hour for the start time, and the **end_hhmm** specifies the end time.

**utc**

Specifies that the time-of-day restriction should be applied according to Universal Coordinated Time (UTC).

**local**

Specifies that the time-of-day restriction should be applied according to the local time on the system being logged on to. This is the default.

Use the Tivoli Policy Director administration command `pdadmin` to set time-of-day restrictions. The following are examples of time-of-day login policy usage:

1. To permit all users to log in only on weekdays from 9:00 A.M. to 5:00 P.M. local time, while permitting the root user to log in at any time, enter:
   
   ```
   pdadmin> policy set tod-access weekday:0900-1700:local
   pdadmin> policy set tod-access anyday:anytime -user root
   ```

2. To additionally constrain unauthenticated users to be allowed to log in only on Mondays, enter:
   
   ```
   pdadmin> policy set tod-access mon:0900-1700:local -user osseal-unauth
   ```

3. To restrict logins regardless of local time zone where the logins take place, enter:
   
   ```
   pdadmin> policy set tod-access weekday:0900-1700:utc
   pdadmin> policy set tod-access anyday:anytime -user root
   pdadmin> policy set tod-access mon:0900-1700:utc -user osseal-unauth
   ```

**Setting Holiday Login Restrictions**

You can specify additional time-of-day restrictions by defining Holidays. Holidays are protected resources that define exceptions to the regular time-of-day restrictions defined in the user registry. Holiday policy is applied when a user logs in.

You define a holiday by creating an object with the appropriate attributes set on it. Give the object a name that describes the holiday.

The ability of a user to log in on the holiday is controlled by the ACL attached to the same resource. The Login (L) permission must be granted to those users allowed to login. The format of the value of the Holiday-Dates extended attribute is a start time followed by an optional space and an end time. The specified time format follows:

```
YYYY-MM-DD[[-hh[:mm[:ss]]][Z]]
```

Where:

- **YYYY** Year specified as four digits.
- **MM** Month specified as a number from 1 to 12.
- **DD** Day of the month specified as a number from 1 to 31.
- **hh** Hour of the day specified from 0 to 23.
Minute of the hour specified from 0 to 59.

Second of the minute specified from 0 to 59.

Specifies use UTC instead of local time.

The following rules apply when interpreting start and end times that are only partially specified:

1. If no end time is specified, the holiday period ends at midnight of the same day on which it started.
2. Any time component not specified with a start time defaults to zero.
3. If an end time is specified with year, month, and day, but no hour, minute, or second, the holiday period ends at midnight of the day specified.
4. If an end time is specified with the hour or the hour and minute, any unspecified components default to zero.
5. If either start time or end time are specified in UTC, then both timestamps are interpreted as UTC.

**Example of Holiday Login**

Assume the three days around the CEO’s birthday, January 18, are a holiday. Only system administrators are allowed to work on January 17, 18, and 19. You could use the following commands to code the Holiday Restriction:

```bash
pdadmin> object create /OSSEAL/Servers/Login/Holidays/CEO-Birthday-Time "Happy" 0 ispolicyattachble yes
pdadmin> object modify /OSSEAL/Servers/Login/Holidays/CEO-Birthday-Time set attribute Holiday-Dates "2001-01-17-09:00:00 2001-01-19-17:00:00"
```

Then create the ACL for the holiday.

```bash
pdadmin> acl create ceo-birthday-time-acl
pdadmin> acl modify ceo-birthday-time-acl set group sys-admins
pdadmin> acl attach /OSSEAL/Servers/Login/Holidays/CEO-Birthday-Time ceo-birthday-time-acl
```

This policy permits only members of the Tivoli Policy Director group sys-admins to log in between 9:00 A.M. January 17, 2001 and 5:00 P.M. on January 19, 2001.

**Specifying Recurring Holidays**

You can specify recurring holidays by specifying multiple values for the Holiday-Dates extended attribute. To define the same CEO birthday policy for the year 2002, you can add the following command:

```bash
pdadmin> object modify /OSSEAL/Servers/Login/Holidays/CEO-Birthday-Time set attribute Holiday-Dates "2002-01-17-09:00:00 2002-01-19-17:00:00"
```

You can also specify holidays that have overlapping ranges. In such cases, the policy that is applied at any time is determined by the following rules:

1. The holiday range with the shortest period, if specified, is observed.
2. For holiday ranges with the same period, the holiday range with the earliest start time is observed.
3. Overlapping ranges specified as multiple values are not combined to form one long range.
To continue the example, if even system administrators were not allowed to log in on the actual birthday of the CEO, January 18, the following holiday policy could be defined:

```bash
pdadmin> object create/OSSEAL/Servers/Login/Holidays/CEO-Birthday "VeryHappy" 0 ispolicyattachable yes
pdadmin> object modify /OSSEAL/Servers/Login/Holidays/CEO-Birthday set attribute
       Holiday-Dates "2001-01-18-09:00:00 2001-01-18-17:00:00"
```

With the policy for both the CEO-Birthday holiday and the CEO-Birthday-Time holiday in effect, when a system administrator attempts to log in after 9:00am on January 17, the time matches the CEO-Birthday-Time holiday range and the login is successful.

If the system administrator attempts to log in after 9:00am on January 18, the attempt is denied. The shorter time of the CEO-Birthday holiday gives it precedence and the login is not successful.

If you attempt to define multiple holidays with the identical Holiday-Dates attributes, the PDOSD log file warnings indicate ambiguous policy specifications. The attempts are not allowed.

### Structure of Holiday Object Names

The structure of the object names beneath the Holidays resource type specifier is free form. You can structure the definition of holiday definitions to use the ACL inheritance. If you define holidays to use ACL inheritance, be aware that the precedence rules carry across all defined holidays within a policy branch without regard to any user-defined hierarchy. For example, you can define holidays named as:

```
/OSSEAL/policy-branch/Login/Holidays/CEO-Birthday/2001
/OSSEAL/policy-branch/Login/Holidays/CEO-Birthday/2002
/OSSEAL/policy-branch/Login/Holidays/CEO-Birthday/2003
```

with different date ranges specified for each year by attaching separate Holiday-Dates attributes for each of the leaf nodes. You could then attach a single ACL to CEO-Birthday.

### Login Location Restrictions

You can specify where users can log in. Define protected resources under the Terminal branch of the Login resource hierarchy to specify where users can log in. Login locations are referred to as terminals in this document.

### Local and Remote Terminals

Terminals are either local or remote. Terminals are local when used for logins to a system from serial devices and graphical consoles. Terminals are remote when used across a TCP/IP network. You can group both kinds of terminals together and use inheritance to define access controls. The names of terminal objects follow the format:

```
/OSSEAL/policy-branch/Login/Terminal/Local/termgroup/device
/OSSEAL/policy-branch/Login/Terminal/Remote/termgroup/hostspec
```

See Table 14 for definitions of terminal objects.

### Table 14. Definitions of Terms about Terminals

<table>
<thead>
<tr>
<th>Object name</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>termgroup</td>
<td>An administrator definable logical grouping of terminals allowing the application of inherited access controls</td>
<td>String. This component of the object name must be included.</td>
</tr>
</tbody>
</table>
Table 14. Definitions of Terms about Terminals (continued)

<table>
<thead>
<tr>
<th>Object name</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>device</td>
<td>The name of a terminal device on a system. For example, /dev/console or /dev/tty/0</td>
<td>A fully qualified UNIX file name specifying the device file. No wildcard names are allowed.</td>
</tr>
<tr>
<td>hostspec</td>
<td>The representation of a host, group of hosts, or network.</td>
<td>One of the following:</td>
</tr>
</tbody>
</table>

- A fully qualified host name from /etc/hosts, DNS, etc. The name can include wildcard characters such as * or ? but must always represent a fully qualified name. A simple, short name is not allowed.
- An IP address/netmask combination in dot notation (IP_address[nbits]). The absence of a specified netmask implies a 32–bit netmask, that is, a host address.

Some examples of login resource specifications follow:

/OSSEAL/policy-branch/Login/Terminal/Local/Modems/dev/tty063
/OSSEAL/policy-branch/Login/Terminal/Remote/Development/*.dev.company.com
/OSSEAL/policy-branch/Login/Terminal/Remote/Xterms/10.1.34.2:24

Access Control on Login Resources

Attach Policy Director access controls at the appropriate point in the Login/Terminal object hierarchy to control resources. For example, you can establish a default policy controlling system access from remote locations by attaching an ACL or a POP to the /OSSEAL/policy-branch/Terminal/Remote object.

Table 15 shows the permission required.

Table 15. Valid Permission to Log In

<table>
<thead>
<tr>
<th>Permission Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login (L)</td>
<td>Permission from the associated terminal</td>
</tr>
</tbody>
</table>

Uniqueness of Terminal Resources Definitions

A terminal can appear in only one terminal group within each policy branch. If a terminal appears in more than one group, a warning is generated in the PDOSD error log. The prevailing policy authorization is undefined. You will not get the expected results.

Login Activity Policy

Tivoli Policy Director for Operating Systems provides the ability to define and enforce policy related to login activity. The policy is defined centrally by using extended attributes of the /OSSEAL/policy-branch/Login object and controls the following aspects of login activity:

- Password expiry
- Account suspensions due to failed login attempts
- Account lockouts due to account inactivity

The status of each user account is recorded on a per-machine basis. Accounts become locked or suspended only on the machine on which they have been active or on which failed login attempts have occurred. Password expiry times are maintained on a per-machine basis. Tivoli Policy Director for Operating Systems login activity policy is applied in addition to any such policy provided natively by the system. The more restrictive of the Tivoli Policy Director for Operating Systems policy and the system policy will apply.

The system files $HOME/.rhosts and /etc/hosts.equiv should not be used when login activity policy is configured. The behavior of the system with these files in use is platform dependent. For instance, on AIX systems, the use of these system files, in conjunction with the authentication methods that use these files, such as rlogin, and rsh, can result in the complete circumvention of the login activity policy provided by Tivoli Policy Director for Operating Systems. Other login policy, such as terminal, time of day, and holiday, is enforced as expected.

There is no integration between the password policy specified in the Tivoli Policy Director user registry for Tivoli Policy Director users and the password expiry implemented by Tivoli Policy Director for Operating Systems for native system accounts. Table 16 describes the extended attributes that control login activity policy.

### Table 16. Login Activity Policy Attributes

<table>
<thead>
<tr>
<th>Login Activity Attribute</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login-MinPasswordDays</td>
<td>Minimum amount of time before a password can be changed. If not specified, a default value of zero is used indicating that password may be changed as frequently as a user likes.</td>
<td>Non-negative integer</td>
</tr>
<tr>
<td>Login-MaxPasswordDays</td>
<td>Maximum amount of time before a password must be changed. If not specified, the default value of zero is assumed and passwords will never be considered to have expired. Once a user’s password has expired they must change it on the next login unless grace logins are enabled. Grace logins are enabled by setting the Login-MaxGraceLogins attribute to a non-zero value.</td>
<td>Non-negative integer</td>
</tr>
<tr>
<td>Login-MaxGraceLogins</td>
<td>Number of times a user can login after their password has expired. If not specified, a default value of zero is assumed and the user is not permitted to login unless the password is changed. If the maximum number of grace logins is exceeded, the account will be locked permanently.</td>
<td>Non-negative integer</td>
</tr>
<tr>
<td>Login Activity Attribute</td>
<td>Description</td>
<td>Type</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Login-MaxConcurrent</td>
<td>Maximum number of terminals that can be logged in from concurrently by a specific user. Multiple logins from the same terminal count as a single login. A terminal is defined as a remote IP address or the local host. If a value is set for the default user, then the policy is applied to all users on a system. If not specified, a default value of zero is used indicating that there is no limit to the number of terminals from which a user can login.</td>
<td>Non-negative integer</td>
</tr>
<tr>
<td>Login-MaxInactiveDays</td>
<td>The number of days before an inactive account is locked permanently. An account is considered inactive from the last time a successful login occurred to that account. If not specified, the default value of zero is assumed and inactive accounts are never locked.</td>
<td>Non-negative integer</td>
</tr>
<tr>
<td>Login-MaxFailedLogins</td>
<td>Number of failed login attempts on an account before that account is suspended. The account is suspended for a period of time as determined by the value of the Login-LockMinutes attribute. The period of time over which the failed login attempts are counted is determined by the Login-LoginMinutes attribute. If the Login-MaxFailedLogins attribute is not specified, the default value of zero is assumed and the account will never be suspended due to failed login attempts.</td>
<td>Non-negative integer</td>
</tr>
<tr>
<td>Login-LockMinutes</td>
<td>The period of time in minutes to suspend an account when the maximum number of failed logins is reached, as determined by the Login-MaxFailedLogins attribute. If the Login-LockMinutes attribute is not specified, the default value of zero is assumed indicating the account will remain permanently suspended.</td>
<td>Non-negative integer</td>
</tr>
</tbody>
</table>
Table 16. Login Activity Policy Attributes (continued)

<table>
<thead>
<tr>
<th>Login Activity Attribute</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login-LoginMinutes</td>
<td>The period of time in minutes over which failed login attempts are counted towards the maximum number of failed login attempts as set in the Login-MaxFailedLogins attribute. If the Login-LoginMinutes attribute is not specified, the default value of zero is assumed indicating there is no time limit. All invalid login attempts while the account is not locked or suspended count towards the maximum number of failures.</td>
<td>Non-negative integer</td>
</tr>
<tr>
<td>Login-PolicyDisabled</td>
<td>Used to disable all login activity policy. If this attribute is present and the value is a non-empty string, then none of the defined login activity policy is enforced.</td>
<td>Non-empty string</td>
</tr>
</tbody>
</table>

Examples of Login Activity Policy

The following are examples of setting login activity policy.

1. To set accounts to be locked after 30 days of inactivity, you could use the `pdadmin` command:

   ```
padmin> object modify /OSSEAL/Servers/Login \
   set attribute Login-MaxInactiveDays 30
   ```

2. To allow only 3 failed login attempts in any one hour before suspending an account for 30 minutes, you could use the `pdadmin` command:

   ```
padmin> object modify /OSSEAL/Servers/Login \
   set attribute Login-MaxFailedLogins 3 
padmin> object modify /OSSEAL/Servers/Login \
   set attribute Login-LockMinutes 30 
padmin> object modify /OSSEAL/Servers/Login \
   set attribute Login-LoginMinutes 60
   ```

3. The login activity policy attributes are all single valued. When modifying a single valued attribute you must first remove the existing attribute value. For example, to change the Login-MaxFailedLogins attribute to 5:

   ```
padmin> object modify /OSSEAL/Servers/Login \
   delete attribute Login-MaxFailedLogins 
padmin> object modify /OSSEAL/Servers/Login \
   set attribute Login-MaxFailedLogins 5
   ```

   Use the `pdoslpadm` command to determine the state of an account or to unlock it. See `pdoslpadm` on page 166 for details on performing this task.
**User Exception Policy**

The user exception policy allows you to define exceptions to the default login activity policy. This capability is provided strictly as a mechanism to define exceptions to the default policy and should not be used to define login activity policy for a large number of users.

The user exception policy is defined by setting the login activity extended attributes on the `/OSSEAL/policy-branch/Login/UserExceptions/user-name` object. Only attributes that are explicitly set for this object apply to the user. Any login activity extended attribute not explicitly set is given a value of 0. These unspecified attributes do not inherit the value from the default login activity extended attributes.

The user exception policy cannot be specified as a task from the Tivoli desktop. Exceptions can only be made using the `pdadmin` command.

**Examples of User Exception Policy**

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
   ```

**Surrogate Policy**

Tivoli Policy Director for Operating Systems provides the ability to control operations that can change a process’s UNIX identity. Such operations are referred to as *surrogate* operations and are controlled by resources of type Surrogate. Surrogate operations can change a process’s user identity or group identity. Access control of each of these kinds of surrogate operations is established by applying authorization policy to the User and Group sub-types of the Surrogate resource type. The object names identify the potential targets of surrogate operations and control the ability, for example, to surrogate to the root user or the system group. Surrogate resources names follow the form:

```
/OSSEAL/policy-branch/Surrogate/User/user-name
/OSSEAL/policy-branch/Surrogate/Group/group-name
```
Table 17 details the surrogate objects presented above.

**Table 17. Surrogate Object Naming**

<table>
<thead>
<tr>
<th>Object Name</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>user-name</td>
<td>A UNIX user name. Attempts to change identity to this user are protected by the access controls applied to this object.</td>
<td>String representing the UNIX user name. Numeric user IDs are not accepted.</td>
</tr>
<tr>
<td>group-name</td>
<td>A UNIX group name. Attempts to change identity to this group are protected by the access controls applied to this object.</td>
<td>String representing the UNIX group name. Numeric group IDs are not accepted.</td>
</tr>
</tbody>
</table>

**Example Surrogate Resources**

Some example surrogate resource specifications are given below:

/OSSEAL/Default/Surrogate/User/root  
/OSSEAL/Default/Surrogate/User/joe  
/OSSEAL/Default/Surrogate/Group/admin

**Note:** The application of access controls to the /OSSEAL/policy-branch/Surrogate/User, the /OSSEAL/policy-branch/Surrogate/Group objects, or the containing /OSSEAL/policy-branch/Surrogate object itself allows the definition of default Surrogate policy. See the "Considerations for Establishing Surrogate Policy" for warnings about the implications of establishing Surrogate policy that is restrictive. No wildcarding is available for Surrogate resources.

The only permission used to control access to Surrogate resources is the Surrogate (G) permission as shown in [Table 18].

**Table 18. Surrogate Operation Permission**

<table>
<thead>
<tr>
<th>Permission</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>G</td>
<td>Surrogate</td>
<td>Permission to perform a user or group surrogate operation.</td>
</tr>
</tbody>
</table>

**Considerations for Establishing Surrogate Policy**

Surrogate operations occur in two fundamentally different ways:

- A running program, in the course of its execution, might change user or group identity.
- A program with either or both of the set user ID or set group ID UNIX file permissions set will change identity on execution.

The distinction is important. Programs that have the set user ID or set group ID permission set are generally intended to be run by unprivileged users who need to perform tasks that temporarily require more privilege than that user would normally have. Such programs are trusted only to perform prescribed operations while running with this elevated privilege. Typical examples, depending on the platform, include programs like /usr/bin/mail, /usr/bin/telnet, and /usr/bin/ps.

Assume these programs are all setuid root. If you restrict general users’ ability to surrogate to root, then they will no longer be able to run these programs. These programs are trusted to perform a limited set of operations while they are executing with elevated privilege. Tivoli Policy Director for Operating Systems lets you define them as part of a Trusted Computing Base so that surrogate operations performed when a program is executed occur without requiring an authorization decision.
Programs defined as Secure-Programs under the TCB resource type are permitted to change their user or group identity on execution without being subject to Surrogate authorization policy. See "Trusted Computing Base Resources" on page 23. If such a program performs subsequent surrogate operations after the program has been executed, then these operations are subject to Surrogate authorization policy.

Consider the /usr/bin/su command. This command lets a user who knows the password of another user, explicitly change to that user’s identity. UNIX security requires that only the root user is allowed to change user identity, therefore, the su command is set up on all UNIX systems as a setuid root program. If the su command were not made a Secure-Program in the Tivoli Policy Director for Operating Systems TCB then even users who are authorized to surrogate to other non-root users would require the ability to surrogate to root as well as the user they really wish to surrogate to. With the command configured as a Secure-Program the only Tivoli Policy Director for Operating Systems Surrogate authorization policy that is enforced is the that protecting the target user of su.

For example, assume user fred is authorized to change identity to the sysop user. When fred runs the su command:

```
fred$ su sysop
```

two surrogate operations occur. The first is a surrogate operation to root as su is a setuid root program. The second occurs when fred correctly enters the sysop account’s password and the su command explicitly changes identity to the sysop user. With the su command configured as a Secure-Program fred does not need Tivoli Policy Director for Operating Systems authority to surrogate to root, only to sysop.

The su command is the only standard UNIX command configured as a Secure-Program by default. Tivoli Policy Director for Operating Systems provides the pdosuidprog command to help you locate other setuid and setgid programs that you might want to add as Secure-Programs if you establish restrictive Surrogate policy. See "pdosuidprog" on page 187 for details of running this command.

If you establish restrictive Surrogate policy and add appropriate setuid and setgid programs as Secure-Programs in the TCB you might find that users running these programs still require Surrogate authority to users or groups you did not anticipate. The programs might be performing surrogate operations after they are executed. If this is the case and you do not wish to provide open access to these restricted user and group identities, then you can use Access-Restrictions to permit users to execute these surrogate operations only when running particular programs. ["Access Restrictions" on page 15] explains how such a policy may be defined.

When a UNIX user successfully executes a surrogate operation, the accessor identity that applies to Tivoli Policy Director for Operating Systems authorization decisions does not change. A surrogate operation cannot be used by a user to become someone else from Tivoli Policy Director for Operating Systems’s point of view. A second class of TCB programs, Impersonator-Programs, allows surrogate operations to change the Tivoli Policy Director for Operating Systems accessor identity as well as the UNIX user identity of the process. See "Trusted Computing Base Resources" on page 23 for more information about the Impersonator-Programs class of TCB resources.

**Access Control on Surrogate Resources**

Authorization policy associated with surrogate resources is expressed by attaching Tivoli Policy Director ACLs to the user name or group name objects. In addition, default surrogate policy for users and groups can be defined by attaching Tivoli Policy Director ACLs to the User or Group container objects and employing ACL inheritance. Also, attaching an ACL to
the Surrogate container object imposes default surrogate permissions for all users and groups (assuming the user and group containers do not have explicitly attached ACLs). The Tivoli Policy Director traverse (T) permission is also employed as part of the access control decision. Table 18 on page 40 details the valid ACL permissions that may be associated with surrogate resources.

**Sudo Policy**

Sudo resources describe commands that require access control at a finer grain than whether or not a particular program can be executed. Sudo commands allow access control based not only on a command but also on the parameters passed to that command. You can use Sudo commands to remove the requirement for users to become root on a system in order to perform administrative tasks. Sudo does this by providing the capability to execute a command as a UNIX user other than that of the invoker.

Sudo resources are identified in the Tivoli Policy Director namespace in the following way:

/OSSEAL/policy-branch/Sudo/sudo-command/[sudo-argclass]

The attributes of the Sudo command are listed in Table 19.

**Table 19. Sudo Objects**

<table>
<thead>
<tr>
<th>Object Name</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>sudo-command</strong></td>
<td>The name of the Sudo command. This is the object with which parameters describing the actual program, UNIX user identity, and password are associated. You specify this name.</td>
<td>String representing a Sudo command.</td>
</tr>
<tr>
<td><strong>sudo-argclass</strong></td>
<td>The name of a class of command arguments. The administrator chooses this name.</td>
<td>String representing a Sudo argument class.</td>
</tr>
</tbody>
</table>

Define the attributes of a Sudo command by creating an object that identifies the Sudo command. Set the Sudo command extended attributes on the object to the appropriate values. Table 20 lists the command attributes.

**Table 20. Sudo Command Attributes**

<table>
<thead>
<tr>
<th>Extended Attribute</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sudo-Command</td>
<td>The program to run when access to the Sudo command is granted. This parameter must be specified for Tivoli Policy Director for Operating Systems to consider the Sudo object as valid. This attribute is single-valued.</td>
<td>A fully qualified UNIX file name specifying the program.</td>
</tr>
</tbody>
</table>
Table 20. Sudo Command Attributes (continued)

<table>
<thead>
<tr>
<th>Extended Attribute</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sudo-Target-User</td>
<td>The UNIX user name under which the program specified by the Sudo-Command is run. This UNIX user must exist on every system on which the Sudo command needs to run. This attribute is optional. The default value is root. This attribute is single-valued.</td>
<td>A string representing the name of the UNIX user.</td>
</tr>
<tr>
<td>Sudo-Invoker-Password</td>
<td>This attribute indicates that the invoker of the Sudo command must enter a password before the command can be executed. The default is to not require the invoker’s password. This attribute is single valued.</td>
<td>The value must be a non-empty string.</td>
</tr>
<tr>
<td>Sudo-Target-Password</td>
<td>This attribute indicates that the invoker of the Sudo command must enter the password of the target user specified by the Sudo-Target-User attribute before the command can be executed. The default is to not require the invoker to supply the target user’s password. This attribute is single valued.</td>
<td>The value must be a non-empty string.</td>
</tr>
</tbody>
</table>

The execute (x) permission is required to execute a Sudo command as shown in Table 21.

Table 21. Permission Required for Sudo

<table>
<thead>
<tr>
<th>Permission Code</th>
<th>Permission Name</th>
<th>Permission Granted</th>
</tr>
</thead>
<tbody>
<tr>
<td>x</td>
<td>Execute</td>
<td>Execute the Sudo command</td>
</tr>
</tbody>
</table>

An Example of Sudo Usage

To define a Sudo command that allows only members of the sys-admin group to use the /usr/sbin/mount system program and that requires the invoker to enter their own password when running the command, you can use the following pdadmin commands:

```
padmin> object create /OSSEAL/Servers/Sudo/mount "mount" 2 \
ispolicyattachable yes
padmin> object modify /OSSEAL/Servers/Sudo/mount set attribute \
   Sudo-Command /usr/sbin/mount
padmin> object modify /OSSEAL/Servers/Sudo/mount set attribute \
   Sudo-Invoker-Password "required"
padmin> acl create sudo-mount
padmin> acl modify sudo-mount set group sys-admin T[OSSEAL]x
padmin> acl attach /OSSEAL/Servers/Sudo/mount sudo-mount
```

You can have fine-grained control over what arguments may be provided by defining a Sudo argument class object subordinate to the Sudo command object. Sudo argument class objects are defined in a similar manner to Sudo command objects by defining extended attributes of the Sudo argument class object. The extended attribute that is used to define a Sudo...
argument class is defined in Table 22:

Table 22. Extended Sudo Attributes for Fine-grained Control

<table>
<thead>
<tr>
<th>Extended Attribute</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sudo-Arguments</td>
<td>A wildcard string used to match command line arguments. This attribute is multi-valued allowing multiple patterns to describe a single argument class. There is no default value.</td>
<td>A wildcard string used to match command line arguments.</td>
</tr>
</tbody>
</table>

To continue the example, to allow members of the group net-admin to mount NFS file systems and only members of the group sys-admin to mount local file systems use the following pdadmin commands in addition to the ones above:

```
pdadmin> object create /OSSEAL/Servers/Sudo/mount/remote "Remote mount argument patterns" 0 ispolicyattachable yes
pdadmin> object modify /OSSEAL/Servers/Sudo/mount/remote set attribute Sudo-Arguments "[-]F nfs"
pdadmin> acl create sudo-net-mount
pdadmin> acl modify sudo-net-mount set group net-admin T[OSSEAL]x
pdadmin> acl attach /OSSEAL/Servers/Sudo/mount/remote sudo-net-mount
pdadmin> object create /OSSEAL/Servers/Sudo/mount/local "Local mount argument patterns" 0 ispolicyattachable yes
pdadmin> object modify /OSSEAL/Servers/Sudo/mount/local set attribute Sudo-Arguments "[-]F *"
pdadmin> acl create sudo-local-mount
pdadmin> acl modify sudo-local-mount set group sys-admin T[OSSEAL]x
pdadmin> acl attach /OSSEAL/Servers/Sudo/mount/local sudo-local-mount
pdadmin> acl modify sudo-mount set group sys-admin ""
```

An explanation of this example

The following notes help explain this example:

1. When setting an attribute value in pdadmin, the value may not start with a dash character. The dash is represented as [-], a character range containing only a hyphen (−).
2. The policy above relies on the precedence of the wildcard patterns. The '[-]F nfs' pattern is more specific than the '[-]F *' pattern.
3. The sys-admin group entry in the sudo-mount ACL attached to /OSSEAL/Servers/Sudo/mount was cleared. This prevents anyone from accessing the mount Sudo command unless they specify a –F parameter as the first option.
4. To accommodate the slightly different syntaxes of the mount command on different platforms, you can make the wildcarded expressions more complex. For example, mount might expect the –t option instead of the –F option in order to specify the file system type, or NFS might be accepted in place of nfs. To accommodate two cases, the value of the Sudo-Arguments attribute of the /OSSEAL/Servers/Sudo/mount/remote object can be replaced with [-][tF] [Nn][FF][Ss].
5. If the same pattern appears in two different Sudo argument classes of the same Sudo command a warning messages identifying the ambiguous policy is generated in the PDOSD daemon’s log file and an administrative audit event is generated. It is undefined which, if any, of the ambiguous policies is applied.

This syntax of UNIX commands can be very complex, allowing specification of command line options and parameters in any order and combination. This can make it difficult to
define argument patterns that cover all possibilities. By defining a default behavior that
denies access to the Sudo command, the combinations and order of command line options
can be restricted to a manageable set.

Wildcarding Sudo Arguments

The Sudo-Arguments attribute uses Tivoli Policy Director for Operating Systems wildcards
in a manner similar to the other resource types. The basic elements of the Sudo-Arguments
wildcard strings are the same as the other wildcards with the following exceptions:

- The wildcard asterisk (*) matches a sequence of non-white space characters rather than a
  sequence of any character. It matches an entire command line argument rather than the
  entire command line. For example, the following pattern matches an arbitrary string as
  the first argument followed by the string root as the second argument:
    * root

  If the second argument is not root this pattern does not match.

- A single space character in the pattern matches any sequence of white space characters
  in the string being matched. The special meaning of the space character can be escaped
  with a back slash character (\), in which case it matches only one space.

- If the Sudo-Arguments attribute has the value "", then this matches the empty string and
  allows the definition of a pattern that matches when no arguments are passed to the
  Sudo command.

- The pattern matches a string even if there are trailing arguments that were not matched
  by the pattern, as long as the preceding arguments matched the entire pattern. For
  example the pattern:
    * root

  matches both of the strings:
  show root
  add root system

The pdossudo Command

Invoke Sudo commands by entering the pdossudo command and specifying the Sudo
command name and any arguments. In "An Example of Sudo Usage" on page 43, the mount
Sudo command would be invoked as follows:

$ pdossudo mount -F nfs host:/shared/directory /local

The authorization process of a Sudo command proceeds in this order:

1. Determining whether the invoking user has execute permission on the requested Sudo
   command, or Sudo argument class if the arguments specified on the command line match
   an argument.

2. If they match, the invoking user is prompted for the required passwords, if any.

3. If all required passwords are entered correctly, then the effective UNIX user ID of the
   process is changed to that of the target user. This identity change is subject to Surrogate
   policy so the invoking user must have authority to Surrogate to the target user (this
   Surrogate authority can be restricted by using an Access-Restrictions attribute in order to
   only permit users to Surrogate when invoking the pdossudo command).

4. The Sudo command is executed only after all of these operations have completed
   successfully with the specified arguments.
You might also want to establish an Access-Restrictions attribute on the program specified in the Sudo-Command attribute restricting execution of this program to the pdossudo command.

The following `pdadmin` commands show how these Access-Restrictions might be established:

```
pdadmin> object create /OSSEAL/Servers/Surrogate/User/root
        "surrogate root" 14 ispolicyattachable yes
pdadmin> acl create root-user
pdadmin> acl modify root-user set any-other T[OSSEAL]G
pdadmin> acl modify root-user set unauthenticated T[OSSEAL]G
pdadmin> acl modify root-user set attribute \Access-Restrictions any-other:G:/opt/pdos/bin/pdossudo
pdadmin> acl modify root-user set attribute \Access-Restrictions unauthenticated:G:/opt/pdos/bin/pdossudo
pdadmin> acl attach /OSSEAL/Servers/Surrogate/User/root root-root-user

pdadmin> object create /OSSEAL/Servers/File/usr/bin/mount
        "mount command" 3 ispolicyattachable yes
pdadmin> acl create mount-program
pdadmin> acl modify mount-program set any-other T[OSSEAL]x
pdadmin> acl modify mount-program set unauthenticated T[OSSEAL]x
pdadmin> acl modify mount-program set attribute \Access-Restrictions any-other:x:/opt/pdos/bin/pdossudo
pdadmin> acl modify mount-program set attribute \Access-Restrictions unauthenticated:x:/opt/pdos/bin/pdossudo
pdadmin> acl attach /OSSEAL/Servers/File/usr/bin/mount mount-program
```

The `pdossudo` command is the only way to change identity to the root user with this policy in place.

In order to protect Sudo commands from being tricked by a user’s setting environment variables with the privilege of another UNIX user, the environment visible to the executed Sudo program is tightly controlled. An example of such a trick attempt is to change the PATH to values that would allow execution of inappropriate programs. Table 23 shows the environment variables that are stripped from the user’s environment before the Sudo command is executed:

**Table 23. Environment Variables Stripped by Sudo**

<table>
<thead>
<tr>
<th>Environment Variable</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>PATH</td>
<td>The command location path</td>
</tr>
<tr>
<td>LD_*</td>
<td>All shared library search path environment variables beginning with LD_*</td>
</tr>
<tr>
<td><em>RLD</em>*</td>
<td>All runtime linker environment variables beginning with <em>RLD</em>*</td>
</tr>
<tr>
<td>SHLIB_PATH</td>
<td>HP-UX only, the shared library search path</td>
</tr>
<tr>
<td>LIBPATH</td>
<td>AIX only, the shared library search path</td>
</tr>
<tr>
<td>IFS</td>
<td>The input field separator</td>
</tr>
<tr>
<td>ENV</td>
<td>Environment file location</td>
</tr>
<tr>
<td>BASH_ENV</td>
<td>Bash environment file location</td>
</tr>
<tr>
<td>KRB_CONF</td>
<td>Kerberos 4 configuration file location</td>
</tr>
<tr>
<td>KRB5_CONFIG</td>
<td>Kerberos 5 configuration file location</td>
</tr>
<tr>
<td>LOCALDOMAIN</td>
<td>Override for domain name in /etc/resolv.conf</td>
</tr>
<tr>
<td>RES_OPTIONS</td>
<td>Options for host name resolution</td>
</tr>
<tr>
<td>HOSTALIASES</td>
<td>Override for location of host alias specification file</td>
</tr>
</tbody>
</table>
Specify the values for these or other environment variables by defining them in the pdossudo configuration file: /opt/pdos/etc/pdossudo.conf. Environment variables are specified by defining them in the [environment] stanza of the file (this is the file’s only stanza). For example, a suitable pdossudo.conf configuration value for including an application’s commands and shared libraries in the appropriate search path might be:

```
[environment]
PATH=/usr/bin:/usr/sbin:/usr/application/bin
LD_LIBRARY_PATH=/usr/lib:/usr/application/lib
```

When the Sudo command is executed, the PATH and LD_LIBRARY_PATH environment variables will be set according those specified in the pdossudo.conf configuration file.

The `pdossudo` command also sets environment variables to permit scripts to identify the invoker of the command. They are defined in Table 24.

**Table 24. Environment Variables Set by Sudo**

<table>
<thead>
<tr>
<th>Environment Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDOS_SUDO_ACCESSOR_NAME</td>
<td>The user name corresponding to the Tivoli Policy Director for Operating Systems accessor ID of the user invoking the Sudo command.</td>
</tr>
<tr>
<td>PDOS_SUDO_ACCESSOR_ID</td>
<td>The numeric ID corresponding to the Tivoli Policy Director for Operating Systems accessor ID of the user invoking the Sudo command.</td>
</tr>
<tr>
<td>PDOS_SUDO_INVOKER_NAME</td>
<td>The user name corresponding to the UNIX user that invoked the <code>pdossudo</code> command. This might differ from the accessor name if an identity change occurred after login, for example, if the user executed the <code>su</code> command.</td>
</tr>
<tr>
<td>PDOS_SUDO_INVOKER_ID</td>
<td>The numeric ID corresponding to the UNIX user that invoked the <code>pdossudo</code> command. This might differ from the accessor name if an identity change occurred after login, for example, if the user executed the <code>su</code> command.</td>
</tr>
</tbody>
</table>
This chapter describes the major components of Tivoli Policy Director for Operating Systems and their operating environment. These components include:

- "The PDOSD Authorization Daemon" on page 50
- "The PDOSAUDITD Audit Daemon" on page 56
- "The PDOSWDD Watchdog Daemon" on page 57
- "The PDOSTECD Tivoli Enterprise Console Daemon" on page 59

The following topics are also described in this chapter:

- "Users and Groups" on page 60
- "Files and Directories" on page 62
- "Initial Policy" on page 65
- "Isolated Operation" on page 67

**Daemons**

The daemons responsible for the major functions of Tivoli Policy Director for Operating Systems are:

**PDOSD - The Authorization Daemon**
Makes authorization decisions and monitors the Trusted Computing Base (TCB).

**PDOSAUDITD - The Audit Daemon**
Receives audit events from other components of PDOS and manages the audit trail.

**PDOSWDD - The Watchdog Daemon**
Ensures that the other daemons remain available. The other daemons also monitor each another.

**PDOSTECD - The Tivoli Enterprise Console Daemon**
Makes many of the Tivoli Policy Director for Operating Systems audit events available to the Tivoli Enterprise Console.

Each daemon maintains a log file that records significant events and error conditions. The records written to the log files contain a UTC timestamp, information identifying the component logging the event, the message classification, and the message text. The log files are persistent across restarts of Tivoli Policy Director for Operating Systems.

You can configure how many log entries can be written to the log file before a new log is started. You can also configure, for each daemon, how many log files to maintain before re-using the files. By default, the log files are not automatically rolled over.
If log rollover is enabled, when the log file reaches the maximum number of entries, a new log file is created by appending a period and a number to the file. For instance, when the `pdosd.log` file is full, logging continues in a file called `pdosd.log.1`. When that log file is full, logging continues in `pdosd.log.2`.

You can set these and other runtime options with the `pdoscfg` command. "pdoscfg" on page 153 lists all the `pdoscfg` options. "Tuning the Configuration" on page 74 shows the mapping between the `pdoscfg` options and the configuration file attributes described in this chapter.

The PDOSD Authorization Daemon

PDOSD, the authorization daemon, does the following:

- Handles the authorization requests generated by the Tivoli Policy Director for Operating Systems kernel extension when it intercepts operations that are subject to policy
- Maps UNIX user identities to Tivoli Policy Director credentials that describe users and their group memberships from a Tivoli Policy Director point of view
- Monitors the files that constitute the TCB in order to detect any changes that would cause them to become untrusted

Credential Acquisition

The credential acquisition service is vital to the PDOSD daemon’s authorization decision process. "The UNIX Identity and Its Relationship to the Tivoli Policy Director User Identity" on page 3 discusses at a high level how a UNIX user’s identity is used to obtain a Tivoli Policy Director credential required for making an authorization decision. This section describes the lower-level aspects of this process. In order for Tivoli Policy Director for Operating Systems to make authorization decisions efficiently and also to ensure its ability to function in isolation from the LDAP user registry, credentials are cached by the PDOSD daemon as they are used. The PDOSD daemon uses an in-memory cache and a disk cache. All credentials are represented in the disk cache. Only active users have their credentials available in the memory cache.

There is one cached credential for each user. Credentials are cached as users login to the system. Each time a user logs into the system, Tivoli Policy Director for Operating Systems retrieves a new credential from the LDAP user registry and stores it in the credential cache. That user continues to use the cached credential until a new login operation is detected for that same user. When a new login operation is detected, Tivoli Policy Director for Operating Systems again retrieves a new credential from the LDAP user registry and replaces the cached credential with the new credential.

Once the new credential has been cached, any operations performed by that user, from any of the user’s login shells, use the newly cached credential until it is replaced or removed from the cache.

Refreshing the credential reflects any changes in the user’s group membership. A user’s group membership can change by being added to groups or by being removed from groups. Changes in group membership are not reflected until a user’s credential is refreshed.

You can use the `pdosrefresh` command to force a user’s credential to be refreshed without waiting for the user to log in again. Any group membership changes are then reflected immediately.

Each cached credential has a refresh time and a hold time associated with it:
Refresh time
When a credential’s refresh time is reached, the PDOSD daemon retrieves a new credential from the LDAP user registry and replaces the cached credential with the new credential.

Hold time
When a credential’s hold time is reached, the PDOSD daemon removes the credential from the cache. A new credential is retrieved from the LDAP user registry the next time it is needed by the PDOSD daemon.

Credential Acquisition and User Type
Tivoli Policy Director for Operating Systems users are classified as either:

- General users
- Administrative users, or administrators

Administrative users are defined as all users who are members of the **osseal-admin** Tivoli Policy Director group and the **osseal** UNIX group. Administrative users have the following attributes above those of general users:

- Credentials of administrative users are never flushed from the disk cache
- Credentials of administrative users are maintained on a system even for administrative users that have never logged on
- The default decision made by the PDOSD daemon when making a decision under error conditions is to grant access. For general users, the default decision is to deny.

Table 25 lists the configuration attributes pertaining to the Tivoli Policy Director for Operating Systems Credential Acquisition Service in the `/opt/pdos/etc/pdosd.conf` configuration file.

Table 25. PDOS Credential Configuration Attributes

<table>
<thead>
<tr>
<th>Stanza</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[credentials]</td>
<td>user-cred-refresh</td>
<td>The number of minutes that user credentials can exist in the credential cache before they are considered due for a refresh. The interval starts at the time the credential is cached. After the refresh interval is exceeded, the credential is refreshed.</td>
</tr>
<tr>
<td>[credentials]</td>
<td>admin-cred-refresh</td>
<td>The frequency of the refresh of the credentials of administrative users. This allows admin user credential refresh periods to be managed independently from those of the general user. It is also specified in minutes.</td>
</tr>
<tr>
<td>[credentials]</td>
<td>cred-hold</td>
<td>The number of minutes that non-admin credentials may remain in the credential cache beyond the time of their last access. Credentials of non-administrative users that remain cached beyond this time will be flushed from the cache. Administrative credentials are never flushed from the cache. The cred-hold interval must be at least as long as the user-cred-refresh interval.</td>
</tr>
</tbody>
</table>

If Tivoli Policy Director for Operating Systems cannot communicate with the Tivoli Policy Director user registry when a credential is due to be refreshed, that credential remains in the cache until communication with the user registry is reestablished. During that time the cached credential continues to be used by Tivoli Policy Director for Operating Systems.
Tivoli Policy Director for Operating Systems and the Tivoli Policy Director User Registry

Tivoli Policy Director for Operating Systems uses the Tivoli Policy Director Runtime Environment configuration for locating and communicating with the user registry. This enables Tivoli Policy Director for Operating Systems to share the user registry configuration with other components of Tivoli Policy Director, for example the location of user registry replicas. See the *Tivoli SecureWay Policy Director Base Administration Guide* for details on configuring the Tivoli Policy Director Runtime Environment. Tivoli Policy Director for Operating Systems supports only LDAP as the Tivoli Policy Director user registry.

Table 26 shows the configuration attributes in the PDOSD configuration file, `/opt/pdos/etc/pdosd.conf`, that control the daemon’s communications with the user registry. These attributes are established during configuration and should not be modified.

**Table 26. Configuration Attributes Controlling PDOSD’s Communications with the User Registry**

<table>
<thead>
<tr>
<th>Stanza</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ldap-server-config</td>
<td>Location of the Tivoli Policy Director Runtime LDAP configuration file.</td>
</tr>
<tr>
<td>[ldap]</td>
<td>ssl-enabled</td>
<td>Boolean flag indicating whether or not to use SSL communications with LDAP.</td>
</tr>
<tr>
<td></td>
<td>bind-dn</td>
<td>The distinguished name (DN) that the PDOSD daemon uses to authenticate.</td>
</tr>
<tr>
<td></td>
<td>bind-pwd</td>
<td>The password that the PDOSD daemon uses to authenticate.</td>
</tr>
</tbody>
</table>

**Security Considerations**

The attributes you set affect the security of your system. Be careful when you set or change these settings.

The use of SSL to communicate to the LDAP server allows for mutual authentication between the PDOSD daemon and the LDAP server. The certificate of the Certification Authority (CA) that signed the LDAP server’s certificate, provided at Tivoli Policy Director for Operating Systems configuration time enables the PDOSD daemon to verify that the LDAP server is the real LDAP server. Because the information provided by the LDAP server is used by the PDOSD daemon, through the Tivoli Policy Director runtime, to construct the user credentials used in making authorization decisions, this information must be trusted. Authentication of the LDAP server by the PDOSD daemon allows this level of trust. See the *Tivoli Policy Director for Operating Systems Installation Guide*.

Other sensitive information contained here is the DN and password used by the PDOSD daemon to authenticate itself to the LDAP user registry. Just as the PDOSD daemon must trust its source of information for constructing credentials, the LDAP server must allow only legitimate access that information.

To protect this information, the default policy established by Tivoli Policy Director for Operating Systems attaches the osseal-restricted ACL to the `/opt/pdos/etc` directory, which contains the Tivoli Policy Director for Operating Systems configuration files. This ACL permits access to only administrative users, that is, members of the osseal-admin group.
Authorization Decision Process

The PDOSD daemon is a local mode Tivoli Policy Director Authorization API application. The Tivoli Policy Director documentation describes this in detail. The PDOSD daemon replicates the master Tivoli Policy Director policy database and makes authorization decisions based on the information stored in this local replica. The first step in making an authorization decision is therefore obtaining a replica of the policy. The policy database is first replicated when Tivoli Policy Director for Operating Systems is initially configured. The master policy database is maintained by the Tivoli Policy Director management server. Updates to policy are distributed to replicas by the following mechanisms:

Active notification

When updates are made to the master policy database, the Tivoli Policy Director management server informs replica servers that have registered for notification that an update has occurred. The replica servers then download the updated database.

Polling

Replica servers periodically poll the Tivoli Policy Director management server to see if any updates to the master policy database have been made. If so, they then download the updated database.

Tivoli Policy Director for Operating Systems can use either or both of these mechanisms. The configuration attributes listed in Table 27 control whether the PDOSD daemon listens actively for policy update notifications or whether itpollsthe Tivoli Policy Director management server at regular intervals. They reside in the /opt/pdos/etc/pdosd.conf configuration file.

Table 27. Authorization Configuration Attributes

<table>
<thead>
<tr>
<th>Stanza</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[policy]</td>
<td>refresh-interval</td>
<td>The interval in minutes that the Tivoli Policy Director management server is polled for updates. A value of zero indicates that polling should not occur.</td>
</tr>
<tr>
<td>[ssl]</td>
<td>ssl-listening-port</td>
<td>The TCP/IP port assigned to the PDOSD daemon to listen for policy update notifications from the Tivoli Policy Director management server. A value of zero indicates that policy updates should not be listened for.</td>
</tr>
</tbody>
</table>

When the Tivoli Policy Director for Operating Systems kernel extension intercepts a system operation that requires an authorization decision, it requests the decision from the PDOSD daemon. The information that is provided by the kernel about the operation being performed is used to make the authorization decision. This information consists of:

- The numerical accessor identity of the user attempting the operation. This can be different from the UID of the process performing the operation because a process in which a surrogate operation has been performed will be running as the surrogate user identity. The accessor identity from a Tivoli Policy Director for Operating Systems point of view is still the original identity of the process. The accessor identity is typically established at login time and is the ID corresponding to the login.
- The resource the operation is being applied to.
- The attempted operation.
- The time the operation is occurring.
- The program being used to perform the operation.
This information is compared by the PDOSD daemon to the policy stored in the local replica of the policy database. Tivoli Policy Director for Operating Systems decides whether or not the operation should be permitted based on the comparison. Only policy contained under the policy branch the machine subscribes to is used in the comparison. The policy-branch is specified during initial configuration of Tivoli Policy Director for Operating Systems. The configuration attribute listed in Table 28 specifies the policy-branch name and is found in the /opt/pdos/etc/osseal.conf file.

During this process an operational error might occur if there is a hardware failure on the machine or if the system has insufficient virtual memory available. Tivoli Policy Director for Operating Systems is structured to minimize the possibility of such events impacting the authorization process. If the PDOSD daemon is unable to make a decision based on the authorization policy, it applies a default decision based on whether the user is an administrative user or not. For an administrative user the default decision under error conditions is to grant access. Non-administrative users are denied access under error conditions.

Table 28. Authorization Policy-branch Configuration Attribute

<table>
<thead>
<tr>
<th>Stanza</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[policy]</td>
<td>branch</td>
<td>Name of the policy branch to which this machine subscribes.</td>
</tr>
</tbody>
</table>

**TCB Monitoring**

The PDOSD daemon periodically checks each file in the TCB for changes. The set of a file’s attributes that are monitored is called that file’s signature. Any change to one of those attributes causes a change to the file’s signature. When the signature change is detected, the PDOSD daemon marks that file as untrusted. Untrusted TCB files cannot be executed. Administrative audit events are generated for other accesses permitted by access controls to an untrusted TCB file.

The following attributes make up a file’s signature:

- File size
- File creation time
- File modify time
- File permissions
- File ownership
- File type (such as regular file, directory, or soft-link)
- Content checksum (for regular files)

The interval over which the PDOSD daemon checks all the TCB files is configurable. The checking of the files is evenly distributed throughout this interval. If the TCB contains a large number of files, this interval might be too short to check every file before the interval expires. If this situation occurs, the PDOSD daemon generates warnings in its log file, /var/pdos/log/pdosd.log.

The PDOSD daemon makes an explicit check of an executable file’s signature when making an authorization decision initiated by the attempted execution of a program defined in the TCB. By default, this includes checking the CRC of the executable file. This behavior can be changed by using the -nocrc_on_exec configuration option.
Several configuration attributes are available to control the amount of processing resource that the PDOSD daemon should devote to TCB file monitoring. Table 29 describes the attributes specified in the /opt/pdos/etc/pdosd.conf configuration file.

**Table 29. PDOSD TCB File Monitoring Resource Configuration Attributes**

<table>
<thead>
<tr>
<th>Stanza</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[tcb]</td>
<td>monitor-threads</td>
<td>Controls the number of threads engaged in TCB monitoring. The TCB monitoring load is evenly distributed among the threads. It is useful to increase this value only on multi-processor systems. You do not need more monitor threads than CPUs.</td>
</tr>
<tr>
<td></td>
<td>interval</td>
<td>The interval in minutes over which the entire TCB is scanned for changes. Increasing this interval reduces the load of the TCB monitoring system but increases the time in which you can expect a change to be detected.</td>
</tr>
<tr>
<td></td>
<td>max-checksum-file-size</td>
<td>Controls the number of bytes that are considered significant in the calculation of a file’s checksum. This provides a degree of checksum monitoring of very large files without committing extensive computing resources. The bytes used in calculation of the checksum are chosen from locations distributed throughout the file instead of just at the beginning or end to maximize the probability of detecting a change. The most expensive operation performed in TCB monitoring is checksum calculation.</td>
</tr>
<tr>
<td></td>
<td>ignore-ctime</td>
<td>Causes ctime to be ignored when performing TCB signature comparisons. When this option is enabled, a change in ctime does not cause the TCB resource to become untrusted.</td>
</tr>
<tr>
<td></td>
<td>nocrc_on_exec</td>
<td>Causes the CRC check that normally occurs as part of the authorization check associated with running an executable file to be skipped. Enabling this option avoids performing the CRC check on large binary files.</td>
</tr>
</tbody>
</table>

The trust states and signatures of TCB files are maintained on a per-machine basis and are not distributed back to the central Tivoli Policy Director management server. This recognizes that the same file might have different signatures on each machine and might be trusted or untrusted independently on each machine. Once a file becomes untrusted it remains untrusted until the `pdosobjsig` command is used to retrust that file. You can also use the `pdosobjsig` command to generate lists of trusted or untrusted files and for other tasks related to maintaining and examining the state of the TCB.

**PDOSD Log Configuration**
The PDOSD daemon maintains a log file called `/var/pdos/log/pdosd.log` that records significant events and error conditions associated with the daemon itself. Entries in this file are written in text format and consist of:

- A UTC (Universal Time Coordinated) timestamp
- Information identifying the component recording the message
- The message classification
- The message text
Table 30 lists the attributes that control this log file.

**Table 30. PDOSD Log Configuration Attributes**

<table>
<thead>
<tr>
<th>Stanza</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[pdosd]</td>
<td>log-entries</td>
<td>The number of entries that can be written to the PDOSD log file before rolling over to a new file. The default value of zero indicates that the log file should never be rolled over.</td>
</tr>
<tr>
<td></td>
<td>logs</td>
<td>The number of log files to be written before recycling the first one. A value of zero indicates that log files should never be recycled. If the log-entries attribute is zero, this value is ignored.</td>
</tr>
</tbody>
</table>

The **PDOSAUDITD Audit Daemon**

The PDOSAUDITD audit daemon manages the Tivoli Policy Director for Operating Systems audit log. The audit daemon receives binary audit records from the daemons, kernel extension, and the pdosobjsig command and stores them in memory and writes them to the audit log on a regular basis. The active audit log is /var/pdos/audit/audit.log.

The PDOSTECD daemon uses the audit.log file as input. If the file is removed, the PDOSTECD daemon shuts down and must be manually restarted after the audit.log file is made available again.

Components generate audit records based on the audit level settings. For authorization decisions, the global audit level, global warning level, resource audit level, and resource warning level are all considered. In the case of a non-authorization decision, only the global audit level is used.

The global audit level is set in the /opt/pdos/etc/osseal.conf configuration file. The format of the global audit level attribute in this file is shown in Table 31. This configuration file is read by the daemons when they start. The pdosctl command can be used to change the global audit level during system operation.

**Table 31. Global Audit Level Configuration Attribute**

<table>
<thead>
<tr>
<th>Stanza</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[audit]</td>
<td>level</td>
<td>The global audit level in effect when the daemons are started.</td>
</tr>
</tbody>
</table>

The PDOSAUDITD daemon maintains a separate log file called /var/pdos/log/pdosauditd.log that records significant events and error conditions associated with the daemon itself. Entries in this file are written in text format and consist of:

- A UTC (Universal Time Coordinated) timestamp
- Information identifying the component recording the message
- The message classification
- The message text

**PDOSAUDITD Configuration**

The configuration of the PDOSAUDITD daemon is controlled by setting attributes in the /opt/pdos/etc/pdosauditd.conf file.

Two attributes in this file control how the audit log is managed.
The **audit-logflush** attribute specifies the frequency, in seconds, at which the PDOSAUDITD daemon should flush audit records from memory to the audit log. By default, the log is flushed every 5 seconds.

The **audit-logsize** attribute specifies the maximum size, in bytes, that the audit log can reach before the audit log is renamed and a new audit log is started. A value of 0 indicates there is no maximum size for the audit log. The default size is 1000000 bytes.

When the audit log reaches the maximum size specified, the current audit log file in the /var/pdos/audit directory is renamed using the current timestamp from audit.log to audit.log.YYYY-MM-DD-HH-MM-SS. Logging then continues in a new audit.log file in the same directory.

Two other attributes in the configuration file control how the PDOSAUDITD log is managed.

- The **log-entries** attribute specifies the maximum number of entries that can be written to the log before the log is renamed and a new one started. The default value is zero, which indicates that the log should never be rolled over.

- The **logs** attribute specifies the maximum number of individual log files that can be written before the oldest one is reused. If the **log-entries** attribute is zero, this value is ignored.

| Table 32 describes all of the PDOSAUDITD configuration file attributes for managing the audit.log file and the pdosauditd.log file. These settings also can be changed with the pdoscfg command described in “pdoscfg” on page 153.

### Table 32. PDOSAUDITD Configuration Attributes

<table>
<thead>
<tr>
<th>Stanza</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[pdosauditd]</td>
<td>audit-logflush</td>
<td>Interval in seconds that PDOSAUDITD daemon flushes the audit records to the audit log. The default is 5 seconds.</td>
</tr>
<tr>
<td></td>
<td>audit-logsize</td>
<td>Maximum size in bytes to which the audit log can grow before PDOSAUDITD rolls over to use a new log file. The default is 1000000 bytes.</td>
</tr>
<tr>
<td></td>
<td>log-entries</td>
<td>The number of entries that can be written to PDOSAUDITD log file before the log file is automatically rolled over to a new file. A value of zero indicates that the log file should never be rolled over. The default value is 0.</td>
</tr>
<tr>
<td></td>
<td>logs</td>
<td>The number of log files to be written before recycling the first one. A value of zero indicates that log files should never be recycled. This value is ignored if the <strong>log-entries</strong> attribute is zero.</td>
</tr>
</tbody>
</table>

For information about enabling auditing see “Using Auditing to Verify Policy” on page 78. See “Viewing Audit Logs” on page 134 for information on viewing audit logs.

#### The PDOSWDD Watchdog Daemon

The PDOSWDD Watchdog Daemon monitors the availability of the PDOSD and PDOSAUDITD daemons. These three daemons monitor each other in the same manner; this is the watchdog daemon’s only function. This self-monitoring function, as implemented by each of the daemons, is the watchdog system. The watchdog system ensures the high availability of Tivoli Policy Director for Operating Systems services on a machine.
Note: The PDOSTECD daemon, described in ‘The PDOSTECD Tivoli Enterprise Console Daemon’ on page 59 is not monitored by either the PDOSD, PDOSAUDITD, or PDOSWDD.

When deployed, Tivoli Policy Director for Operating Systems constitutes a core component of the system that it is protecting. Ensuring that it remains available is vital to maintaining the integrity of the system and helps protect against attacks that might cause the daemons to terminate abnormally.

The PDOSWDD daemon maintains a log file called /var/pdos/log/pdoswdd.log that records significant events and error conditions associated with the daemon itself. Entries in this file are written in text format and consist of:

- A UTC (Universal Time Coordinated) timestamp
- Information identifying the component recording the message
- The message classification
- The message text

**PDOSWDD Configuration**

Configuration of the PDOSWDD daemon is done using the PDOSWDD configuration file, /opt/pdos/etc/pdoswdd.conf.

The two attributes in the configuration file control how the PDOSWDD log is managed.

- The **log-entries** attribute specifies the maximum number of entries that can be written to the log before the log is renamed and a new one started. The default value is zero, which indicates that the log should never be rolled over.

- The **logs** attribute specifies the maximum number of individual log files that can be written before the oldest one is reused. If the **log-entries** attribute is zero, this value is ignored.

Table 34 on page 60 describes the PDOSWDD configuration file attributes for managing the pdoswdd.file.

**Table 33. PDOSWDD Configuration Attributes**

<table>
<thead>
<tr>
<th>Stanza</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[pdoswdd]</td>
<td>log-entries</td>
<td>The number of entries that can be written to the PDOSWDD daemon log file before rolling over to a new file. The default value of zero indicates that the log file should never be rolled over.</td>
</tr>
<tr>
<td></td>
<td>logs</td>
<td>The number of log files to be written before recycling the first one. A value of zero indicates that log files should never be recycled. If the <strong>log-entries</strong> attribute is zero, this value is ignored.</td>
</tr>
</tbody>
</table>

If one of the daemons terminates abnormally, the watchdog system detects this and generates a log message in the error log of the daemon that detected the abnormal termination. Watchdog log messages can therefore appear in any daemon log file:

**PDOSD**

/var/pdos/log/pdosd.log

**PDOSAUDITD**

/var/pdos/log/pdosauditd.log
If administrative audit events are enabled, an audit event also is written to the audit log to record the abnormal termination.

The PDOSTECD Tivoli Enterprise Console Daemon

The PDOSTECD daemon makes a subset of the audit events produced by Tivoli Policy Director for Operating Systems available to the Tivoli Enterprise Console. The daemon reads the active log file, /var/pdos/audit/audit.log, and records relevant audit events to a file called /var/pdos/tec/tec.log which the Tivoli Enterprise Console logfile adapter can monitor. A description of the events made available can be found in Appendix C, “Tivoli Enterprise Console Events” on page 209.

If the PDOSTECD daemon cannot access the /var/pdos/audit/audit.log file, the daemon shuts down. The daemon must be manually restarted after the audit.log file becomes available again.

The tec.log file grows unbounded and must be cleared periodically to keep the /var filesystem from becoming full. See “Periodic Log Maintenance” on page 60 for details.

The PDOSTECD daemon maintains a log file called /var/pdos/pdostecd/pdostecd.log that records significant events and error conditions associated with the daemon itself. Entries in this file are written in text format and consist of:

- A UTC (Universal Time Coordinated) timestamp
- Information identifying the component recording the message
- The message classification
- The message text

PDOSTECD Configuration

Configuration of the PDOSTECD daemon is done using the PDOSTECD configuration file, /opt/pdos/etc/pdostecd.conf.

The two attributes in the configuration file control how the PDOSTECD log is managed.

- The log-entries attribute specifies the maximum number of entries that can be written to the log before the log is renamed and a new one started. The default value is zero, which indicates that the log should never be rolled over.
- The logs attribute specifies the maximum number of individual log files that can be written before the oldest one is reused. If the log-entries attribute is zero, this value is ignored.

Table 34 on page 60 describes the PDOSTECD configuration file attributes for managing the /var/pdos/pdostecd/pdostecd.log file.
Table 34. PDOSTECD Configuration Attributes

<table>
<thead>
<tr>
<th>Stanza</th>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[pdostecd]</td>
<td>log-entries</td>
<td>The number of entries that can be written to the PDOSTECD daemon log file before rolling over to a new file. The default value of zero indicates that the log file should never be rolled over.</td>
</tr>
<tr>
<td></td>
<td>logs</td>
<td>The number of log files to be written before recycling the first one. A value of zero indicates that log files should never be recycled. If the log-entries attribute is zero, this value is ignored.</td>
</tr>
</tbody>
</table>

Periodic Log Maintenance

The /var/pdos/tec/tec.log grows unbounded. This file must be cleared periodically to prevent the /var filesystem from running out of space. This can be accomplished by the Tivoli Scheduler, or with a script using the UNIX cron utility.

The basic operation of the script would be as follows.

1. Stop the PDOSTECD daemon. This stops new records from being written to the log file.
   
   /opt/pdos/bin/rc.pdostecd stop

2. Sleep for a sufficient amount of time to allow the Tivoli Enterprise Console UNIX logfile adapter to complete the processing of the existing records in the tec.log file. For instance, to sleep for 5 minutes:
   
   sleep 300

3. Restart the PDOSTECD daemon. The daemon deletes the existing tec.log file and creates a new one.

   /opt/pdos/bin/rc.pdostecd start

This operation should be done during periods of minimal activity in the system. The PDOSTECD daemon attempts to resume processing the audit log file at the place where it stopped. If there was a lot of audit activity while the daemon was inactive, it is possible that the audit log file has wrapped. If the PDOSTECD daemon is unable to locate its resume point, processing resumes at the end of the current audit log file.

Users and Groups

Tivoli Policy Director for Operating Systems uses various Tivoli Policy Director and UNIX users and groups. The necessary Tivoli Policy Director users and groups are created during the initial configuration of Tivoli Policy Director for Operating Systems. The UNIX users and groups are created on each Tivoli Policy Director for Operating Systems system during installation.

The role of each of these users and groups is discussed in this section.

osseal-admin Group

The osseal-admin group is a Tivoli Policy Director group that identifies users that are administrative users, or administrators. The corresponding UNIX group is called osseal. Administrators are treated slightly differently from general users, according to the following rules.
Credentials of administrators are never flushed from the disk cache. The credentials of a general user are flushed from the disk cache after the credential hold time expires for those credentials.

Credentials of administrators are maintained on a system even if an administrator has never logged on to the system. It is important to allow administrators to access a system they have never logged into before, even if that system is isolated from the Tivoli Policy Director user registry. General users do not have a credential cached on a system until they have logged in to it for the first time.

The default decision made by the PDOSD daemon when making a decision under error conditions is to grant access for administrators. For general users the default decision is to deny. “The PDOSD Authorization Daemon” on page 50 has more information about such error conditions.

When Tivoli Policy Director for Operating Systems is configured for the first time, the membership of the osseal-admin group consists of two users, root and osseal. Do not remove the osseal user ID from this group.

osseal Group

The osseal group is a UNIX group that identifies users that are administrative users, or administrators on a particular system. This group corresponds to the osseal-admin group in Tivoli Policy Director. This group is used to permit access using the various setgid commands provided by Tivoli Policy Director for Operating Systems to resources protected by UNIX security under the /var/pdos directory. This group is the primary group of the osseal UNIX user ID. Do not remove the osseal user ID from this group.

Users who are members of both the osseal-admin and osseal groups are called Tivoli Policy Director for Operating Systems runtime administrators and are authorized to perform the tasks associated with managing the Tivoli Policy Director for Operating Systems runtime environment.

osseal User

The osseal user is represented in both Tivoli Policy Director and UNIX. Tivoli Policy Director for Operating Systems treats this user in a special way on the UNIX system. The osseal user is an identity that the Tivoli Policy Director for Operating Systems daemons and commands adopt when they are running.

root User

Configuring Tivoli Policy Director for Operating Systems initially creates a Tivoli Policy Director user ID of root. This user corresponds to the root UNIX user to ensure that root can never be treated as an unauthenticated user. The root user is initially made a member of the osseal-admin group. The root user’s membership in the osseal-admin group ensures that the root user’s credentials are always available on all Tivoli Policy Director for Operating Systems systems.

The root user represents the UNIX root user across all Tivoli Policy Director for Operating Systems systems sharing the same Tivoli Policy Director user registry.

osseal-auditors Group

The osseal-auditors group is a Tivoli Policy Director group that identifies users that are auditors. The corresponding UNIX group is called ossaudit.

When Tivoli Policy Director for Operating Systems is configured for the first time, the membership of the osseal-auditors group consists of two users, root and osseal.
ossaudit Group

The ossaudit group is a UNIX group that identifies users that are auditors. This group corresponds to the osseal-auditors group in Tivoli Policy Director. The osseal user is a member of this group.

Users who are members of both the osseal-auditors and ossaudit groups are called Tivoli Policy Director for Operating Systems auditors and are authorized to perform the tasks associated with accessing the Tivoli Policy Director for Operating Systems audit trail. Do not remove the osseal user ID from this group.

osseal-unauth User

The osseal-unauth user has only a Tivoli Policy Director representation. It has no UNIX equivalent. It controls time-of-day login restrictions for unauthenticated, from a Tivoli Policy Director point of view, users independently from authenticated users. This is similar to the role of the unauthenticated entry in an ACL entry.

pdosd-hostname User

The Tivoli Policy Director management server does not allow every user to replicate the policy database. A Tivoli Policy Director user is created during configuration for each instance of the PDOSD daemon that runs in the secure domain managed by the Tivoli Policy Director management server. Because one of these users is created for each Tivoli Policy Director for Operating Systems system, the fully-qualified DNS host name for the machine is included in the name, for example, pdosd-hostname user. When the DNS name is not available the host’s name is used instead. The PDOSD daemon authenticates to the Tivoli Policy Director management server as this user in order to receive policy updates. Do not modify this user and its group membership.

Files and Directories

Tivoli Policy Director for Operating Systems installs itself into common locations on all platforms. This is necessary because various components have important implications to the security of the system and access is controlled to these components using Tivoli Policy Director for Operating Systems policy. A simpler policy results if the location of common resources is consistent across systems.

This section summarizes the role of the various files and directories used by Tivoli Policy Director for Operating Systems.

/opt/pdos/bin

Contains all of the binary executable images that comprise the user level runtime.

/opt/pdos/etc

Contains configuration files for the various components that use configuration files; in particular:

osseal.conf

A general configuration file containing configuration common to all components.

pdosd.conf

The PDOSD daemon’s configuration file.

pdosaudidt.conf

The PDOSAUDITD daemon’s configuration file.
pdoswdd.conf
The PDOSWDD daemon’s configuration file.

pdostecd.conf
The PDOSTECO daemon’s configuration file.

pdossudo.conf
The PDOSSUDO configuration file.

lpm.conf
The login activity policy configuration file.

This directory also contains other administrative information such as descriptions of
the initial policy established during configuration, the files and directories that are
backed up and restored by the pdosbkup and pdosrstr commands, and template
configuration files that provide basic descriptions of the various configuration
attributes.

/opt/pdos/kernel
Contains binaries and files related to Tivoli Policy Director for Operating Systems
kernel functionality.

/opt/pdos/lib
Contains the shared libraries that contain executable code shared by the various
commands.

/var/pdos/audit
Contains the Tivoli Policy Director for Operating Systems audit file,
/var/pdos/audit/audit.log.

/var/pdos/azn
Contains the local replica of the Tivoli Policy Director policy database in
authzn_replica.db.

/var/pdos/certs
Contains files that contain the certificates that the PDOSD daemon uses when
mutually authenticating with both the Tivoli Policy Director management server and
the LDAP User Registry server.

/var/pdos/cred
Contains the cached Tivoli Policy Director credentials.

/var/pdos/hla
Contains the host look-aside database that is used to cache IP address to hostname
mappings when this feature is enabled.

/var/pdos/log
Contains the log files for all of the daemons (except the PDOSTECO daemon) and
the configuration, unconfiguration, backup, and restore commands.

/var/pdos/login
Contains temporary files associated with the login activity policy.

/var/pdos/lpm
Contains the local machine information needed to enforce login account activity and
password policy.

/var/pdos/nls
Contains language specific files.
Files and Directories

/var/pdos/pdosauditd
This directory is used as the current working directory for the PDOSAUDITD daemon while it is running. If an error resulting in a core file occurs, this directory is where the core file will be located.

/var/pdos/pdosbkup
This directory is used as the current working directory for the pdosbkup and pdosrsstr commands while they are running. The backup file created by the pdosbkup command is written to this directory by default. If an error resulting in a core file occurs during the execution of either command, this directory is where the core file will be located.

/var/pdos/pdoscfg
This directory is used as the current working directory for the pdoscfg and pdosucfg commands while they are running. If an error resulting in a core file occurs, this directory is where the core file will be located.

/var/pdos/pdosd
This directory is used as the current working directory for the PDOSD daemon while it is running. If an error resulting in a core file occurs, this directory is where the core file will be located.

/var/pdos/pdossteed
This directory is used as the current working directory for the PDOSTECD daemon while it is running. If an error resulting in a core file occurs, this directory is where the core file will be located. This is also the location of the error log for the PDOSTECD daemon.

/var/pdos/pdoswdd
This directory is used as the current working directory for the PDOSWDD daemon while it is running. If an error resulting in a core file occurs, this directory is where the core file will be located.

/var/pdos/tcb
Contains the information used to detect changes to the files comprising the Trusted Computing Base (TCB).

/var/pdos/tec
Contains the file with audit events that is monitored by the Tivoli Enterprise Console logfile adapter.

/var/pdos/uid
Contains the cache of UIDs and GIDs to user and group names when this feature is enabled. No management of this cached information is required.

/var/pdos/umsg
Contains files used for inter-process communication and synchronization between components of Tivoli Policy Director for Operating Systems.

/var/pdos/uuid
Caches information related Tivoli Policy Director group names and UUID. No management of this cached information is required.

/var/pdos/watch
Contains files used by the watchdog system to detect abnormal termination of the PDOSD, PDOSAUDITD, or PDOSWDD daemons.
Initial Policy

The following components of the policy are established when Tivoli Policy Director for Operating Systems is initially configured:

**once-only**
This policy is shared across all policy branches. It comprises the actions used to represent Tivoli Policy Director for Operating Systems operations, ACLs used to protect resources, the users and groups discussed previously, and the /OSSEAL object space under which all protected objects reside.

**per-policy**
This policy is established for each policy branch that you use. It describes the contents of the Trusted Computing Base (TCB) and attaches the ACLs and POPs that Tivoli Policy Director for Operating Systems uses to protect itself from being compromised.

The default policy established by Tivoli Policy Director for Operating Systems ensures that the system functions properly and maintains a secure environment. The existing default policy should not be modified.

The remainder of this section describes the ACLs established during policy creation and the resources that they protect. The default policy is sufficient to protect Tivoli Policy Director for Operating Systems without adding any additional authorization policy to other resources on a system except for system programs defined as initial members of the TCB. See "Trusted Computing Base Resources" on page 23 for more information about the initial population of the TCB.

**osseal-audit**
This ACL controls access to the /var/pdos/audit directory, where the Tivoli Policy Director for Operating Systems audit trail resides, and to the /var/pdos/tec directory. The ACL permits only members of the osseal-auditors group to access the directory or, by inheritance, its contents.

**osseal-audit-exec**
This ACL controls access to the pdosaudview command, /opt/pdos/bin/pdosaudview. Members of the osseal-auditors group are granted full access to this command. All other users are restricted from this command.

**osseal-credentials**
This ACL controls access to the directories that make up the Tivoli Policy Director for Operating Systems credential cache: /var/pdos/cred and /var/pdos/uuid. It grants all users the ability to refresh and destroy credentials but only using the pdosrefresh and pdosdestroy commands. Tivoli Policy Director for Operating Systems ensures that users are allowed to refresh and destroy only their own credentials unless granted access by access controls to the credential cache directories. This ACL restricts the ability to refresh or destroy any user’s credentials to members of the osseal-admin group.

**osseal-default**
This is a fully permissive ACL. It is applied at namespace root for Tivoli Policy Director for Operating Systems: /OSSEAL. Its presence ensures that authorization decisions never propagate all the way to the root of the Tivoli Policy Directory object name space.
osseal-default-file
This is a fully permissive ACL that is in place as a reminder that Tivoli Policy Director for Operating Systems File resources violate the Tivoli Policy Director inheritance algorithm by not inheriting ACLs from placed above this point in the tree.

osseal-default-login
This ACL defines default Login resource policy. It permits everyone to login.

osseal-default-net-incoming
This ACL define default NetIncoming resource policy. It permits incoming connections from any host to any service to be accepted by any user.

osseal-default-net-outgoing
This ACL defines default NetOutgoing resource policy. It permits any user to make outgoing connections to any host to access any remote service.

osseal-default-sudo
This ACL defines default Sudo resource policy. It permits any user to execute any Sudo command

osseal-default-surrogate
This ACL defines default Surrogate resource policy. It permits anybody to surrogate to any user or group.

osseal-exec-open
This ACL controls access to the /opt/pdos/lib and /opt/pdos/nls directories and the non-administrative commands in the /opt/pdos/bin directory: pdosdestroy, pdosrefresh, pdossudo, and pdoswhoami. This ACL permits any user access to the non-administrative commands and to the Tivoli Policy Director for Operating Systems shared libraries used by these commands, along with the message catalogs.

osseal-hla
This ACL controls access the IP address to hostname cache maintained by Tivoli Policy Director for Operating Systems in the /var/pdos/hla directory. It permits administration of the cache by members of the osseal-admin group using the pdoshla command

osseal-logs
This ACL controls access to log files generated by the Tivoli Policy Director for Operating Systems daemons and commands in the /var/pdos/log directory. It restricts access to the directory to members of the osseal-admin group and prohibits Change Ownership (o), Change Permission (p) and Update Timestamp (U) actions, even to members of this group.

osseal-open
This ACL controls access to the /opt/pdos/etc/lpm.conf and /opt/pdos/etc/pdossudo.conf files. It permits any user to read the files, but not to modify them. Members of the osseal-admin group are granted full access to resources protected by this ACL.

osseal-privileged-user
This ACL controls the ability to surrogate to the osseal UNIX user. Access is restricted to members of the osseal-admin group although any user can also surrogate to osseal using the pdossudo command. This is necessary because the pdossudo command must perform a surrogate operation to the osseal user so that the correct authorization decision can be made.
when a user attempts to execute a Sudo command. Disabling the `pdossudo` command’s ability to surrogate to the osseal user also disables the function of the Sudo command.

**osseal-restricted**

This ACL protects the more sensitive information associated with Tivoli Policy Director for Operating Systems. It grants full access to members of the osseal-admin group and denies all access to non-members. It is attached to the `/opt/pdos/etc` and `/var/pdos/pdosbkip` directories.

**Note:** The `pdossudo.conf` file in the `/opt/pdos/etc` directory has the `osseal-open` ACL directly attached and is, by default, less restricted.

**osseal-restricted-read**

This very restrictive ACL controls the ability to start and stop the Tivoli Policy Director for Operating Systems daemons and to execute the administrative commands. It only grants Change Directory (D), Read (r), List Directory (l), Kill (k), and Execute (x) permission to members of the osseal-admin group and denies non-members any access at all. It protects all the directories under both `/var/pdos` and `/opt/pdos` that maintain runtime state that do not require administrative action.

**osseal-tcb**

This ACL controls access to the Trusted Computing Base object signature database maintained by Tivoli Policy Director for Operating Systems in `/var/pdos/tcb`. This ACL restricts access to this directory to members of the osseal-admin group. They can only access resources contained by this directory by using the `pdosobjsig` command.

**osseal-umsg**

This ACL restricts access to the `/var/pdos/umsg` directory that is involved with communication between the various Tivoli Policy Director for Operating Systems components. Access is allowed only when using a Tivoli Policy Director for Operating Systems command that requires access to this directory.

**osseal-var-lpm**

This ACL controls access to the `/var/pdos/lpm` directory. It permits any user read and write access to the files underneath the `/var/pdos/lpm` directory. This access is necessary to ensure that the Login Activity Policy enforcement code can function properly. Members of the osseal-admin group and the root user are granted full access to resources protected by this ACL.

**Isolated Operation**

During normal operation, Tivoli Policy Director for Operating Systems relies on the network to communicate with the Tivoli Policy Director management server, the Tivoli Policy Director user registry (LDAP), and, in some cases a non-local UNIX User Registry such as NIS, and a non-local host name database such as DNS server. Tivoli Policy Director for Operating Systems can continue to function in an environment in which it becomes isolated from one or more of these servers, registries, or the network itself. Isolation means the loss of ability to communicate. This loss can occur for various reasons:

- The network itself might be down in which case Tivoli Policy Director for Operating Systems is isolated from everything
- The Tivoli Policy Director management server might be down
- The Tivoli Policy Director user registry (LDAP) might be down
The NIS server may be down
The DNS server might be down

The following sections discuss each type of isolation and how they affect Tivoli Policy Director for Operating Systems.

**Isolation from the Tivoli Policy Director Management Server**

If Tivoli Policy Director for Operating Systems becomes isolated from the Tivoli Policy Director management server, the PDOSD daemon is unable to receive updates to the policy database. Any updates made to the policy on the master policy database will not be propagated to Tivoli Policy Director for Operating Systems until communication between Tivoli Policy Director for Operating Systems and the Tivoli Policy Director management server is re-established. See "Authorization Decision Process" on page 53 for a description of the PDOSD daemon’s interaction with the Tivoli Policy Director management server. During normal operation of the PDOSD daemon, all policy decisions are made using the local replica of the policy database in combination with the TCB. During the time that the PDOSD daemon is isolated from the Tivoli Policy Director management server, all policy decisions will continue to be made by using the local replica of the policy database. Once the PDOSD daemon has re-established communication with the Tivoli Policy Director management server, any pending updates to the policy database are received through the specified means, active notification or polling.

**Isolation from the Tivoli Policy Director User Registry**

If Tivoli Policy Director for Operating Systems becomes isolated from the Tivoli Policy Director User Registry (LDAP), the PDOSD daemon is unable to obtain new Tivoli Policy Director credentials. This means that the PDOSD daemon is unable to obtain new credentials for users as they log into the system and it is unable to refresh cached credentials. See "Credential Acquisition" on page 50 for a description of how credentials are managed by the PDOSD daemon in normal operation.

When the PDOSD daemon detects that it has become isolated from the LDAP user registry, it does not remove any credentials from the cache even if they are overdue for a refresh or have exhausted their hold interval. This lets any user who is currently logged in to the system to continue to function normally using their cached credential.

Any user with a cached credential can log in to the system while the PDOSD daemon is isolated from the LDAP user registry and will use their cached credential. If a user who doesn’t have a cached credential logs in while the PDOSD daemon is isolated from the LDAP user registry, that user will run as an unauthenticated user.

Administrative users always have a cached credential. If an Administrative user logs in while the PDOSD daemon is isolated from the LDAP user registry, that administrator always has a cached credential to use.

When the PDOSD daemon is once again able to communicate with the LDAP user registry, it refreshes any credentials that should have been refreshed during the time of isolation from the LDAP user registry.

The Tivoli Policy Director per user time-of-day login restrictions are also stored in the LDAP User Registry. The Time of Day Login Restrictions are retrieved by the PDOSD daemon when a user logs in and are cached along with the credentials. When the PDOSD daemon is isolated from the LDAP User Registry it uses the cached Time of Day Login Restrictions.
Isolation from Non-local UNIX User Registry

Systems using a non-local UNIX user registry such as NIS, might become isolated from that user registry. When this happens, users might not be able to login to the system. Users who are logged in should be able to retrieve new Tivoli Policy Director credentials or use existing cached Tivoli Policy Director credentials.

The user’s native numerical UNIX ID is converted to the user’s UNIX name using standard UNIX operating system functions that communicate with the non-local UNIX user NIS or NIS+ registry. The UNIX Identity and Its Relationship to the Tivoli Policy Director User Identity on page 3 explains how Tivoli Policy Director credentials are obtained.

If the Tivoli Policy Director for Operating Systems system becomes isolated from its user registry this conversion will not succeed. Tivoli Policy Director for Operating Systems includes a UNIX uid/gid to username/groupname Cache which can be enabled when Tivoli Policy Director for Operating Systems is configured. When the UNIX uid/gid to username/groupname Cache is enabled and the PDOSD daemon becomes isolated from its UNIX user registry, the PDOSD daemon uses this cache to map the UNIX ID to the UNIX name. After the UNIX name is known, the PDOSD daemon can retrieve the credential from the Tivoli Policy Director User Registry (LDAP) or the credential cache.

This cache is only ever used as a backup and is only needed when users log in or perform Surrogate operations.

By default, the UNIX uid/gid to UNIX username/groupname Cache is not enabled because the remote UNIX registry service is likely to provide its own mechanism for caching this information. If the remote UNIX registry service you are using does not provide such a caching feature you can enable the Tivoli Policy Director for Operating Systems uid/gid cache by entering:

```
pdoscfg -uid on
```

See the Tivoli Policy Director for Operating Systems Installation Guide for details on configuring Tivoli Policy Director for Operating Systems.

Isolation from the Host Name Resolution Server

Tivoli Policy Director for Operating Systems can become isolated from a remote host name resolution server such as DNS or NIS. If this happens, Tivoli Policy Director for Operating Systems might be isolated from the Tivoli Policy Director management server, the Tivoli Policy Director User Registry, and in some cases a non-local UNIX User Registry. The sections above describe the behavior of Tivoli Policy Director for Operating Systems in each of these cases.

Isolation from the host name resolution server can cause additional problems. Tivoli Policy Director for Operating Systems Network policy may be specified by using either an IP address or a DNS hostname. The PDOSD daemon needs to be able to convert the IP address to a DNS hostname when making policy decisions for network resources identified by host name. Tivoli Policy Director for Operating Systems includes an IP Address to Hostname Cache to allow the PDOSD daemon to continue to do this conversion even when isolated from a remote hostname resolution server.

By default, the IP Address to DNS Hostname Cache is enabled. Use the `pdoshla` command to manage the IP Address to DNS Hostname Cache. You can use this command to pre-populate entries in the cache. If your operating system provides a local IP Address to DNS Hostname Cache, you might want to disable this feature. Enter

```
pdoscfg -dns off
```

3. Runtime
to disable this feature or set the **dns** attribute of the [cache] stanza in the 
/opt/pdos/etc/osseal.conf configuration file set to **off**. See the *Tivoli Policy Director for Operating Systems Installation Guide* for details on configuring Tivoli Policy Director for Operating Systems.

The Tivoli Policy Director for Operating Systems IP Address to Hostname Cache is always consulted first before querying a remote hostname resolution service. This is done to ensure that the authorization of network accesses is performed efficiently. Because it is queried first, stale information might be used. Tivoli Policy Director for Operating Systems caches IP address to host name mapping for 6 hours after which the cache entry is refreshed on the next lookup. If you need to make sure that a host’s IP address change is reflected immediately, use the `pdoshla` command to immediately remove stale entries from the cache.
This chapter explains the administrative tasks required to manage the Tivoli Policy Director for Operating Systems runtime and illustrates performing those tasks using the command line. It describes:

- Establishing a consistent username space to ensure that the appropriate mapping exists between the native username space and the Tivoli Policy Director User Registry
- Ongoing administration of Tivoli Policy Director for Operating Systems including managing its processes, the Trusted Computing Base (TCB), the credentials cache, and the hostname look-aside database
- Monitoring the effect of authorization policy on a system, and backing up and restoring the Tivoli Policy Director for Operating Systems configuration and database files

This chapter provides an overview of the administrative tasks. See Chapter 7, “Commands” on page 147 for detailed information about each command. Tivoli Policy Director for Operating Systems administrative tasks also can be performed from the Tivoli desktop. See Chapter 5, “Tasks Available from Tivoli Desktop” on page 89 for details.

Administering Tivoli Policy Director for Operating Systems consists of the following tasks:

- “Defining Runtime Administrators and Auditors”
- “Establishing a Consistent Username Space” on page 72
- “Tuning the Configuration” on page 74
- “Managing Tivoli Policy Director for Operating Systems Processes” on page 75
- “Verifying Policy” on page 77
- “Managing the Trusted Computing Base” on page 80
- “Managing Login Activity Policy” on page 81
- “Managing Credentials” on page 84
- “Determining the Accessor Identity” on page 85
- “The Hostname Look-aside Database” on page 86
- “Backing Up and Restoring Configuration Files and Databases” on page 87

### Defining Runtime Administrators and Auditors

A Tivoli Policy Director for Operating Systems runtime administrator is authorized to perform administrative tasks to manage the Tivoli Policy Director for Operating Systems runtime environment. To be a runtime administrator, you must be a member of both of the following groups.
- osseal-admin group in the Tivoli Policy Director user registry
- osseal group in UNIX

A Tivoli Policy Director for Operating Systems auditor is authorized to perform audit-related tasks in Tivoli Policy Director for Operating Systems. To be an auditor, you must be a member of both of the following groups.

- osseal-auditors group in the Tivoli Policy Director user registry
- ossaudit group in UNIX

Auditors are authorized to run the `pdosaudview` command and access the files in the `/var/pdos/audit` and `/var/pdos/tec` directories.

It is recommended that all runtime administrators be made auditors as well.

### Establishing a Consistent Username Space

When setting up a Tivoli Policy Director for Operating Systems environment, you need to understand the relationship between a system’s native user registry and the Tivoli Policy Director User Registry. For Tivoli Policy Director for Operating Systems, the Tivoli Policy Director User Registry has to be an LDAP based user registry.

When acquiring the credentials needed to make authorization decisions, Tivoli Policy Director for Operating Systems maps a native user ID to a Tivoli Policy Director user. The user’s native username is obtained from the system’s native User Registry using this numerical ID. The native username is mapped directly to a Tivoli Policy Director user of the same name. The Tivoli Policy Director user defines the primary user information and group membership. This identity is used in Tivoli Policy Director for Operating Systems authorization decisions.

**Note:** The group membership in the native user definition is not used in Tivoli Policy Director for Operating Systems decisions.

If there is no Tivoli Policy Director user corresponding to the user’s native username, then the user is treated as unauthenticated when making authorization decisions. Because of this relationship, all systems sharing the same Tivoli Policy Director User Registry should use a consistent and distinct native username for each user in the environment. The UNIX Identity and Its Relationship to the Tivoli Policy Director User Identity” on page 3 gives an example of this relationship. The `pdosrgyimp` command assists in the task of populating the Policy Director User Registry. This task requires careful planning.

### Identifying Users and Groups

Consider how you will define groups. Aligning groups with job functions, projects, or roles is useful for establishing ACLs using group entries instead of individual user entries. This helps simplify policy definition and management. It also aids in efficient evaluation of policy by Tivoli Policy Director for Operating Systems.

First, identify which UNIX users and groups should be included in the Tivoli Policy Director User Registry. This step depends on the policy decisions you make for a particular environment. For instance, you might set up the policy in such a way that objects are protected through access controls that restrict or allow access based on a few specific user credentials and unauthenticated credentials for most other users. In this case, only the specific users of interest need to have Tivoli Policy Director entries. All other users can run with unauthenticated credentials.
Or, you might set up a more selective policy to restrict access to specific users and groups. In this case, most, if not all, users need to have Tivoli Policy Director entries.

**Identifying Duplicate User Names**

Do the following steps to set up the registry:

1. Look at all of the machines that will belong to a Tivoli Policy Director domain.
2. Identify duplicate user or group entries across multiple machines.
3. Resolve any duplicate entries. The duplicates might represent the same person or group.

For example: user maggie on machine A might represent the person Maggie Smith and user maggie on machine B might also represent the person Maggie Smith. Because user maggie represents the same person, one Tivoli Policy Director entry could cover both maggies. In other cases, the duplicates represent different users or groups. For example: user riley on machine A represents the person Riley Smith and user riley on machine B represents the person Riley Jones. Because the user riley represents two different people, two Tivoli Policy Director entries are needed. "The UNIX Identity and Its Relationship to the Tivoli Policy Director User Identity" on page 3 shows another example of duplication. To resolve this duplication, the UNIX name of one of the users must be changed.

**Using pdsosrgyimp**

After you have identified the UNIX users and groups to be imported, use the `pdsosrgyimp` command on each machine that has UNIX registry users and groups to be imported. See "pdsosrgyimp" on page 175 for a description of the `pdsosrgyimp` command. The `pdsosrgyimp` command creates user entries for all UNIX users and groups found in the UNIX registry. Any newly created groups are also populated with the user entries corresponding to the members of the UNIX group. The syntax is as follows:

```
pdosrgyimp -S o=tivoli -l sec_master
```

If almost all of UNIX users or groups are to be imported, you can create an exclude file with a list of the users and groups to exclude. In this case, all UNIX users and groups found in the UNIX registry are imported except those listed in the exclude file. The syntax is as follows:

```
pdosrgyimp -S o=tivoli -l sec_master -E excludefilename
```

If only a few UNIX users or groups are to be imported, you can create an include file with a list of the users and groups to include. In this case only the UNIX users and groups listed in the include file are imported. The syntax is as follows:

```
pdosrgyimp -S o=tivoli -l sec_master -I includelfilename
```

Use the `-u` or `-g` options to import UNIX users and groups separately. Take care when importing groups separately from users. When groups are populated, an attempt is made to add all non-excluded users to the group. In this case you can specify both the include and exclude files. List the group in the include file. List the users that are to be left out of the group in the exclude file. The syntax is as follows:

```
pdosrgyimp -S o=tivoli -l sec_master -I includelfilename -E excludefilename
```

The `pdsosrgyimp` command creates two files. The file `pdsosrgyimp.import` contains a list of `pdadmin` commands that were successfully executed. The file `pdsosrgyimp.conflict` contains a list of `pdadmin` commands that failed.

Most failures occur because an entry already exists or because the Policy Director server is down. The `pdsosrgyimp.conflict` file can be used to aid in conflict resolution. Instead of
running the **pdosrgyimp** command again, modify the text in the pdosrgyimp.conflict file. Then pipe it directly to the **pdadmin** command:

```
pdadmin -a sec_master -p password < pdosrgyimp.conflict
```

The `-n` option specifies that **pdosrgyimp** should generate a list of **pdadmin** commands without actually executing them. Use this option to test what actions would be taken before you do the import. You can use the `-n` option with any of the **pdosrgyimp** examples listed above. The list of **pdadmin** commands is saved in the pdosrgyimp.import file.

## Tuning the Configuration

Use the configuration command **pdoscfg** to reconfigure certain Tivoli Policy Director for Operating Systems configuration parameters after the initial configuration. Changes made using **pdoscfg** take effect the next time Tivoli Policy Director for Operating Systems is stopped and restarted. You can enable or disable autostart, global warning, the use of a hostname look-aside and ID to name mapping. You can tune credentials cache management and monitor the Trusted Computing Base. You can also modify how the Tivoli Policy Director for Operating Systems daemons handle the log files. The global audit level can be set. You can refresh the certificate of the LDAP server’s Certification Authority if necessary.

You can also use the **pdoscfg** command to delete parameters from the configuration files so that the daemons use default values on the next restart. You cannot change the policy branch name and the suffix. To change these parameters, you must first use the **pdosucfg** command to unconfigure Tivoli Policy Director for Operating Systems and then configure it again. *“pdoscfg” on page 153* lists all the **pdoscfg** options.

Tivoli Policy Director for Operating Systems configuration information is kept in a set of configuration files, one for each daemon. The files are named `daemon_name.conf`. Another file, containing common configuration data is named `osseal.conf`. The configuration files have stanzas containing sets of `attribute=value` pairs. Table 35 and the following tables show which files contain which stanzas, and how the stanza attributes map to the pdoscfg command line options.

### Table 35. Attribute Equivalents of pdoscfg Options in osseal.conf

<table>
<thead>
<tr>
<th>Stanza</th>
<th>Attribute</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>[audit]</td>
<td>level</td>
<td>–audit_level</td>
</tr>
<tr>
<td>[authorization]</td>
<td>warning</td>
<td>–warning</td>
</tr>
<tr>
<td>[cache]</td>
<td>dns</td>
<td>–dns</td>
</tr>
<tr>
<td></td>
<td>uid</td>
<td>–uid</td>
</tr>
<tr>
<td>[policy]</td>
<td>branch</td>
<td>–branch</td>
</tr>
</tbody>
</table>

### Table 36. Attribute Equivalents of pdoscfg Options for pdosd.conf

<table>
<thead>
<tr>
<th>Stanza</th>
<th>Attribute</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ldap]</td>
<td>ssl-certificate</td>
<td>–ldap_ssl_cacert</td>
</tr>
<tr>
<td>[pdosd]</td>
<td>kmsg-handler-threads</td>
<td>–kmsg_hnd_threads</td>
</tr>
<tr>
<td></td>
<td>log-entries</td>
<td>–pdosd_log_entries</td>
</tr>
<tr>
<td></td>
<td>logs</td>
<td>–pdosd_logs</td>
</tr>
<tr>
<td>[credentials]</td>
<td>admin-cred-refresh</td>
<td>–admin_cred_refresh</td>
</tr>
<tr>
<td></td>
<td>cred-hold</td>
<td>–cred_hold</td>
</tr>
<tr>
<td></td>
<td>user-cred-refresh</td>
<td>–user_cred_refresh</td>
</tr>
</tbody>
</table>

**Establishing a Consistent Username Space**
Table 36. Attribute Equivalents of `pdoscfg` Options for pdosd.conf (continued)

<table>
<thead>
<tr>
<th>Stanza</th>
<th>Attribute</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>[policy]</td>
<td>refresh-interval</td>
<td>–refresh_interval</td>
</tr>
<tr>
<td>[ssl]</td>
<td>ssl-listening-port</td>
<td>–ssl_listening_port</td>
</tr>
<tr>
<td>[tcb]</td>
<td>interval</td>
<td>–tcb_interval</td>
</tr>
<tr>
<td></td>
<td>max-checksum-file-size</td>
<td>–tcb_max_file_size</td>
</tr>
<tr>
<td></td>
<td>monitor-threads</td>
<td>–tcb_monitor_threads</td>
</tr>
</tbody>
</table>

Table 37. Attribute Equivalents of `pdoscfg` Options in pdosauditd.conf

<table>
<thead>
<tr>
<th>Stanza</th>
<th>Attribute</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>[pdosaudid]</td>
<td>log-entries</td>
<td>–audit_log_entries</td>
</tr>
<tr>
<td></td>
<td>audit-logflush</td>
<td>–audit_logflush</td>
</tr>
<tr>
<td></td>
<td>logs</td>
<td>–audit_logs</td>
</tr>
<tr>
<td></td>
<td>audit-logsize</td>
<td>–audit_log_size</td>
</tr>
</tbody>
</table>

Table 38. Attribute Equivalents of `pdoscfg` Options in pdoswdd.conf

<table>
<thead>
<tr>
<th>Stanza</th>
<th>Attribute</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>[pdoswdd]</td>
<td>log-entries</td>
<td>–pdoswdd_log_entries</td>
</tr>
<tr>
<td></td>
<td>logs</td>
<td>–pdoswdd_logs</td>
</tr>
</tbody>
</table>

You can use both the `pdoscfg` and `pdosctl` commands for some configuration actions. The `pdoscfg` command is used to modify the configuration files. These modifications do not take effect until the next time Tivoli Policy Director for Operating Systems is stopped and restarted.

The `pdosctl` command dynamically changes Tivoli Policy Director for Operating Systems while it is running. The changes take effect immediately and are not persistent when you restart. The following sections show both the `pdoscfg` options and the `pdosctl` options where appropriate.

Managing Tivoli Policy Director for Operating Systems Processes

This section tells how to start, stop, and monitor Tivoli Policy Director for Operating Systems processes.

Starting Tivoli Policy Director for Operating Systems

Tivoli Policy Director for Operating Systems can be started manually from the command line or automatically at system boot time. You should start Tivoli Policy Director for Operating Systems automatically at system boot time to ensure proper enforcement of authorization policy. To have Tivoli Policy Director for Operating Systems start automatically at boot time, enter:

`pdoscfg –autostart on`

When the system reboots, Tivoli Policy Director for Operating Systems starts automatically.

To disable automatic startup at boot time, enter:

`pdoscfg –autostart off`
When the system reboots, Tivoli Policy Director for Operating Systems will not start automatically.

To start Tivoli Policy Director for Operating Systems from the command line, enter:

```
rc.osseal start
```

**Note:** If this is the first time that Tivoli Policy Director for Operating Systems is being started after a system reboot, this command must be run as root to ensure that the kernel extension gets loaded correctly.

By default, Tivoli Policy Director for Operating Systems is configured to start automatically at system boot time when it is initially configured on a system. You can override the automatic start on the `pdoscfg` command line by specifying `--autostart off` during initial configuration.

### Stopping Tivoli Policy Director for Operating Systems

You can stop Tivoli Policy Director for Operating Systems from the command line. To stop all the Tivoli Policy Director for Operating Systems processes and deactivate the kernel extension, enter:

```
rc.osseal stop
```

You can also use the `pdosctl` command to stop selected daemons. For example, you might want to stop the PDOSAUDITD daemon and restart it with a different logging parameter. To stop daemons with `pdosctl`, use the `-k` option and specify the daemon name. For example, to stop the PDOSAUDITD daemon, enter:

```
pdosctl -k pdosauditd
```

The output is: `pdosauditd shutdown`. Use the command `rc.osseal start` to restart the daemon.

### Checking Daemon Status

Use the `pdosctl` command to check whether the PDOSD, PDOSAUDIT, and PDOSWDD daemons are running. The `-s` option, when specified with no arguments, displays the status of each of the daemons. Use the `-s` option followed by a daemon name to display the status of a single daemon. You can use the `-s` option multiple times on a single command line.

You can use the `-q` option with the `-s` option. The `-q` option suppresses the messages generated by the `-s` option and sets the return code to 0 on success and 1 if any of the queried daemons are down. The `-q` option makes it simpler to use `pdosctl` in a shell script.

Enter:

```
pdosctl -s
```

The output is:

- `pdosd is running normally`
- `pdoswdd is running normally`
- `pdosauditd is running normally`

If the PDOSD daemon is running in isolation mode, the output is:

- `pdosd is running under abnormal conditions`
- `isolated from the user registry`
- `pdoswdd is running normally`
- `pdosauditd is running normally`

**Note:** The `pdosctl` command does not affect the PDOSTECD daemon.
Daemon Log Files

Each Tivoli Policy Director for Operating Systems daemon maintains a log file that records significant events and error conditions. The records written to the log files contain a UTC timestamp, information identifying the Tivoli Policy Director for Operating Systems code logging the message, the message classification, and the message text. The message classification indicates the severity of the message and is NOTIFY, WARNING, ERROR, or FATAL. These log files are in the directory /var/pdos/log and are named pdos_daemon_name.log. The log files can be useful for diagnostic purposes.

Use the pdoscfg command to tune how the daemons handle the log files. For the supported daemon, either PDOSD, PDOSAUDIT, or PDOSWDD, you can specify the number of entries that can be written to the log file before the log file automatically rolls over to a new file. You can also specify the number of log files to be written before recycling the first file. The default configuration is to never roll over the log files.

Table 39. pdoscfg Options that Control the Daemon Log Files

<table>
<thead>
<tr>
<th>Log File</th>
<th>Options that control the Log File</th>
</tr>
</thead>
<tbody>
<tr>
<td>pdosd</td>
<td>--pdosd_log_entries, --pdosd_logs</td>
</tr>
<tr>
<td>pdoswdd</td>
<td>--pdoswdd_log_entries, --pdoswdd_logs</td>
</tr>
<tr>
<td>pdosauditd</td>
<td>--audit_log_entries, --audit_logs</td>
</tr>
</tbody>
</table>

Note: The PDOSTECD daemon maintains its log file in a separate directory and the pdoscfg command can not be used to adjust its logging configuration.

Verifying Policy

You should verify that the policies you set are effective, and verify policy whenever you change a policy. You can use either warning mode or audit mode to verify policy.

Using Warning Mode to Verify Policy

You can check the effects of authorization policy on a system without enabling enforcement of the policy by enabling warning mode. If warning mode is enabled, an audit record is generated for accesses to resources that would normally be denied due to policy but are granted because of warning mode. View the audit log to determine if the current authorization policy is having the desired effect. You can enable warning mode globally for all policy or for specific protected resources.

Note: If you enable global warning, you have no enforcement in effect. Make sure you enable enforcement again, when required.

Enabling, Disabling, and Querying Global Warning Mode

To enable global warning mode immediately, enter:

    pdosctl –w on

To disable global warning mode immediately, enter:

    pdosctl –w off

To enable global warning mode to take effect the next time Tivoli Policy Director for Operating Systems is restarted, enter:

    pdoscfg –warning on
To disable global warning mode to take effect at the next restart of PDOS, enter:

```
pdoscfg –warning off
```

To query the current global warning mode setting, specify the `–w` with no arguments:

```
pdosctl –w
```

The output is:

```
The global warning mode setting is off
```

**Enabling, Disabling, and Querying Resource Warning Mode**

To enable warning mode for a specific resource, set up a Protected Object Policy (POP) with warning mode enabled and attach it to the protected resource. Access to a protected object that would normally be denied by access controls, is granted if a POP is attached or if inherited with warning mode enabled. An audit record is generated regardless of the audit level setting in the POP or the global audit level. Warning mode is disabled by default.

For example, to enable warning mode for accesses to the protected object name `/OSSEAL/Default/NetIncoming/TCP/telnet/*.company.com`, enter:

```
pdadmin> pop create sample_pop
pdadmin> pop modify sample_pop set warning yes
pdadmin> pop attach /OSSEAL/Default/NetIncoming/TCP/telnet/*.company.com
```

Netincoming accesses using telnet from systems with hostnames that match the pattern `*.company.com` that would normally be denied are now permitted. An audit record is generated that shows that access was permitted due to resource warning mode. To disable warning mode, set the warning attribute to `no` or detach the POP from the protected object name. If you are using other attributes in the POP for the object and you want to disable only warning mode leaving the other attributes intact, set warning mode to `off`:

```
pdadmin> pop modify sample_pop set warning no
```

Warning mode is now disabled.

If you are using this POP only for warning mode or it is also controlling other protected objects for which you still want warning mode enabled, detach the POP from the protected object to disable warning mode for just that object:

```
pdadmin> pop detach /OSSEAL/Default/NetIncoming/TCP/telnet/*.company.com
```

To query the warning mode setting in a POP, enter:

```
pdadmin> pop show pop_name
```

**Using Auditing to Verify Policy**

Use the auditing tools to monitor the effects of authorization policy on a system. You must be defined as a Tivoli Policy Director for Operating Systems auditor to use the auditing tools. See "Defining Runtime Administrators and Auditors" on page 71 for details.

Auditing can be set globally or for a specific protected resource. 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. See Chapter 6, "Auditing" on page 131 for more information about auditing.

Use the `pdosaudview` command to see the results of auditing. See "pdosaudview” on page 148 for a description of the `pdosaudview` command.

**Setting and Querying the Global Audit Level**

To set the global audit level that goes into effect the next restart of Tivoli Policy Director for Operating Systems, enter:

```
pdoscfg –audit_level level
```

```
Verifying Policy
```
You can use the **pdosctl** command to set or reset the global audit level during runtime.

The **-A** option resets the current global audit level to the specified value. If multiple **-A** options are specified on a single command line, the global audit level is set to all the specified values. The **-a** option modifies the global audit level by resetting just the specified audit level. Multiple **-a** options can be specified on a single command line. To reset or modify the global audit level, the **-a** and **-A** options must be followed by an audit level and the keyword **on** or **off** separated by a colon (:). Valid values for audit level are: all, none, permit, deny, loginpermit, logindeny, admin, verbose, info, trace_exec, and trace_file. To reset the current global auditing to specific levels immediately, enter:

```
pdosctl -A level:[on | off]
```

To turn on additional global audit levels, enter:

```
pdosctl -a level:[on | off]
```

To set the global audit level to permit and deny, enter:

```
pdosctl -A permit:on -A deny:on
```

To add the admin audit level to the global audit level, enter:

```
pdosctl -a admin:on
```

Any audit levels currently enabled are still enabled. The **-a** and **-A** options when specified with no arguments display the current global audit level of the PDOSD, PDOSAUDITD, and PDOSWDD daemons.

To query the global audit level, enter:

```
pdosctl -a
```

The output is:

```
pdosd has the following audit levels on: permit, deny, admin
pdoswdd has the following audit levels on: permit, deny, admin
pdosauditd has the following audit levels on: permit, deny, admin
```

### Setting and Querying the Resource Audit Level

To set the audit level for a specific resource, set up a POP with the audit level set to the desired level and attach it to the protected object name. The audit level specified controls under what circumstances an access to an object generates an audit record. The audit level can be set to one of the following values:

- permit
- deny
- admin
- all
- none

The default is to not have an audit level set. For example, to set an audit level of permit and deny for accesses to the protected object name `/OSSEAL/Default/NetIncoming/TCP/telnet/*.company.com` using the POP sample_pop:

```
padmin> pop modify sample_pop set audit-level permit,deny
padmin> pop attach /OSSEAL/Default/NetIncoming/TCP/telnet/*.company.com
```

An audit record is generated for all netincoming accesses using telnet from systems with hostnames that match the pattern `*.company.com`. The audit record indicates whether the access was permitted or denied. To prevent generating audit records, set the audit level attribute to `none` or detach the POP from the protected object name. If you are using other...
attributes in the POP for the object and you only want to turn off the audit-level, leaving the other attributes intact, set the audit level to none:

```
padmin> pop modify sample_pop set audit-level none
```

If you are using this POP only for resource auditing or if it is also controlling other protected objects that you still want to audit, detach the POP from the protected object to disable warning mode for just that object:

```
padmin> pop detach /OSSEAL/Default/NetIncoming/TCP/telnet/*.company.com
```

To query the audit level setting in a POP, enter:

```
padmin> pop show pop_name
```

**Testing Programs in an Unauthenticated Environment**

Because administrative users usually have Tivoli Policy Director for Operating Systems credentials, it is difficult to test policy affecting users and environments that do not have Tivoli Policy Director for Operating Systems credentials. The `pdosunauth` command spawns a shell that is treated as unauthenticated. See `pdosunauth` on page 190 for information about the `pdosunauth` command. You can use this shell to verify policy affecting unauthenticated users and environments. If an optional command is specified, the spawned shell executes only the specified command. The following sequence is an example of `pdosunauth` usage:

1. Run the following command as root:
   ```
   pdoswhoami -a
   ```
   The output is
   0 root

2. Run the `pdosunauth` command to spawn a shell that will be treated as unauthenticated for Tivoli Policy Director for Operating Systems authentication decisions:
   ```
   pdosunauth
   ```

3. Run the `pdoswhoami` command again:
   ```
   pdoswhoami -a
   ```
   The output is
   Unauthenticated

Any other commands executed in this shell are treated as unauthenticated for the purposes of Tivoli Policy Director for Operating Systems authorization decisions. This allows the root user verify that the policy permits and denies access for unauthenticated users in the expected manner.

**Note:** Use the `pdosunauth` command sparingly. Do not give access to it to many users.

**Managing the Trusted Computing Base**

The set of files comprising a system’s Trusted Computing Base (TCB) is defined under the policy branch that system subscribes to. The trust states and signatures of TCB files are maintained on a per-machine basis in the Object Signature Database. The PDOSD daemon monitors the files in the TCB for changes to a file’s signature. If the PDOSD daemon detects that the signature has changed, the file is marked untrusted in the Object Signature Database. Authorization requests to execute an untrusted TCB file are denied.

When a file’s state is set to untrusted in the Object Signature Database, it remains untrusted until explicit administrative action is taken to retrust that file. You must retrust a TCB file after an updated version of the file has been installed on the system.
Tuning the PDOSD Daemon’s TCB Monitoring

The `pdoscfg` command has options for tuning TCB monitoring. The `tcb_interval` parameter is the interval in minutes which the entire TCB should be scanned for changes. Increasing this interval reduces the load of the TCB monitoring system but increases the time before a change is detected.

The `tcb_max_file_size` parameter is the maximum number of bytes considered significant in the calculation of a file’s checksum.

The `tcb_monitor_threads` parameter is the number of threads dedicated to monitoring the files.

The `tcb_ignore_ctime` parameter causes the ctime to be ignored when performing TCB signature comparisons. When this option is enabled, a change in ctime does not cause the TCB resource to become untrusted.

The `tcb_nocrc_on_exec` parameter causes the CRC check that normally occurs as part of the authorization check associated with running an executable file to be skipped. Enabling this option avoids performing the CRC check on large binary files.

The values for these parameters are stored in the `/opt/pdos/etc/pdosd.conf` file in the `[tcb] stanza when Tivoli Policy Director for Operating Systems is initially configured. You can use the `pdoscfg` command to change the parameters. The changes take effect the next time Tivoli Policy Director for Operating Systems is stopped and restarted on the system. See “pdoscfg” on page 153 for more information about the `pdoscfg` command parameters.

Managing the Object Signature Database

Use the `pdosobjsig` command to check and modify the current trust state of TCB files in the Object Signature Database. The `pdosobjsig` command can list all files, all trusted files, or all untrusted files in the database. The `-l` parameter determines which files to check or modify.

Use the `-g` option to display the state of a specific file.

The `pdosobjsig` command can also modify the current trust state of a TCB file. Use both `-u` and `-s` together, or the `-S` option alone to modify the state. The `-u` parameter sets the state of a specific file to trusted or untrusted. The `-S` parameter sets the state of all files to either trusted or untrusted. For example, you install a new application `/usr/local/app/bin/applicationA`. You want applicationA to be part of the TCB:

1. Enter:
   ```bash
   pdadmin> object create \n   /OSSEAL/<policy-branch>/TCB/Secure-Program/usr/local/app/bin/applicationA
   ```
2. Set the state to trusted:
   ```bash
   pdosobjsig -u /usr/local/app/bin/applicationA -s trusted
   ```
3. In the future, you install an updated version of applicationA. If you take no action, the Tivoli Policy Director for Operating Systems TCB monitor detects that the signature has changed and sets the state to untrusted. No one can run this application. To avoid this, explicitly retrust the updated applicationA:
   ```bash
   pdosobjsig -u /usr/local/app/bin/ApplicationA -s trusted
   ```

Managing Login Activity Policy

The Tivoli Policy Director for Operating Systems Login Activity Policy is enforced on a per-machine basis based on the activity of an account that is defined on the machine. The `pdoslpadm` command is used to view and manage the login activity policy.
Viewing Account Records

As part of the login activity policy, a local database maintains records for all users that have logged in since login activity policy was activated. These records can be view using the -r option of the `pdoslpadm` command. To see all the records that are currently in the database, specify the -r option with no operand.

```
# pdoslpadm -r
```

<table>
<thead>
<tr>
<th>User (uid)</th>
<th>State: Time Locked</th>
</tr>
</thead>
<tbody>
<tr>
<td>gbland(1114)</td>
<td>Unlocked</td>
</tr>
<tr>
<td>root(0)</td>
<td>Unlocked</td>
</tr>
<tr>
<td>uduck(1118)</td>
<td>Unlocked</td>
</tr>
</tbody>
</table>

Detailed information about an account can be displayed by using the -f option. To see details about the `gbland` and `uduck` user IDs:

```
# pdoslpadm -r -f gbland uduck
```

```
--------------------------------------------------
Account state for gbland, id 1114:
  Lock status: Unlocked
  Last successful login: Sun 02 Dec 2001 05:53:01 PM CST
  Current grace logins: 0
  Password change date: Thu 08 Nov 2001 12:00:00 AM CST
  Login failure data:
    Concurrent logins(allowed): 0(0)
--------------------------------------------------
--------------------------------------------------
Account state for uduck, id 1118:
  Lock status: Unlocked
  Last successful login: Sun 02 Dec 2001 03:09:25 PM CST
  Current grace logins: 0
  Password change date: Thu 04 Oct 2001 12:00:00 AM CDT
  Login failure data:
    Failure record 1:
      TTY name: /dev/pts/4
      rhost name: bigserv.mycomp.com
      ruser name:
      Failing pid: 657 (login)
      Failure time: Sun 02 Dec 2001 03:04:22 PM CST
    Concurrent logins(allowed): 0(10)
--------------------------------------------------
```

Locking and Unlocking Accounts

User accounts can be locked or suspended due to violations of login activity policy. A Tivoli Policy Director for Operating Systems administrator can also explicitly lock an account by using the -l option of the `pdoslpadm` command. To lock the account associated with the `bsmith` user ID and prevent future logins, use the following command:

```
pdoslpadm -l bsmith
```

To re-enable an account for login and reset any values that are causing the account to be locked or suspended due to a past violation of login activity policy, use the -u option:

```
pdoslpadm -u bsmith
```

Password Change Date for User Accounts

The login activity policy attempts to use the password change date data from the local system data. This information is often part of the shadow password data that is stored for locally defined user accounts on UNIX systems. However, password change date data is not available in all environments. On HP-UX systems that are not trusted secure systems and in environments with a distributed user registry, such as NIS, NIS+, and DCE, the password change date data is not available.
In environments where the password change date data is not available, the Tivoli Policy Director for Operating Systems administrator can explicitly set a password change data on a user account basis by using the \texttt{-m} option of the \texttt{pdoslpadm} command. This should be done for all user accounts on systems that have policy in place that relies on the password change data, such as a grace login policy or a minimum or maximum password lifetime policy.

**Creation of Local User Accounts with Minimum Password Age Policy**

The specification of a minimum password age policy might cause problems when new accounts are created for locally-defined users or when a password is changed by a system administrator and a password change is required at their first login after the change.

The problem is that when a new user account is created, the password change date is set to the current date. When the new user attempts to login, Tivoli Policy Director for Operating Systems does not allow a password change due to a violation of the minimum password age policy. This problem can also occur on some UNIX systems where the system administrator changes a password and forces the user to change their password at their next login.

An administrator should perform the following steps to ensure that a new local user account with a password can be changed immediately by the user.

1. Create an account using the standard system tools, such as \texttt{mkuser} on AIX or \texttt{useradd} on Solaris.

2. Set the password change date using the \texttt{pdoslpadm -m} command so that the date is sufficiently old to allow the change of the password without violating the current minimum password age policy in effect.

This sequence permits the user to login and change their password without violating login activity policy.

**Configuring NIS for Login Activity Policy**

As previously mentioned in "Password Change Date for User Accounts" on page 83, login activity policy in NIS environments with a distributed user registry is complicated by the fact that password change date data is not maintained. The \texttt{pdoslpadm -m} command can be used to provide the password change data for individual accounts, but this can become an administrative burden.

Tivoli Policy Director for Operating Systems provides support that allows an administrator to configure an NIS server to support password change dates, assuming that the password change dates are available from the system files used to build the NIS maps. The NIS clients also must be configured to request the password change data from the NIS server.

To configure the NIS server to generate a new map that provides password change dates for all user IDs, enter the following command on the NIS server:

\texttt{pdoslpadm -c on -n server}

Note that this new map is generated from the same files as the \texttt{passwd} map that is served by the NIS server. The NIS administrator needs to create a \texttt{cron} job or other administrative task to ensure that the \texttt{passwdchg} map is regenerated every time the \texttt{passwd} map changes.

On the NIS clients, enter the following command to have the NIS clients request the updated \texttt{passwdchg} map from the NIS server:

\texttt{pdoslpadm -c on -n client}

To unconfigure this support on either the NIS client or the NIS server, enter the command specifying the \texttt{-c off} option.
Managing Credentials

Credentials are cached so that Tivoli Policy Director for Operating Systems can make authorization decisions efficiently and also to ensure that it can function isolated from the Tivoli Policy Director user registry.

The PDOSD daemon uses an in-memory cache and a disk cache.

Tuning the Credentials Cache

The `pdoscfg` command has options for tuning the PDOSD daemon’s credential cache:

- **user-cred-refresh**
  The number of minutes that a user’s credentials can exist in the credentials cache before they are considered to be due for a refresh. The interval starts at the time the credential is cached. When the refresh interval is exceeded, the credential is refreshed.

- **admin-cred-refresh**
  The frequency of refresh of the credentials associated with PDOS administrative users. This lets you manage the credentials refresh period for administrative users independently of the general user.

- **cred-hold**
  The number of minutes that credentials associated with a non-administrative user can be kept in the credentials cache beyond the time of the user’s last access. Credentials associated with non-administrative users are flushed from the cache after this interval. The credentials associated with administrative users are never flushed from the cache. The `cred-hold` interval must be at least as long as the `user-cred-refresh` interval.

The values for these parameters are stored in the `/opt/pdos/etc/pdosd.conf` file in the `[credentials]` stanza when Tivoli Policy Director for Operating Systems is initially configured. For most environments, the default values are probably sufficient. You can change the value with the `pdoscfg` command but the changes do not take effect until the next time Tivoli Policy Director for Operating Systems is stopped and restarted on the system. See “`pdoscfg`” on page 153 for more information about the `pdoscfg` command.

Explicitly Refreshing Credentials

Credentials are initially retrieved or refreshed from the Policy Director User Registry when a user logs into a system using a supported and defined login program while Tivoli Policy Director for Operating Systems is running. All authorization decisions made for operations performed by processes subsequently run by this user are made using these credentials. You can explicitly refresh the credentials of a user already logged into the system, or a user can refresh their own credentials. The `pdosrefresh` command refreshes the cached credentials for the specified users.

A user can refresh current credentials by invoking the `pdosrefresh` command with no options. An administrative user can refresh another user’s credentials by specifying the UID or name. You can specify multiple users in a single invocation of the command.

Assume that you change the group membership in the Tivoli Policy Director User registry for the users sally and riley. To have this change take effect immediately, the credentials associated with these users need to be refreshed.

1. To refresh the credentials of users **sally** and **riley**, enter:
   ```
   pdosrefresh -n sally -n riley
   ```
2. Sally and Riley can each refresh their credentials by entering: **pdosrefresh**

### Explicitly Destroying Credentials

The **pdosdestroy** command removes the cached credentials of the specified users. A user can destroy the current credentials by invoking the **pdosdestroy** command with no options. You can remove the credentials of another user by specifying the UID or name. You can specify more than one user on the command line.

To destroy the credentials of the invoking user, enter:
```
pdosdestroy
```
To destroy the credentials of users sally and riley, the user whose UID is 300, enter:
```
pdosdestroy -n sally -u 300
```

### Determining the Accessor Identity

You might need to explicitly check the Tivoli Policy Director for Operating Systems accessor identity associated with the environment of a user or of a running process.

The **pdoswhoami** command displays the Tivoli Policy Director for Operating Systems accessor information associated with the invoking user. The command, with no options, displays the Tivoli Policy Director for Operating Systems username. The **-n** option displays the invoking user’s accessor ID. The **-a** option displays both the username and ID.

The **-l** option displays the user’s group membership, the time the credentials were last refreshed, the credentials refresh expiry, the time the credentials was last accessed, and the credentials’ hold time expiry.

### Examples of pdoswhoami and pdoswhois

The user **sally** is logged into a system running Tivoli Policy Director for Operating Systems. Sally can view her own credentials by entering the command:
```
pdoswhoami -l
```
The output is:
```
106 sally
The credential is associated with the following groups:
  osseal-testers
  osseal-developers
The credential was last refreshed at Sat Nov 4 14:07:21 2000
The credential refresh time expires at Sun Nov 5 02:07:21 2000
The credential was last accessed at Sat Nov 4 14:07:29 2000
The credential hold time expires at Sat Nov 11 14:07:29 2000
```

The root user, who is a Tivoli Policy Director for Operating Systems administrator by default, enters the command:
```
pdoswhoami -l
```
The output is:
```
0 root
The credential is associated with the following groups:
  osseal-admin
  osseal-auditors
The credential was last refreshed at Sat Nov 4 11:52:56 2000
The credential refresh time never expires.
The credential was last accessed at Sat Nov 4 14:12:56 2000
The credential hold time never expires.
The `pdoswhois` command displays the Tivoli Policy Director for Operating Systems accessor information associated with running processes specified by process ids (pids). The list of pids must be specified last on the `pdoswhois` command line. For each pid specified, the accessor ID and username are displayed. If the `-l` option is specified, then the group membership, the time the credentials were last refreshed, the credentials refresh expiry, the time the credentials were last accessed, and the credentials hold time expiry are also displayed.

You, an administrator, can determine what credentials are associated with the running processes whose process IDs are 1756 and 1806 by entering:

```
pdoswhois 1756 1806
```

The output is

```
Pid, 1756, is running under the uid = 106, user name = sally.
Pid, 1806, is running under the uid = 300, user name = riley.
```

### Accessor Identity and the UNIX Identity Differences

The Tivoli Policy Director for Operating Systems accessor identity and the UNIX identity in effect for a user or a running process might be different. For example, issuing a `su` command might change a user’s UNIX identity but does not change the user’s Tivoli Policy Director for Operating Systems accessor identity. Executing a setuid or setgid program might change the UNIX identity of the process but the Tivoli Policy Director for Operating Systems accessor identity associated with the process will still be that of the invoker. For example, the user sally is permitted to perform a change ID operation to the root user and runs the `/bin/su` command to become the root user. The Tivoli Policy Director for Operating Systems accessor identity associated with this user is still sally but the UNIX identity is the root user.

First the user sally issues these commands:

```
# id
uid = 106(sally)

# pdoswhoami -a
106 sally

/bin/su
```

After issuing `/bin/su`:

```
# id
uid=0(root)

# pdoswhoami -a
106 sally
```

### The Hostname Look-aside Database

To eliminate the need to consult the native naming service for every IP address or hostname lookup, Tivoli Policy Director for Operating Systems maintains a hostname look-aside database. This database is populated at runtime as the lookups occur. The use of this database is enabled by default when Tivoli Policy Director for Operating Systems is initially configured on a system.

### Configuring the Hostname Look-aside Database

Use the `pdoscfg` command to disable the hostname look-aside database by specifying `-dns off`. You can enable or disable the hostname look-aside database at any time with the
**pdoscfg** command but the changes do not take effect until the next time Tivoli Policy Director for Operating Systems is stopped and restarted.

To enable the hostname look-aside database for the next restart, enter: `pdoscfg –dns on`.

To disable the hostname look-aside database for the next restart, enter: `pdoscfg –dns off`.

### Managing the Hostname Look-aside Database

Use the **pdoshla** command to manage the database. You might need to do this when cached information became obsolete due to changes in the native naming service. The **pdoshla** command adds, deletes, refreshes, and views entries in the database.

The **–l** option lists the existing database entries; it can be qualified by specifying all, stale, or fresh. You can add an entry for a given IP address by using the **–a** option.

The native naming service is used to resolve the hostname unless the **–H** option is used to specify the associated hostname.

The entry’s default time-to-live value is 6 hours (21600 seconds). Use the **–T** option and explicitly specify the time-to-live value to override the default.

The **–F** option flushes the entire database. The **-f** option flushes stale entries from the database. The **–r** option flushes the specified entry.

Use the **–u** option to refresh all the database entries and cause a native name service lookup to occur for each entry found in the database.

### Examples of Using pdoshla

The following are examples of using the **pdoshla** command.

1. To add an entry to the default database for IP address 146.84.107.11, enter:
   ```
   pdoshla -a 146.84.107.11
   ```

2. To view all of the entries in the default database, enter:
   ```
   pdoshla -l all
   ```
   The output is:
   ```
   # Internet Address   Hostname
   9.41.3.101   test1.austin.lab.tivoli.com
   146.84.107.11  office1.tivoli.com
   9.41.3.123   test3.austin.lab.tivoli.com
   ```

3. To view stale entries found in the default database, enter:
   ```
   pdoshla -l stale
   ```
   The output is:
   ```
   # Internet Address   Hostname
   9.41.3.123   test3.austin.lab.tivoli.com
   ```

4. To flush stale entries from the default database, enter: `pdoshla -f`

5. To refresh all entries found in the default database, enter:
   ```
   pdoshla -u
   ```

### Backing Up and Restoring Configuration Files and Databases

The **pdosbkup** and **pdosrstr** commands back up and restore Tivoli Policy Director for Operating Systems configuration files and databases.
Backing Up Configuration Files and Databases

You should stop Tivoli Policy Director for Operating Systems before backing it up. If the `pdosbkup` command is executed while the daemons are running, the state of some of the files can change during the backup.

The `pdosbkup` command backs up all files and directories in the `/opt/pdos/etc/pdosbkuplist` file. If `–x` is specified, the files and directories listed in the `/opt/pdos/etc/pdosbkuplistx` file are backed up. If a directory is specified in the backup list, only files immediately under that directory are backed up. Subdirectories are traversed.

By default, the backup file created is placed in a file with the date and timestamp appended to it in the form of: `/var/pdos/pdosbkup/pdosbkupDDMMMYYYY.HH_MM_SS.tar`. For example, a backup performed at 12:34:56 on November 19, 2001 would be named: `/var/pdos/pdosbkup/pdosbkup19Nov2001.12_34_56.tar`

Use the `-p` option to change the directory in which the backup file is placed. Use the `–f` option to change the backup file name.

Examples of Backing Up Tivoli Policy Director for Operating Systems

The following are examples of backing up Tivoli Policy Director for Operating Systems.

1. To backup critical configuration files, enter:
   `pdosbkup`

2. To do an extended back up, enter:
   `pdosbkup -x`

Restoring Tivoli Policy Director for Operating Systems

The `pdosrstr` command restores Tivoli Policy Director for Operating Systems files that were previously saved using the `pdosbkup` command. Files are restored from the backup file specified by the `-f` option.

Example of Restoring Tivoli Policy Director for Operating Systems

The following is an example of restoring Tivoli Policy Director for Operating Systems from a backup file.

1. To restore files saved in the `pdosbkup25Oct2001.14_32_41.tar` file, enter:
Tasks Available from Tivoli Desktop

The tasks and jobs described in this chapter are available only if you have installed the Tivoli Policy Director for Operating Systems Management Tasks component. For information on installing this component, see the *Tivoli Policy Director for Operating Systems Installation Guide*. If you did not install the Tivoli Policy Director for Operating Systems Management Tasks component, the information in this section does not apply to you. Instead, you should consult [Chapter 4, “Administrative Tasks” on page 71](#) for information on using the command line to administer Tivoli Policy Director for Operating Systems.

When the Tivoli Policy Director for Operating Systems Management Tasks component is installed, a **PDOS Tasks** task library is made available to the Tivoli desktop that allows you to manage Tivoli Policy Director for Operating Systems and its daemons. The **PDOS Tasks** task library is located in the **Policy Director Region** policy region.

**Note:** All of the Tivoli Policy Director for Operating Systems Management Tasks run as root on the target system. The tasks rely on root’s privileges as a Tivoli Policy Director for Operating Systems runtime administrator. If the root user ID is removed as a Tivoli Policy Director for Operating Systems runtime administrator, the tasks must be modified to run as a different runtime administrator.

In addition to the tasks provided with Tivoli Policy Director for Operating Systems, you can create your own tasks and jobs. A job is a task for which the targets and output parameters are preconfigured. See the *Tivoli Management Framework User’s Guide* for more information about task libraries, tasks, and jobs.

You can modify the default execution characteristics of a particular job, such as where the output of a job is displayed and on which machines the job will run. You can also specify whether a job runs serially on each machine, in parallel on all machines, or staged in groups of machines.

**Task Overview**

When you run a task, you must explicitly specify the nodes on which the task will run. As a convenience, jobs have been provided for those tasks that you typically run on all Tivoli Policy Director for Operating Systems nodes. These jobs are configured to run on all the nodes that are subscribers of the Tivoli Policy Director for Operating Systems profile manager (**PDOS**), except where noted. All of the managed nodes on which you install Tivoli Policy Director for Operating Systems are subscribed to the **PDOS** profile manager automatically. You can also install Tivoli Policy Director for Operating Systems on endpoints. Use the **Subscribe PDOS Endpoints** job to subscribe the Tivoli Policy Director for Operating Systems endpoints to the **PDOS** profile manager.
These tasks can be modified to run on selected subscribers. You can also create your own tasks and jobs. For example, you can create separate tasks to start and stop Tivoli Policy Director for Operating Systems servers on specific managed nodes. See the *Tivoli Management Framework User’s Guide* for more information about task libraries, tasks, and jobs, and about creating your own tasks and jobs.

The following table provides the authorization role information for each of the Tivoli Policy Director for Operating Systems tasks and jobs. The context for each authorization role is the task library.

**Table 40. Authorization for Tivoli Policy Director for Operating Systems Tasks**

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Authorization Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add/Remove PDOS Auditors/Administrators</td>
<td>admin</td>
</tr>
<tr>
<td>Backup PDOS Database</td>
<td>admin</td>
</tr>
<tr>
<td>Certificate Transfer Utility</td>
<td>user</td>
</tr>
<tr>
<td>Configure PDOS Auditing</td>
<td>admin</td>
</tr>
<tr>
<td>Configure PDOS Caching</td>
<td>admin</td>
</tr>
<tr>
<td>Configure PDOS Logging</td>
<td>admin</td>
</tr>
<tr>
<td>Configure PDOS Login and Password Policy</td>
<td>admin</td>
</tr>
<tr>
<td>Configure PDOS Server</td>
<td>admin</td>
</tr>
<tr>
<td>Configure PDOS TCB</td>
<td>admin</td>
</tr>
<tr>
<td>Display PDOS Hostname Cache</td>
<td>admin</td>
</tr>
<tr>
<td>Import UNIX TCB</td>
<td>admin</td>
</tr>
<tr>
<td>Import UNIX Users and Groups</td>
<td>admin</td>
</tr>
<tr>
<td>Manage PDOS Credential Cache</td>
<td>admin</td>
</tr>
<tr>
<td>Manage PDOS Server State</td>
<td>admin</td>
</tr>
<tr>
<td>Manage PDOS TCB</td>
<td>admin</td>
</tr>
<tr>
<td>Migrate TACF to PDOS</td>
<td>admin</td>
</tr>
<tr>
<td>Purge PDOS Hostname Cache</td>
<td>admin</td>
</tr>
<tr>
<td>Query PDOS Login and Password Policy</td>
<td>admin</td>
</tr>
<tr>
<td>Query PDOS Server State</td>
<td>admin</td>
</tr>
<tr>
<td>Query PDOS TCB</td>
<td>admin</td>
</tr>
<tr>
<td>Restore PDOS Database</td>
<td>admin</td>
</tr>
<tr>
<td>Set PDOS Server Audit Level</td>
<td>admin</td>
</tr>
<tr>
<td>Set PDOS Server Trace Level</td>
<td>admin</td>
</tr>
<tr>
<td>Setup TEC Event Server for PDOS</td>
<td>admin, senior, super</td>
</tr>
<tr>
<td>Show PDOS Auditing Configuration</td>
<td>admin</td>
</tr>
<tr>
<td>Show PDOS Auditors/Administrators</td>
<td>admin</td>
</tr>
<tr>
<td>Show PDOS Caching Configuration</td>
<td>admin</td>
</tr>
<tr>
<td>Show PDOS Logging Configuration</td>
<td>admin</td>
</tr>
<tr>
<td>Show PDOS Server Audit Level</td>
<td>admin</td>
</tr>
<tr>
<td>Show PDOS Server Configuration</td>
<td>admin</td>
</tr>
<tr>
<td>Show PDOS TCB Configuration</td>
<td>admin</td>
</tr>
<tr>
<td>Start TEC Adapter</td>
<td>admin</td>
</tr>
<tr>
<td>Stop TEC Adapter</td>
<td>admin</td>
</tr>
</tbody>
</table>
Table 40. Authorization for Tivoli Policy Director for Operating Systems Tasks (continued)

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Authorization Roles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscribe PDOS Endpoints</td>
<td>admin</td>
</tr>
<tr>
<td>Update PDOS Hostname Cache</td>
<td>admin</td>
</tr>
</tbody>
</table>

General Information Regarding wrunjob and wruntask

You can use the `wrunjob` and `wruntask` commands to run the Tivoli Policy Director for Operating Systems tasks from a script, and you can use the `wschedjob` command to schedule jobs. In the following sections, each Tivoli Policy Director for Operating Systems task description includes the arguments required for `wruntask` and `wrunjob`. All arguments listed must be used, and they must be used in the order shown. For more information about the `wruntask` and `wrunjob` commands, as well as the `wschedjob` command for scheduling jobs, see the *Tivoli Management Framework Reference Manual.*

Add/Remove PDOS Auditors/Administrators

This task can be used to add or remove users as Tivoli Policy Director for Operating Systems auditors or administrators. To add a user as an administrator, you must make the user a member of the local UNIX group, `osseal`, and a member of the associated Tivoli Policy Director group, `osseal-admin`. To add a user as an auditor, you must make the user a member of the local UNIX group, `ossaudit`, and a member of the associated Tivoli Policy Director group, `osseal-auditors`.

To remove a user’s privileges as an administrator, you should remove the user from the `osseal` group. To remove a user’s privileges as an auditor, you should remove the user from the `ossaudit` group. If you remove the user from `osseal-auditors` or `osseal-admin`, you will remove the user’s privileges on all Tivoli Policy Director for Operating Systems machines. Both the Add and Remove actions require a Tivoli Policy Director Administrator’s ID and password to be specified.

**Note:** All of the Tivoli Policy Director for Operating Systems Management Tasks run as root on the target system. The tasks rely on root’s privileges as a Tivoli Policy Director for Operating Systems runtime administrator. If the root user ID is removed as a Tivoli Policy Director for Operating Systems runtime administrator, the tasks must be modified to run as a different runtime administrator. See the *Tivoli Management Framework User’s Guide* for more information about task libraries, tasks, and jobs.
The following job dialog corresponds to the **Add/Remove PDOS Auditors/Administrators** task:

![Add/Remove PDOS Auditors/Administrators dialog](image)

Use the following steps to perform this task:

1. If the user is to be added to or removed from the **osseal-auditors** or **osseal-admin** group, you must specify the first two fields.
2. Specify the name of the user to be added or removed.
3. Select the desired operation: **Add** or **Remove**.
4. Click the **Execute and Close** button to perform the task.

**Syntax for wrunjob and wruntask**

Use the following arguments, in the order shown, to run this task from the command line or a script using `wrunjob` or `wruntask`:

```
wrunjob "Add/Remove PDOS Auditors/Administrators" -l "PDOS Tasks" -a pd_admin_id -a pd_admin_passwd -a account -a action -a osssaudit -a osseal_auditors -a osseal -a osseal_admin
```

```
wruntask -t "Add/Remove PDOS Auditors/Administrators" -l "PDOS Tasks" -a pd_admin_id -a pd_admin_passwd -a account -a action -a osssaudit -a osseal_auditors -a osseal -a osseal_admin -h task_endpoint
```

where:

- **pd_admin_id**
  Specifies the name of a Tivoli Policy Director Administrative account that will be used to perform the **Add** or **Remove** action. This argument is required only if any of the Tivoli Policy Director group checkboxes are marked.

- **pd_admin_passwd**
  Specifies the password of the administrative account. This argument is required only if any of the Tivoli Policy Director group checkboxes are marked.

- **account**
  Specifies the user account from which to add or remove privileges. Completion of this parameter is required.
**action** Specifies whether to add or remove privileges from the specified account. This value must be either **ADD** or **REMOVE**.

**ossaudit**

If this parameter is set to **TRUE**, then the user will be added to or removed from the local UNIX group, **ossaudit**. This value must be either **TRUE** or **FALSE**.

**osseal_auditors**

If this parameter is set to **TRUE**, then the user will be added to or removed from the Tivoli Policy Director group, **osseal-auditors**. This value must be either **TRUE** or **FALSE**.

**osseal**

If this parameter is set to **TRUE**, then the user will be added to or removed from the local UNIX group, **osseal**. This value must be either **TRUE** or **FALSE**.

**osseal_admin**

If this parameter is set to **TRUE**, then the user will be added to or removed from the Tivoli Policy Director group, **osseal-admin**. This value must be either **TRUE** or **FALSE**.

**task_endpoint**

Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.

### Backup PDOS Database

This task allows the administrator to back up the Tivoli Policy Director for Operating Systems databases and configuration files to an optionally specified file name. The file name may be specified as a relative or absolute path. If the path is relative, it is assumed relative to the directory `/var/pdos/pdosbkup`. The file name may contain format characters supported by the **date** command. These characters will be automatically expanded. If not specified, the file name defaults to `/var/pdos/pdosbkup/pdosbkup%m%d%y.tar`.

By default, backup files can be restored on a machine that is configured as a Tivoli Policy Director client. Extended backup files can be created to restore a machine to a working state in an isolated environment where the Tivoli Policy Director server is not available.

The following job dialog corresponds to the **Backup PDOS Database** task:

![Backup PDOS Database](image)

Use the following steps to perform this task:

1. Enter a name for the Tivoli Policy Director for Operating Systems database backup file. This may be specified as an absolute or relative path; if relative, it is assumed relative to `/usr/pdos/backup`. The file name can contain format characters as supported by the **date** command. These will be automatically expanded. If unspecified, the file name used is `/var/pdos/pdosbkup/pdosbkup%m%d%y.tar`.

2. If an extended backup is required, check **Perform extended backup**.
3. Click the **Execute and Close** button to perform the task.

**Syntax for wrunjob and wruntask**

Use the following arguments, in the order shown, to run this task from the command line or a script using **wrunjob** or **wruntask**:

```
wrunjob "Backup PDOS Database" –l "PDOS Tasks" –a file_name –a extended_backup
wruntask –t "Backup PDOS Database" –l "PDOS Tasks" –a file_name –a extended_backup –h task_endpoint
```

where:

* `file_name` Specifies the file name in which to store the database backup. If this value is the empty string, the default name is used.

* `extended_backup` Specifies whether or not to perform an extended backup. The value is either **TRUE** or **FALSE**.

* `task_endpoint` Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.

**Certificate Transfer Utility**

Before a managed node or endpoint can be installed with Tivoli Tivoli Policy Director for Operating Systems, it must have the digital CA certificates needed to configure both the Tivoli Policy Director runtime environment and Tivoli Policy Director for Operating Systems.

Tivoli Policy Director for Operating Systems requires the LDAP SSL certificate used by the LDAP server for SSL communications as well as the CA certificate for the Tivoli Policy Director management server. If the management server has not been configured to automatically download the CA certificate during configuration of the Tivoli Policy Director runtime environment, the certificate must be obtained manually from the management server. This task provides an easy method to transfer the two certificates to target systems. The two certificates must be placed in directories on a managed node. The certificates do not need to be in the same directory. The task itself generates tasks that will be run on each destination system selected.
The following job dialog corresponds to the **Certificate Transfer Utility** task:

![Certificate Transfer Utility Image]

Use the following steps to perform this task:

1. Enter the path name for the **LDAP SSL certificate**. This path name must be on the Tivoli management region server. It must be readable by the root user.
2. Enter the path name for the **PD Server certificate**. This path name must be on the Tivoli management region server. It must be readable by the root user.
3. Enter the path name for the **Destination Directory** on the target systems. It must be writable by the root user.
4. Select the desired **Destination Systems**.
5. Click the **Execute and Close** button to perform the task.

### Syntax for wrunjob and wruntask

Use the following arguments, in the order shown, to run this task from the command line or a script using **wrunjob** or **wruntask**:

**wrunjob** "Certificate_Transfer" –l "PDOS Tasks" –a ldap_certificate –a pd_certificate –a dest_directory –a dest_system [–a dest_system,...]

**wruntask** –t "Certificate_Transfer" –l "PDOS Tasks" –a ldap_certificate –a pd_certificate –a dest_directory –a dest_system [–a dest_system,...] –h task_endpoint

**Note:** While the Tivoli Policy Director for Operating Systems install requires the installation images be put on a local directory, the certificates can be placed in a common network location. Use this tool if this cannot be done or if you cannot use other methods, such as FTP, to transfer the certificates to a Tivoli Policy Director for Operating Systems target system.

where:

- **ldap_certificate** Specifies the LDAP SSL certificate.
- **pd_certificate** Specifies the Policy Director Server certificate.
- **dest_directory** Specifies the destination directory.
- **dest_system** Specifies the destination system. Destination systems must be specified as either "system(Endpoint)" or "system(ManagedNode)".
<task_endpoint> Specifies the name of the managed node where the certificates to be transferred are stored. This task should not be run on an endpoint or profile manager.

Configure PDOS Auditing

This task allows the administrator to modify the Tivoli Policy Director for Operating Systems configuration parameters related to auditing.

Two parameters can be modified: the audit log size limit and the audit log flush frequency. If a value is not specified, the configuration parameter is left unchanged. Changes can either be placed into effect immediately or wait until the next restart of Tivoli Policy Director for Operating Systems.

The following job dialog corresponds to the Configure PDOS Auditing task:

![Configure PDOS Auditing dialog]

Use the following steps to perform this task:

1. Enter values for the parameters you wish to change. Parameters with no value set will be left unchanged.

2. If Tivoli Policy Director for Operating Systems should be restarted after making the configuration changes, check **Apply changes immediately**. Otherwise, changes will not take effect until the next restart of Tivoli Policy Director for Operating Systems.

3. Click the **Execute and Close** button to perform the task.

Syntax for wrunjob and wruntask

Use the following arguments, in the order shown, to run this task from the command line or a script using **wrunjob** or **wruntask**:

**wrunjob** "Configure PDOS Auditing" –l "PDOS Tasks" –a apply_now –a size –a frequency

**wruntask** –t "Configure PDOS Auditing" –l "PDOS Tasks" –a apply_now –a size –a frequency –h task_endpoint

where:

- **apply_now** Indicates that Tivoli Policy Director for Operating Systems should be restarted after the changes are made. This value must be either **TRUE** or **FALSE**.

- **size** Specifies the size limit for audit logs in bytes. If this value is the empty string, no change is made.

- **frequency** Specifies the frequency of flushes to the audit log in seconds. If this value is the empty string, no change is made.
**Configure PDOS Caching**

This task allows the administrator to modify the Tivoli Policy Director for Operating Systems configuration parameters related to caching.

Five parameters can be modified: the refresh frequency of administrator credentials, the refresh frequency of user credentials, how long to cache unaccessed user credentials, whether a hostname resolution cache should be used, and whether a username resolution cache should be used. If a value is not specified, the configuration parameter is left unchanged. Changes can either be placed into effect immediately or wait until the next restart of Tivoli Policy Director for Operating Systems.

The following job dialog corresponds to the **Configure PDOS Caching** task:

![Configure PDOS Caching dialog](image)

Use the following steps to perform this task:

1. Enter values for the parameters you wish to change. If a value is left unspecified, it will be left unchanged. The refresh intervals and credential hold period are in minutes.

2. If Tivoli Policy Director for Operating Systems should cache hostnames and IP addresses, check **Cache hostname to IP address mapping**.

3. If Tivoli Policy Director for Operating Systems should cache user/group names and user/group IDs, check **Cache username to uid/gid mapping**.

4. If Tivoli Policy Director for Operating Systems should be restarted after making the configuration changes, check **Apply changes immediately**. Otherwise, changes will not take effect until the next restart of Tivoli Policy Director for Operating Systems.

5. Click the **Execute and Close** button to perform the task.

**Syntax for wrunjob and wruntask**

Use the following arguments, in the order shown, to run this task from the command line or a script using **wrunjob** or **wruntask**:

```
wrunjob "Configure PDOS Caching" -l "PDOS Tasks" --apply_now --admin_refresh --user_refresh --user_credential_hold --cache_hosts --cache_users
```
Configure PDOS Caching

wruntask -t "Configure PDOS Caching" -l "PDOS Tasks" -a apply_now -a admin_refresh -a user_refresh -a user_cred_hold -a cache_hosts -a cache_users -h task_endpoint

where:

apply_now Indicating that Tivoli Policy Director for Operating Systems should be restarted after the changes are made. This value must be either TRUE or FALSE.

admin_refresh Specifies how often cached administrator credentials should be refreshed in minutes. If this value is the empty string, no change is made.

user_refresh Specifies how often cached user credentials should be refreshed in minutes. If this value is the empty string, no change is made.

user_cred_hold Specifies how long to cache unaccessed user credentials in minutes. This value must be greater than or equal to the configured values for the administrator and user credentials refresh intervals. If this value is the empty string, no change is made.

cache_hosts Indicates whether hostname resolution should use a local cache. This value must be either TRUE or FALSE.

cache_users Indicates whether username resolution should use a local cache. This value must be either TRUE or FALSE.

task_endpoint Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.

Configure PDOS Logging

This task allows the administrator to modify the Tivoli Policy Director for Operating Systems configuration parameters related to logging.

Six configuration parameters related to logging can be modified. These parameters specify the number of log files and the maximum number of entries per log file to use for logging in the Tivoli Policy Director for Operating Systems daemons, PDOSD, PDOSAUDITD, and PDOSWDD. If a value is not specified, the configuration parameter is left unchanged. Changes can either be placed into effect immediately or wait until the next restart of Tivoli Policy Director for Operating Systems.
The following job dialog corresponds to the **Configure PDOS Logging** task:

![Configure PDOS Logging dialog](image)

Use the following steps to perform this task:

1. Enter values for the parameters you wish to change. If a value is not specified, the parameter will be left unchanged.
2. If Tivoli Policy Director for Operating Systems should be restarted after making the configuration changes, check **Apply changes immediately**. Otherwise, changes will not take effect until the next restart of Tivoli Policy Director for Operating Systems.
3. Click the **Execute and Close** button to perform the task.

**Syntax for wrunjobj and wruntask**

Use the following arguments, in the order shown, to run this task from the command line or a script using **wrunjobj** or **wruntask**:

```
wrunjobj "Configure PDOS Logging" -t "PDOS Tasks" -a apply_now -a pdosd_logs -a pdosd_entries -a pdoswdd_logs -a pdoswdd_entries -a pdosauditd_logs -a pdosauditd_entries
wruntask -t "Configure PDOS Logging" -t "PDOS Tasks" -a apply_now -a pdosd_logs -a pdosd_entries -a pdoswdd_logs -a pdoswdd_entries -a pdosauditd_logs -a pdosauditd_entries -h task_endpoint
```

where:

- **apply_now** Indicates that Tivoli Policy Director for Operating Systems should be restarted after the changes are made. This value must be either **TRUE** or **FALSE**.
- **pdosd_logs** Specifies the number of log files to use for the PDOSD daemon. If this value is the empty string, the parameter is left unchanged.
- **pdosd_entries** Specifies the number of entries to allow per log for the PDOSD daemon. If this value is the empty string, the parameter is left unchanged.
Configure PDOS Logging

pdoswdd_logs  Specifies the number of log files to use for the PDOSWDD daemon. If this value is the empty string, the parameter is left unchanged.

pdoswdd_entries  Specifies the number of entries to allow per log for the PDOSWDD daemon. If this value is the empty string, the parameter is left unchanged.

pdosaudidt_logs  Specifies the number of log files to use for the PDOSAUDITD daemon. If this value is the empty string, the parameter is left unchanged.

pdosaudidt_entries  Specifies the number of entries to allow per log for the PDOSAUDITD daemon. If this value is the empty string, the parameter is left unchanged.

task_endpoint  Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.

Configure PDOS Login and Password Policy

This task allows the administrator to configure parameters related to Tivoli Policy Director for Operating Systems Login and Password Policy. The following policy can be configured:

- Tivoli Policy Director for Operating Systems Login and Password Policy can be enabled or disabled. By default, the field is blank and does not change the current setting.
- A specified user account can be locked, unlocked, have its login activity records deleted, or have the password change date set to the current date.

The following job dialog corresponds to the Configure PDOS Login and Password Policy task:

Use the following steps to perform this task:

1. You can enable, disable, or leave Tivoli Policy Director for Operating Systems Login and Password Policy at its current setting.

2. Specify the User account to be modified.
3. Select the operation you wish to perform.
4. Specify whether to reset the date.
5. Click the **Execute and Close** button to perform the task.

**Syntax for wrunjob and wruntask**

Use the following arguments, in the order shown, to run this task from the command line or a script using **wrunjob** or **wruntask**:

```bash
wrunjob "Configure PDOS Login and Password Policy" -l "PDOS Tasks" -a enable_login -a account -a action
wruntask -t "Configure PDOS Login and Password Policy" -l "PDOS Tasks" -a enable_login -a account -a action -h task_endpoint
```

where:

**enable_login**
Indicates whether or not to enable Tivoli Policy Director for Operating Systems Login and Password Policy processing. This value must be either **TRUE** or **FALSE**. If this value is the empty string, no change is made.

**account**
If this parameter is not blank, then the action specified in the action parameter will be performed on the specified user account.

**action**
Indicates what action to perform on the specified account. Valid values are DELETE, LOCK, UNLOCK, and CHANGEDATE.

**task_endpoint**
Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.

**Configure PDOS Server**

This task allows the administrator to modify miscellaneous Tivoli Policy Director for Operating Systems configuration parameters.

Six parameters can be modified: the port Tivoli Policy Director for Operating Systems uses to receive notifications of policy updates, how often (in minutes) policy refreshes occur, whether system login and password restrictions are enabled, the number of kernel threads used to handle authorization requests, the certificate used to communicate and authenticate with the LDAP server, and whether Tivoli Policy Director for Operating Systems should be automatically started at system startup. If the **Policy Update Notification Port** or **LDAP SSL CA certificate** is to be changed, then a password must be specified for the administrator. If a value is not specified, the configuration parameter is left unchanged.
The following job dialog corresponds to the **Configure PDOS Server** task:

![Configure PDOS Server Interface](image)

Use the following steps to perform this task:

1. Tivoli Policy Director for Operating Systems can be configured to receive policy update notifications on a specified port. If the **Policy Update Notification Port** is set to 0, then policy updates will not be received by notification. A password for the administrator must be supplied in order to change this parameter. If a value is not specified, the parameter will be left unchanged.

2. Tivoli Policy Director for Operating Systems can be configured to poll the Policy Director management server for policy updates. The **Policy Update Polling Interval** is specified in minutes, and a value of 0 will disable policy update polling. If a value is not specified, the parameter will be left unchanged.

3. Tivoli Policy Director for Operating Systems can be enabled or disabled to enforce system login and password restrictions. If a value is not specified, the parameter will be left unchanged.

4. The number of kernel threads used to handle authorization requests can be changed. This value must be positive. If a value is not specified, the parameter will be left unchanged.

5. The **LDAP SSL CA certificate** can be changed by supplying the full pathname to a file containing the new LDAP certificate. If a value is not specified, the parameter will be left unchanged.

6. The startup behavior of Tivoli Policy Director for Operating Systems can be changed with the **Automatically start PDOS at system startup** drop-down box. If a value is not specified, the parameter will be left unchanged.

7. Click the **Execute and Close** button to perform the task. The Tivoli Policy Director for Operating Systems instance will be restarted with the new configuration.

### Syntax for wrunjob and wruntask

Use the following arguments, in the order shown, to run this task from the command line or a script using **wrunjob** or **wruntask**:

```
wrunjob "Configure PDOS Server" -l "PDOS Tasks" -a notification_port -a refresh_interval -a login_policy -a threads -a ldap_certificate -a autostart -a password
```
Configure PDOS TCB

This task allows the administrator to modify the Tivoli Policy Director for Operating Systems configuration parameters related to the trusted computing base (TCB). The following five parameters can be modified:

- the number of monitoring threads,
- the delay interval (in seconds) between monitoring attempts,
- the maximum number of megabytes of a file to be used for calculating a checksum (TCB signature),
- whether to ignore a file’s ctime in TCB signature comparisons, and
- task_endpoint

where:

notification_port Specifies a port to use to receive policy update notifications. A value of 0 will disable policy update notifications. If this value is the empty string, the parameter is left unchanged. A password must be specified to change this parameter.

refresh_interval Specifies an interval in minutes that the Policy Director Management server is polled for policy updates. A value of 0 will disable policy updates polling. If this value is the empty string, the parameter is left unchanged.

login_policy Specifies whether Tivoli Policy Director for Operating Systems should enforce system login and password restrictions. This value can be TRUE, FALSE, or the empty string.

threads Specifies the number of kernel threads used to handle authorization requests. If this value is the empty string, the parameter is left unchanged.

ldap_certificate Specifies a certificate to communicate and authenticate with the LDAP server. A full pathname to a file containing the certificate must be specified. If this value is the empty string, the parameter is left unchanged. A password must be specified to change this parameter.

autostart Specifies whether Tivoli Policy Director for Operating Systems should be automatically started at system startup. This value can be TRUE, FALSE, or the empty string.

password Specifies the administrator’s password. This field must be specified in order to change the notification_port or ldap_certificate parameters.

task_endpoint Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.
whether to perform the CRC checksum calculation and comparison during execution authorizations.

If a value is not specified for the first three parameters, the configuration parameter is left unchanged. Changes can either be placed into effect immediately or wait until the next restart of Tivoli Policy Director for Operating Systems.

The following job dialog corresponds to the Configure PDOS TCB task:

Use the following steps to perform this task:

1. Enter values for the parameters you wish to change. If a value is not specified, the parameter will be left unchanged.

2. If Tivoli Policy Director for Operating Systems should be restarted after making the configuration changes, check **Apply changes immediately**. Otherwise, changes will not take effect until the next restart of Tivoli Policy Director for Operating Systems.

3. Click the **Execute and Close** button to perform the task.

**Syntax for wrunjob and wruntask**

Use the following arguments, in the order shown, to run this task from the command line or a script using **wrunjob** or **wruntask**:

**wrunjob** "Configure PDOS TCB" –l "PDOS Tasks" –a apply_now –a threads –a interval –a checksum_max_size –a ignore_ctime –a nocrc_on_exec

**wruntask** –t "Configure PDOS TCB" –l "PDOS Tasks" –a apply_now –a threads –a interval –a checksum_max_size –a ignore_ctime –a nocrc_on_exec –h task_endpoint

where:

- **apply_now** Indicates that Tivoli Policy Director for Operating Systems should be restarted after the changes are made. This value must be either **TRUE** or **FALSE**.

- **threads** Specifies the number of threads used to monitor TCB objects. If this value is the empty string, the parameter is left unchanged.

- **interval** Specifies the interval in seconds between monitoring sweeps of the TCB. If this value is the empty string, the parameter is left unchanged.

- **checksum_max_size** Specifies the maximum number of megabytes of a file to be used when computing its *checksum* (TCB signature). The bytes are distributed throughout the file. If this value is the empty string, the parameter is left unchanged.

- **ignore_ctime** If this parameter is set to **TRUE** (enabled), the *ctime* will be ignored in all
TCB signature comparisons. A change in ctime will not cause the TCB resource to become untrusted. This value must be either TRUE or FALSE. The default value is FALSE.

nocrc_on_exec If this parameter is set to TRUE (enabled), the CRC data checksum calculation and comparison will be skipped on TCB signature checks during Tivoli Policy Director for Operating Systems execution authorization processing. This value must be either TRUE or FALSE. The default value is FALSE.

task_endpoint Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.

Display PDOS Hostname Cache

This task allows the administrator to view entries in the IP address/hostname translation cache used by Tivoli Policy Director for Operating Systems.

All stale entries, all valid entries, or both may be displayed.

The following job dialog corresponds to the Display PDOS Hostname Cache task:

Use the following steps to perform this task:

1. Select the type(s) of entries to display: expired, valid, or both.
2. Click the Execute and Close button to perform the task.

Syntax for wrunjob and wruntask

Use the following arguments, in the order shown, to run this task from the command line or a script using wrunjob or wruntask:

wrunjob "Display PDOS Hostname Cache" –l "PDOS Tasks" –a display_valid –a display_stale

wruntask –t "Display PDOS Hostname Cache" –l "PDOS Tasks" –a display_valid –a display_stale –h task_endpoint

where:

display_valid Indicates that all valid entries should be displayed. This value must be either TRUE or FALSE.

display_stale Indicates that all stale entries should be displayed. This value must be either TRUE or FALSE.

task_endpoint Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.
Import UNIX TCB

This task allows the administrator to populate the trusted computing base (TCB) by recursively searching the UNIX system for setuid/setgid programs.

The administrator must specify the class of resources to populate: Login-Programs, Secure-Files, Secure-Programs, Impersonator-Programs, or Immune-Programs. The default is Secure-Programs. Additionally, one or more directories to recursively search may be supplied in the form of a comma-separated list. If desired, another list of directories to exclude from the search may be provided. A specific policy branch into which to populate may optionally be supplied. If omitted, the current subscribed policy branch is used. Also, you can choose whether to generate a script to update the TCB with records for the discovered files or simply report the discovered files.

Finally, you can choose whether or not to add multiple entries to the TCB for hard links to files.

The following job dialog corresponds to the Import UNIX TCB task:

Use the following steps to perform this task:

1. Choose the category of files on which to search.
2. As an option, you can specify directories to be included or excluded from the search.
3. If the files discovered in the file system search should generate a script to update the TCB, check Generate update script. Otherwise, the found files will be reported in a window.
4. If files with hard links to them should generate multiple entries in the TCB, check Generate duplicate entry for hard links. Otherwise, one entry will be generated regardless of the number of links to the file.
5. Click the Execute and Close button to perform the task.

Syntax for wrunjob and wruntask

Use the following arguments, in the order shown, to run this task from the command line or a script using wrunjob or wruntask:

wrunjob "Import UNIX TCB" -l "PDOS Tasks" -a class -a branch -a directories -a excludes -a duplicate_links -a generate_script

wruntask -t "Import UNIX TCB" -l "PDOS Tasks" -a class -a branch -a directories -a excludes -a duplicate_links -a generate_script -h task_endpoint

where:
**Import UNIX TCB**

- **class**: Specifies the class of TCB resource to create. This must be one of the classes listed above.

- **branch**: Specifies into which policy branch to import TCB resources. If empty, the currently subscribed policy branch is used.

- **directories**: Specifies a comma-separated list of directories to recursively search.

- **excludes**: Specifies a comma-separated list of directories to exclude from the search.

- **duplicate_links**: Indicates whether multiple entries should be generated for hard linked files. This value must be either TRUE or FALSE.

- **generate_script**: Indicates that a script should be generated to add the discovered files to the TCB. This value must be either TRUE or FALSE.

- **task_endpoint**: Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.

**Import UNIX Users and Groups**

This task allows the administrator to populate the Policy Director account registry using local UNIX account information.

The users and groups provided in comma-separated lists are used to obtain account data from UNIX. Each list may be either Inclusive or Exclusive. An Inclusive list means only those specified users/groups should be imported. An Exclusive list means all users/groups except those specified should be imported. A list value of * indicates all users. List entries must be user/group names, not UIDs/GIDs. An LDAP suffix that will be appended to created users/groups must be supplied. An administrative account in Policy Director and its password are also required to import data. You can specify how to import data for users/groups already existing in LDAP. If a user/group to be imported has a corresponding entry in LDAP, an administrator can specify whether to import information from LDAP or the local UNIX sources.

Optionally, the administrator may choose to only report on the accounts that would be imported. For users, the administrator may specify whether accounts are created enabled (the default) or disabled. The administrator may also specify a default group for users without group membership and a default password (if empty, a random password is assigned). For groups, the administrator may specify the behavior when the group already exists in Policy Director. The administrator may specify that group entries be refreshed for groups that already exist in Policy Director.
The following job dialog corresponds to the **Import UNIX Users and Groups** task:

![Import UNIX Users and Groups dialog](image)

Use the following steps to perform this task:

1. You must specify the first three fields in the **Policy Director** block. All other fields are optional.

2. Click the **Execute and Close** button to perform the task.

### Syntax for wrunjob and wruntask

Use the following arguments, in the order shown, to run this task from the command line or a script using `wrunjob` or `wruntask`:

```
wrunjob "Import UNIX Users and Groups" -l "PDOS Tasks" -a admin_id -a admin_pwd -a suffix -a ldap_import -a report_only -a user_list -a user_list_type -a create_disabled -a default_group -a default_passwd -a group_list -a group_list_type -a group_refresh
```

```
wruntask -t "Import UNIX Users and Groups" -l "PDOS Tasks" -a admin_id -a admin_pwd -a suffix -a ldap_import -a report_only -a user_list -a user_list_type -a create_disabled -a default_group -a default_passwd -a group_list -a group_list_type -a group_refresh -h task_endpoint
```

where:

- **admin_id** Specifies the name of a Tivoli Policy Director administrative account to use to import entries. Completion of this argument is required.

- **admin_pwd** Specifies the password of the administrative account. Completion of this argument is required.
suffix Specifies the LDAP suffix to append to created users and groups. Completion of this argument is required.

ldap_import Indicates that the user or group should be imported from LDAP if it exists there and it is not already a Tivoli Policy Director user or group. This value must be either TRUE or FALSE.

report_only Indicates that the task should only report what it would do and not update the database. This value must be either TRUE or FALSE.

user_list Specifies a comma-separated list of usernames to import (or exclude from import).

user_list_type Indicates whether the list is of users to include or exclude. This value must be either Inclusive or Exclusive.

create_disabled Indicates that users should be created disabled. This value must be either TRUE or FALSE.

default_group Specifies a default Tivoli Policy Director group to which to add created users if they have no group membership.

default_passwd Specifies a default password to assign to the created users.

group_list Specifies a comma-separated list of group names to import, or exclude from import.

group_list_type Indicates whether the list of groups is inclusive or exclusive. This value must be either Inclusive or Exclusive.

group_refresh Indicates whether, if the group already exists, the group membership should be updated to match the UNIX group. This value must be either TRUE or FALSE.

task_endpoint Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.

Manage PDOS Credential Cache

This task allows the administrator to refresh and/or destroy entries in the credential cache used by Tivoli Policy Director for Operating Systems.

The administrator may specify two comma-separated lists, one to indicate credentials to refresh and the other to indicate credentials to destroy. Either is optional. List entries may be either a UID or a username.

The following job dialog corresponds to the Manage PDOS Credential Cache task:
Use the following steps to perform this task:

1. Enter a comma-separated list of users and/or UIDs whose cached credentials should be refreshed. An empty list indicates no credentials should be refreshed.

2. Enter a comma-separated list of users or UIDs whose cached credentials should be destroyed. An empty list indicates no credentials should be destroyed.

3. Click the **Execute and Close** button to perform the task.

**Syntax for wrunjob and wruntask**

Use the following arguments, in the order shown, to run this task from the command line or a script using *wrunjob* or *wruntask*:

```
wrunjob "Manage PDOS Credential Cache" –l "PDOS Tasks" –a refresh_list –a destroy_list
wruntask –t "Manage PDOS Credential Cache" –l "PDOS Tasks" –a refresh_list –a destroy_list –h task_endpoint
```

where:

- **refresh_list** Specifies UIDs/usernames for which the cached credential should be refreshed. If empty, no cached credentials are refreshed.

- **destroy_list** Specifies UIDs/usernames for which the cached credential should be removed. If empty, no cached credentials are removed.

- **task_endpoint** Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.

**Manage PDOS Server State**

This task allows the administrator to individually change the state of the daemons comprising a running Tivoli Policy Director for Operating Systems instance.

The PDOSD, PDOSAUDITD, and PDOSWDD daemons can be told to **Do Nothing, Start, Stop, or Restart.** **Do Nothing** leaves the daemon’s state unchanged. **Start** starts any daemons not currently running in the Tivoli Policy Director for Operating Systems instance. **Stop** stops the daemon, if it is not already stopped. **Restart** stops all the daemon in the Tivoli Policy Director for Operating Systems instance and restarts it.
The following job dialog corresponds to the **Manage PDOS Server State** task:

![Manage PDOS Server State](image)

Use the following steps to perform this task:

1. Set the desired state changes for each daemon.
2. Click the **Execute and Close** button to perform the task.

**Syntax for wrunjob and wruntask**

Use the following arguments, in the order shown, to run this task from the command line or a script using *wrunjob* or *wruntask*:

**wrunjob** "Manage PDOS Server State" –l "PDOS Tasks" –a pdosd_state –a pdosauditd_state –a pdoswdd_state

**wruntask** –t "Manage PDOS Server State" –l "PDOS Tasks" –a pdosd_state –a pdosauditd_state –a pdoswdd_state –h task_endpoint

where:

- **pdosd_state** Indicates the change to make to the state of the PDOSD daemon. If not one of **Start**, **Stop**, or **Restart**, the daemon’s state will remain unchanged.

- **pdosauditd_state** Indicates the change to make to the state of the PDOSAUDITD daemon. If not one of **Start**, **Stop**, or **Restart**, the daemon’s state will remain unchanged.

- **pdoswdd_state** Indicates the change to make to the state of the PDOSWDD daemon. If not one of **Start**, **Stop**, or **Restart**, the daemon’s state will remain unchanged.

- **task_endpoint** Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.

**Manage PDOS TCB**

This task allows the administrator to modify or validate the trust status of objects in the Tivoli Policy Director for Operating Systems Trusted Computing Base (TCB).
An operation and a comma-separated list of objects on which to apply the operation must be supplied. Valid operations are Trust, Untrust, and Validate. Trust marks the specified objects as trusted. Untrust marks the specified objects as untrusted. Validate checks the signature of the specified objects and if they have been modified, marks them untrusted. Objects must be specified as absolute paths. A list value of * indicates all objects in the TCB.

The following job dialog corresponds to the Manage PDOS TCB task:

Use the following steps to perform this task:

1. Enter a comma-separated list of files in the TCB on which you wish to modify the trust state. A value of * can be used to indicate all files in the TCB.
2. Select an operation to perform. Trust marks the files as trusted. Untrust marks the files as untrusted. Validate checks the signature of the files and if they have been modified, marks them untrusted.
3. Click the Execute and Close button to perform the task.

Syntax for wrunjob and wruntask

Use the following arguments, in the order shown, to run this task from the command line or a script using wrunjob or wruntask:

wrunjob "Manage PDOS TCB" -l "PDOS Tasks" -a operation -a objects
wruntask -t "Manage PDOS TCB" -l "PDOS Tasks" -a operation -a objects -h task_endpoint

where:

operation Indicates the operation to apply. It must be one of Trust, Untrust, or Validate.

objects Specifies the objects to which to apply the operation. If this value is the empty string, no objects are modified.

task_endpoint Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.

Migrate TACF to PDOS

This task allows the administrator to import the contents of an existing Tivoli Access Control Facility database into the Tivoli Policy Director for Operating Systems database. Options are provided to allow an administrator to import policy data, user/group data, or both from Tivoli Access Control Facility. Additionally, an option is provided to simply generate the migration script, without executing it. This option allows the administrator to review any proposed changes to Tivoli Policy Director for Operating Systems, before making them.
The following job dialog corresponds to the Migrate TACF to PDOS task:

![Migrate TACF to PDOS dialog](image)

Use the following steps to perform this task:

1. Enter your **Policy Director Administrator ID**, which is required to execute the migration script.
2. Enter your **Policy Director Administrator Password**, which is required to execute the migration script.
3. Optionally, enter the **PDOS Branch Name**. If you leave this field empty, the configured default will be used.
4. Enter the appropriate **LDAP suffix** if you wish to migrate user/group information.
5. If you wish to populate PD policy information, check **Process resource commands**.
6. If you wish to move user/group information into the Tivoli Policy Director registry, check **Process registry commands**.
7. Click the **Execute and Close** button to perform the task.

**Syntax for wrunjob and wruntask**

Use the following arguments, in the order shown, to run this task from the command line or a script using `wrunjob` or `wruntask`:

```bash
wrunjob "Migrate TACF to PDOS" -l "PDOS Tasks" -a admin_id -a admin_passwd -a pdos_branch -a user_suffix -a group_suffix -a create_templates -a process_resource -a process_registry -a report_only

wruntask -t "Migrate TACF to PDOS" -l "PDOS Tasks" -a admin_id -a admin_passwd -a pdos_branch -a user_suffix -a group_suffix -a create_templates -a process_resource -a process_registry -a report_only -h task_endpoint
```

where:

- `admin_id` Indicates the Tivoli Policy Director administrator ID.
- `admin_passwd` Indicates the Tivoli Policy Director administrator’s password.
- `pdos_branch` Specifies the Tivoli Policy Director for Operating Systems profile name.
- `user_suffix` Specifies the LDAP user suffix.
- `group_suffix` Specifies the LDAP group suffix.
- `create_templates` Create objects for resources created with Tivoli Access Control Facility
editres or newres commands. If this option is set to FALSE, Tivoli Policy Director for Operating Systems will not migrate Tivoli Access Control Facility objects that were created with the Tivoli Access Control Facility editres command. This value must be either TRUE or FALSE.

process_resource
Specifies whether to import policy information. This value must be either TRUE or FALSE.

process_registry
Specifies whether to import user/group information. This value must be either TRUE or FALSE.

report_only
Specifies whether to simply report the migration script, or to execute it. This value must be either TRUE or FALSE.

task_endpoint
Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.

Purge PDOS Hostname Cache

This task allows the administrator to remove entries from the IP address/hostname translation cache used by Tivoli Policy Director for Operating Systems.

Two non-exclusive options are available—removing all stale entries and removing entries by name. Entries to be removed are specified by hostname or IP address in a comma-separated list. If this list contains the special value *, all entries will be removed. If the list is empty, no entries will be removed.

The following job dialog corresponds to the Purge PDOS Hostname Cache task:

Use the following steps to perform this task:

1. Enter a comma-separated list of the IP addresses and/or hostnames that are to be removed from the cache. The value * can be used to indicate all cache entries.

2. If cache entries that have exceeded their expiration date should be removed, check Remove all stale entries from database.

3. Click the Execute and Close button to perform the task.

Syntax for wrunjob and wruntask

Use the following arguments, in the order shown, to run this task from the command line or a script using wrunjob or wruntask:

wrunjob "Purge PDOS Hostname Cache" –l "PDOS Tasks" –a remove_entries –a remove_stale

wruntask –t "Purge PDOS Hostname Cache" –l "PDOS Tasks" –a remove_entries –a remove_stale –h task_endpoint
where:

remove_entries Indicates which entries to remove from the cache. If this value is the empty string, no entries will be removed.

remove_stale Indicates whether stale entries should be removed. This value must be either TRUE or FALSE.

task_endpoint Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.

### Query PDOS Login and Password Policy

This task allows the administrator to generate reports related to Tivoli Policy Director for Operating Systems Login and Password Policy. Two types of reports can be generated:

- Reports can be created that show the status of user accounts or that show all details related to a user’s record in the Tivoli Policy Director for Operating Systems Login Activity Database.
- Reports can be created detailing the default Login and Password Policy for all users or the policy for specific users.

The following job dialog corresponds to the **Query PDOS Login and Password Policy** task:

Use the following steps to perform this task:

1. If you wish to generate a user status report, click **Generate user status report** and specify the reporting requirements.
2. A comma-separated list of users whose status should be queried can be specified.
3. For login and password information, click **Display login and password policy**.
4. A comma-separated list of users whose login and password policy should be reported can be specified.

5. Click the **Execute and Close** button to perform the task.

**Syntax for wrunjob and wruntask**

Use the following arguments, in the order shown, to run this task from the command line or a script using **wrunjob** or **wruntask**:

```bash
wrunjob "Query PDOS Login and Password Policy" -l "PDOS Tasks" -a
  generate_report -a detailed -a enabled -a disabled -a report_users -a display_policy -a policy_users
wruntask -l "Query PDOS Login and Password Policy" -l "PDOS Tasks" -a
  generate_report -a detailed -a enabled -a disabled -a report_users -a display_policy -a policy_users -h task_endpoint
```

where:

- **generate_report**
  Indicates whether or not to create a report showing the user entries in the PDOS Login Activity Database. This value must be either **TRUE** or **FALSE**.

- **detailed**
  Specifies if the user status report should include detailed information on each user entry, or simply its status. This value must be either **TRUE** or **FALSE**.

- **enabled**
  If this parameter is set to **TRUE**, only unlocked (**enabled**) user entries will be shown. If this parameter is set to **TRUE**, **disabled** cannot also be set to **TRUE**.

- **disabled**
  If this parameter is set to **TRUE**, only locked (**disabled**) user entries will be shown. If this parameter is set to **TRUE**, **enabled** cannot also be set to **TRUE**.

- **report_users**
  A comma-separated list of users can be specified. Only the user entries from the users in the list will be reported.

- **display_policy**
  Indicates whether or not to create a report showing the Tivoli Policy Director for Operating Systems Login and Password Policy. This value must be either **TRUE** or **FALSE**.

- **policy_users**
  A comma-separated list of users can be specified. Only the Tivoli Policy Director for Operating Systems Login and Password Policy for the users in the list will be reported. If this parameter is blank, then the default Tivoli Policy Director for Operating Systems Login and Password Policy will be reported.

- **task_endpoint**
  Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.
Query PDOS Server State

This task allows the administrator to individually determine the current state of the daemons comprising a running Tivoli Policy Director for Operating Systems instance.

The following job dialog corresponds to the **Query PDOS Server State** task:

Use the following steps to perform this task:

1. Select the daemons on which to report status.
2. Click the **Execute and Close** button to perform the task.

**Syntax for wrunjob and wruntask**

Use the following arguments, in the order shown, to run this task from the command line or a script using `wrunjob` or `wruntask`:

```
# wrunjob
wrunjob "Query PDOS Server State" -l "PDOS Tasks" -a query_pdosd -a query_pdosaudittd -a query_pdoswdd

# wruntask
wruntask -t "Query PDOS Server State" -l "PDOS Tasks" -a query_pdosd -a query_pdosaudittd -a query_pdoswdd -h task_endpoint
```

where:

- `query_pdosd` Indicates whether the state of the PDOSD daemon should be reported. It must be either **TRUE** or **FALSE**.
- `query_pdosaudittd` Indicates whether the state of the PDOSAUDITD daemon should be reported. It must be either **TRUE** or **FALSE**.
- `query_pdoswdd` Indicates whether the state of the PDOSWDD daemon should be reported. It must be either **TRUE** or **FALSE**.
- `task_endpoint` Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.

**Query PDOS TCB**

This task allows the administrator to query the trust status of objects in the Tivoli Policy Director for Operating Systems Trusted Computing Base (TCB).

A comma-separated list of objects on which to report the trust status must be specified. Object names must be provided as absolute paths. Three special list values can be used: * specifies all objects in the TCB, **AnyTrusted** specifies all trusted objects in the TCB, and **AnyUntrusted** specifies all untrusted objects in the TCB.
The following job dialog corresponds to the **Query PDOS TCB** task:

![Query PDOS TCB](image1)

Use the following steps to perform this task:

1. Specify any general categories of file system objects to report using the **Report all trusted/untrusted files** options.
2. Optionally, select any specific file system objects to be reported.
3. Click the **Execute and Close** button to perform the task.

**Syntax for wrunjob and wruntask**

Use the following arguments, in the order shown, to run this task from the command line or a script using `wrunjob` or `wruntask`:

**wrunjob** "Query PDOS TCB" ~l "PDOS Tasks" ~a query_objects

**wruntask** ~t "Query PDOS TCB" ~l "PDOS Tasks" ~a query_objects ~h task_endpoint

where:

- **query_objects** Specifies a list of objects on which to report the trust status. Three special list values can be used: * specifies all objects in the TCB, **AnyTrusted** specifies all trusted objects in the TCB, and **AnyUntrusted** specifies all untrusted objects in the TCB
- **task_endpoint** Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.

**Restore PDOS Database**

This task allows the administrator to restore a specified Tivoli Policy Director for Operating Systems backup file. The path to the backup file may be absolute or relative. If the path is relative, it is assumed to be relative to `/var/pdos/pdosbkap`.

The following job dialog corresponds to the **Restore PDOS Database** task:

![Restore PDOS Database](image2)

Use the following steps to perform this task:

1. Enter the name of a backup file to restore. The name can be either an absolute or relative path; if relative, it is assumed relative to `/usr/pdos/pdosbkap`.
2. Click the **Execute and Close** button to perform the task.
Syntax for wrunjob and wruntask

Use the following arguments, in the order shown, to run this task from the command line or a script using wrunjob or wruntask:

\texttt{wrunjob "Restore PDOS Database" –l "PDOS Tasks" –a filename}

\texttt{wruntask –t "Restore PDOS Database" –l "PDOS Tasks" –a filename –h task_endpoint}

where:

- \texttt{filename} Specifies the name of a backup file to restore.
- \texttt{task_endpoint} Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.

Set PDOS Server Audit Level

This task allows the administrator to set the audit levels of the Tivoli Policy Director for Operating Systems instance.

The audit level is specified as a mask with the possible masked events being permitted accesses, denied accesses, administrative events, Tivoli Policy Director for Operating Systems updates, permitted logins, denied logins, process invocations, and accesses to protected files. Auditing can be made verbose. Tivoli Policy Director for Operating Systems may also be placed into \texttt{warning mode}, where accesses normally denied will be granted, but an audit record will be generated indicating the bypass. In addition, a modifier indicating how and when the change occurs must be supplied. Valid modifiers are \texttt{Permanent}, \texttt{Temporary}, and \texttt{Deferred}. \texttt{Permanent} indicates the change will be effective immediately and persist across a restart of the instance. \texttt{Temporary} indicates the change will be effective immediately but will not persist across a restart of the instance. \texttt{Deferred} indicates the change will not take effect until a restart of the instance.

The following job dialog corresponds to the Set PDOS Server Audit Level task:

Use the following steps to perform this task:

1. Select the audit events that should be enabled. Only events of the specified types will appear in the audit log.

2. Check \texttt{Run in warning mode} if Tivoli Policy Director for Operating Systems should not enforce security policy, but only log violations of the policy.
3. Select how the auditing changes should be applied. **Deferred** changes will not take effect immediately; they take effect on the next restart of Tivoli Policy Director for Operating Systems. **Permanent** changes take effect immediately and will persist even after restarting Tivoli Policy Director for Operating Systems. **Temporary** changes take effect immediately but will not persist after Tivoli Policy Director for Operating Systems is restarted.

4. Click the **Execute and Close** button to perform the task.

**Syntax for wrunjob and wruntask**

Use the following arguments, in the order shown, to run this task from the command line or a script using **wrunjob** or **wruntask**:

```
wrunjob "Set PDOS Server Audit Level" -l "PDOS Tasks" -a audit_permit -a audit_deny -a audit_admin -a audit_info -a logpermit -a logdeny -a trace_exec -a trace_file -a warning_mode -a change_type
```

```
wruntask -t "Set PDOS Server Audit Level" -l "PDOS Tasks" -a audit_permit -a audit_deny -a audit_admin -a audit_info -a logpermit -a logdeny -a trace_exec -a trace_file -a warning_mode -a change_type -h task_endpoint
```

where:

- **audit_permit** Indicates that auditing of permitted accesses should be done. This value must be either **TRUE** or **FALSE**.
- **audit_deny** Indicates that auditing of denied accesses should be done. This value must be either **TRUE** or **FALSE**.
- **audit_admin** Indicates that auditing of administrative events should be done. This value must be either **TRUE** or **FALSE**.
- **audit_info** Indicates that auditing of automatic actions taken within Tivoli Policy Director for Operating Systems, such as receiving valid policy updates, should be done. This value value must be either **TRUE** or **FALSE**.
- **logpermit** Indicates that auditing of all authorization decisions that permit a login should be done. This value must be either **TRUE** or **FALSE**.
- **logdeny** Indicates that auditing of all authorization decisions that deny a login should be done. This value must be either **TRUE** or **FALSE**.
- **trace_exec** Indicates that auditing of all process invocations should be done. This value must be either **TRUE** or **FALSE**.
- **trace_file** Indicates that auditing of all accesses to protected files should be done. This value must be either **TRUE** or **FALSE**.
- **warning_mode** Indicates that Tivoli Policy Director for Operating Systems should run in warning mode. This value must be either **TRUE** or **FALSE**.
- **change_type** Indicates the type of change. This value must be one of **Permanent**, **Temporary**, or **Deferred**.
- **task_endpoint** Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.
**Set PDOS Server Trace Level**

This task allows the administrator to set the current tracing levels of the daemons comprising the Tivoli Policy Director for Operating Systems instance and is intended to be used in conjunction with Tivoli Customer Support. The entry of random strings for trace levels is not recommended.

The following job dialog corresponds to the **Set PDOS Server Trace Level** task:

![Set PDOS Server Trace Level dialog](image)

Use the following steps to perform this task:

1. Enter serviceability trace strings for the desired daemons.
2. Click the **Execute and Close** button to perform the task.

**Syntax for wrunjob and wruntask**

Use the following arguments, in the order shown, to run this task from the command line or a script using **wrunjob** or **wruntask**:

```bash
wrunjob "Set PDOS Server Trace Level" -l "PDOS Tasks" -a pdosd_trace -a pdosaudited_trace -a pdoswdd_trace
wruntask -t "Set PDOS Server Trace Level" -l "PDOS Tasks" -a pdosd_trace -a pdosaudited_trace -a pdoswdd_trace -h task_endpoint
```

where:

- **pdosd_trace** Indicates the change to make to the trace level of the PDOSD daemon. If the empty string is specified, the daemon’s trace level will remain unchanged.

- **pdosaudited_trace** Indicates the change to make to the trace level of the PDOSAUDITD daemon. If the empty string is specified, the daemon’s trace level will remain unchanged.

- **pdoswdd_trace** Indicates the change to make to the trace level of the PDOSWDD daemon. If the empty string is specified, the daemon’s trace level will remain unchanged.
task_endpoint  Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.

Setup TEC Event Server for PDOS

The Setup TEC Event Server for PDOS task automatically configures the Tivoli Enterprise Console event server to recognize Tivoli Policy Director for Operating Systems events. The task and job are available only if both Tivoli Policy Director for Operating Systems Enterprise Console Integration and Tivoli Enterprise Console Server are installed. For more information about installing the Tivoli Enterprise Console logfile adapter on a Tivoli Policy Director for Operating Systems endpoint to send Tivoli Policy Director for Operating Systems events, see Chapter 8, “Integrating with Tivoli Enterprise Console” on page 197. For more information about Tivoli Enterprise Console, see the Tivoli Enterprise Console User’s Guide.

By default, this job will run on the Tivoli Enterprise Console event server (because this task should only be run on the Tivoli Enterprise Console event server). The following job dialog corresponds to the Setup TEC Event Server for PDOS job and task:

Use the following steps to perform this task:

1. Select one or two Tivoli Policy Director for Operating Systems integration targets. The available selections are Integrate with Tivoli Enterprise Console and Integrate with Tivoli Risk Manager. The task will fail if None is selected.

2. Specify whether you want this task to create a new rule base or add information to an existing rule base.
   - If you create a new rule base, you must provide the following additional information:
**New Rule Base name.** Specifies a name for the new rule base. If a rule base already exists with this name, an error will occur. The default rule base name is **PDOS**.

**Rule Base to clone.** Specifies the name of an existing rule base from which to copy configuration files. The default name is **Default**. If **Integrate with Tivoli Risk Manager** is selected, the rule base to clone from must be installed and configured by Tivoli Risk Manager. For more information, see the **Tivoli Risk Manager User’s Guide**.

**Path for new Rule Base.** Specifies the directory on the Tivoli Enterprise Console server in which the new rule base’s configuration files are to be stored. If this path does not exist, it will be created.

- If you choose to add to an existing rule base, you must specify a name for the existing rule base. The default rule base name is **PDOS**. If the rule base you specify does not already exist, an error will occur.

3. Select the name of the event console to configure. Selecting a console from the list causes the Tivoli Policy Director for Operating Systems event group (through which all Tivoli Policy Director for Operating Systems related events are accessible) to be added to the selected console. If you choose **None**, you will not receive any Tivoli Policy Director for Operating Systems events at any event console.

4. Click the **Set and Close** button to perform the task.

### Syntax for wrunjob and wruntask

Use the following arguments, in the order shown, to run this task from the command line or a script using **wrunjob** or **wruntask**:

**wrunjob** "Setup TEC Event Server for PDOS" -l "PDOS Tasks" -a "IntegrateTEC" -a "IntegrateRM" -a "NeworExisting" -a "ExistingRuleBase" -a "NewRuleBase" -a "CloneRuleBase" -a "RuleBasePath" -a "EventConsole"

**wruntask** -t "Setup TEC Event Server for PDOS" -l "PDOS Tasks" -a "IntegrateTEC" -a "IntegrateRM" -a "NeworExisting" -a "ExistingRuleBase" -a "NewRuleBase" -a "CloneRuleBase" -a "RuleBasePath" -a "EventConsole" -h task_endpoint

where:

- **IntegrateTEC** Specifies whether to integrate with Tivoli Enterprise Console. Valid values are **on** (integrate with Tivoli Enterprise Console) and **off** (do not integrate).

- **IntegrateRM** Specifies whether to integrate with Tivoli Risk Manager. Valid values are **on** (integrate with Tivoli Risk Manager) and **off** (do not integrate).

- **NeworExisting** Specifies whether to create a new rule base or use an existing rule base. Valid values are **new** (create new database) and **exist** (use an existing database). If you specify **new**, you must also specify a name for **NewRuleBase**. If you specify **exist**, you must also specify a name for **ExistingRuleBase**.

- **ExistingRuleBase** Specifies the name of the rule base in which to add information. If the **exist** option is specified, you must supply the name of an existing database. The default name is **PDOS**.
NewRuleBase  Specifies a name for the new rule base. If a rule base already exists with this name, an error will occur. If the **new** option is specified, you must supply a name for the new database.

CloneRuleBase  Specifies the name of an existing rule base from which to copy configuration files. The default name is **Default**.

RuleBasePath  Specifies the full path of the directory on the Tivoli Enterprise Console server in which the new rule base’s configuration files are to be stored. If this path does not exist, it will be created.

EventConsole  Specifies the name of the event console to be configured with this rule base.

task_endpoint  Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.

**Note:** If you choose integration with Tivoli Risk Manager, and the Tivoli Enterprise Console event server in your environment is running on a Microsoft Windows NT system, you must customize the `$BINDIR/RISKMGR/corr/riskmgr_baroc.lst` file to include the `pdosrm.baroc` file. Include the `pdos.baroc` file also if the event server should send events to the Tivoli Enterprise Console as well. Make your changes effective by entering the following commands using the bash shell from the event server after running this task:

```
cd $BINDIR/RISKMGR/corr
cp ../../../generic_unix/TME/PDOSTASKS/pdosrm.baroc ./tec
cp ../../../generic_unix/TME/PDOSTASKS/pdos.baroc ./tec
./rmcorr_cfg -update
```

**Show PDOS Auditing Configuration**

This task allows you to review the parameters related to Tivoli Policy Director for Operating Systems auditing. When you run this task from the desktop, the audit parameters are displayed in a window. Displayed output includes the maximum file size of an audit log and how often, in seconds, audit log buffers are flushed to disk. If a parameter’s value is blank, it has never been explicitly configured and is using its default value.

**Syntax for wrunjob and wruntask**

Use the following arguments, in the order shown, to run this task from the command line or a script using **wrunjob** or **wruntask**:

```
wrunjob "Show PDOS Auditing Configuration" -l "PDOS Tasks"
wruntask -t "Show PDOS Auditing Configuration" -l "PDOS Tasks" -h task_endpoint
```

where:

```
task_endpoint  Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.
```
Show PDOS Auditors/Administrators

This task can be used to display users who have Auditor or Administrator privileges. To be an Auditor, the user must be a member of both the osseal-auditors Tivoli Policy Director group and the ossaudit UNIX group. To be an Administrator, the user must be a member of the osseal-admin Tivoli Policy Director group and a member of the osseal UNIX group.

The Show Auditors and Show Administrators checkboxes are used to select which UNIX and Tivoli Policy Director groups to display. To run this task, a Tivoli Policy Director Administrator’s ID and password must be specified.

The following job dialog corresponds to the Show PDOS Auditors/Administrators task:

Use the following steps to perform this task:

1. You must specify the first two fields.
2. Select the types of Tivoli Policy Director for Operating Systems users you want to display.
3. Click the Execute and Close button to perform the task.

Syntax for wrunjob and wruntask

Use the following arguments, in the order shown, to run this task from the command line or a script using wrunjob or wruntask:

wrunjob "Show PDOS Auditors/Administrators" –l "PDOS Tasks" –a pd_admin_id –a pd_admin_passwd –a show_auditors –a show_admins

wruntask –t "Show PDOS Auditors/Administrators" –l "PDOS Tasks" –a pd_admin_id –a pd_admin_passwd –a show_auditors –a show_admins –h task_endpoint

where:

pd_admin_id
Specifies the name of a Tivoli Policy Director administrative account that will be used to generate the report. Completion of this parameter is required.

pd_admin_passwd
Specifies the password of the administrative account. Completion of this parameter is required.

show_auditors
If this parameter is set to TRUE, the members of the Tivoli Policy Director osseal-auditors group and the UNIX osseal group are displayed. This value must be either TRUE or FALSE.
show_admins
If this parameter is set to TRUE, the members of the Tivoli Policy Director osseal-admin group and the UNIX ossadmin group are displayed. This value must be either TRUE or FALSE.

task_endpoint
Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.

Show PDOS Caching Configuration
This task allows you to review the parameters related to Tivoli Policy Director for Operating Systems’ internal caches. When you run this task from the desktop, the cache parameters are displayed in a window. Displayed output includes how often (in minutes) to refresh cached administrator credentials, how often (in minutes) to refresh cached user credentials, how long (in minutes) to cache unaccessed user credentials, whether hostname caching is turned on, and whether username caching is turned on. If a parameter’s value is blank, it has never been explicitly configured and is using its default value.

Syntax for wrunjob and wruntask
Use the following arguments, in the order shown, to run this task from the command line or a script using wrunjob or wruntask:

erunjob "Show PDOS Caching Configuration" –l "PDOS Tasks"
eruntask –t "Show PDOS Caching Configuration" –l "PDOS Tasks" –h task_endpoint

where:

task_endpoint Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.

Show PDOS Logging Configuration
This task allows you to review the parameters related to logging for the Tivoli Policy Director for Operating Systems daemons, PDOSD, PDOSWDD, and PDOSAUDITD. When you run this task from the desktop, the logging parameters are displayed in a window. Displayed output includes the number of log files and the maximum number of entries in the log files. If a parameter’s value is blank, it has never been explicitly configured and is using its default value.

Syntax for wrunjob and wruntask
Use the following arguments, in the order shown, to run this task from the command line or a script using wrunjob or wruntask:

wrunjob "Show PDOS Logging Configuration" –l "PDOS Tasks"
wruntask –t "Show PDOS Logging Configuration" –l "PDOS Tasks" –h task_endpoint

where:

task_endpoint Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.
Show PDOS Server Audit Level

This task allows you to review the parameters related to the Tivoli Policy Director for Operating Systems instance’s auditing level. When you run this task from the desktop, these parameters are displayed in a window. Displayed output includes the current audit level (permitted accesses, denied accesses, and administrative events) and whether Tivoli Policy Director for Operating Systems is in warning mode, where all accesses are granted but accesses that would normally be denied generate audit records. Also, the configured audit levels are displayed. Configured audit levels will be in effect after the next restart of Tivoli Policy Director for Operating Systems. If a parameter’s value is blank, it has never been explicitly configured and is using its default value.

Syntax for wrunjob and wruntask

Use the following arguments, in the order shown, to run this task from the command line or a script using wrunjob or wruntask:

wrunjob "Show PDOS Server Audit Level" –l "PDOS Tasks"
wruntask –t "Show PDOS Server Audit Level" –l "PDOS Tasks" –h task_endpoint

where:

task_endpoint Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.

Show PDOS Server Configuration

This task allows you to review miscellaneous parameters for the Tivoli Policy Director for Operating Systems server. When you run this task from the desktop, the parameters are displayed in a window. If a parameter’s value is blank, it has never been explicitly configured and is using its default value. Displayed output includes the following information.

- the port Tivoli Policy Director for Operating Systems uses to receive notifications of policy updates
- how often, in minutes, to poll for policy updates
- whether system and password login restrictions are enabled
- the number of kernel threads used to handle authorization requests
- whether Tivoli Policy Director for Operating Systems is configured to start automatically at system startup
- the policy branch name

Syntax for wrunjob and wruntask

Use the following arguments, in the order shown, to run this task from the command line or a script using wrunjob or wruntask:

wrunjob "Show PDOS Server Configuration" –l "PDOS Tasks"
wruntask –t "Show PDOS Server Configuration" –l "PDOS Tasks" –h task_endpoint

where:
Show PDOS TCB Configuration

This task allows you to review parameters related to the Tivoli Policy Director for Operating Systems Trusted Computing Base (TCB). When you run this task from the desktop, the parameters are displayed in a window. Displayed output includes the number of threads used to monitor TCB objects, the interval (in seconds) between TCB monitoring runs, and the maximum number of bytes in megabytes from a file to use in a checksum (TCB signature). If a parameter’s value is blank, it has never been explicitly configured and is using its default value.

Syntax for wrunjob and wruntask

Use the following arguments, in the order shown, to run this task from the command line or a script using wrunjob or wruntask:

```bash
wrunjob "Show PDOS TCB Configuration" -l "PDOS Tasks"
wruntask -t "Show PDOS TCB Configuration" -l "PDOS Tasks" -h task_endpoint
```

where:

- `task_endpoint` Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.

Start TEC Adapter

This task allows the administrator to start the Tivoli Policy Director for Operating Systems Tivoli Enterprise Console daemon and the Tivoli Enterprise Console logfile adapter. This task will not start the processes if they are already running.

Syntax for wrunjob and wruntask

Use the following arguments, in the order shown, to run this task from the command line or a script using wrunjob or wruntask:

```bash
wrunjob "Start TEC Adapter" -l "PDOS Tasks"
wruntask -t "Start TEC Adapter" -l "PDOS Tasks" -h task_endpoint
```

where:

- `task_endpoint` Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.

Stop TEC Adapter

This task allows the administrator to stop the Tivoli Policy Director for Operating Systems Tivoli Enterprise Console daemon and the Tivoli Enterprise Console logfile adapter.

Syntax for wrunjob and wruntask

Use the following arguments, in the order shown, to run this task from the command line or a script using wrunjob or wruntask:

```bash
wrunjob "Stop TEC Adapter" -l "PDOS Tasks"
wruntask -t "Stop TEC Adapter" -l "PDOS Tasks" -h task_endpoint
```

where:

- `task_endpoint` Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.
wrunjob "Stop TEC Adapter" –l "PDOS Tasks"
wruntask –t "Stop TEC Adapter" –l "PDOS Tasks" –h task_endpoint

where:

(task_endpoint) Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.

**Subscribe PDOS Endpoints**

This task creates a list of all managed nodes and endpoints that have had Tivoli Policy Director for Operating Systems installed on them. These managed notes and endpoints are then added to the subscriber list of the local PDOS policy manager.

**Syntax for wrunjob and wruntask**

Use the following arguments, in the order shown, to run this task from the command line or a script using wrunjob or wruntask:

wrunjob "Subscribe PDOS Endpoints" –l "PDOS Tasks"
wruntask –t "Subscribe PDOS Endpoints" –l "PDOS Tasks" –h task_endpoint

where:

(task_endpoint) Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple names with spaces.

**Update PDOS Hostname Cache**

This task allows the administrator to add entries to the IP address/hostname translation cache used by Tivoli Policy Director for Operating Systems, as well as to force a refresh of all cache entries.

Two non-exclusive options are available—refreshing all cache entries and adding new cache entries. New entries to add are specified by hostname or IP address in a comma-separated list. If this list is empty, no entries will be added. When adding entries, a time-to-live may be provided indicating how many seconds the entry will remain valid in the cache. If omitted, a reasonable default is used.

The following job dialog corresponds to the **Update PDOS Hostname Cache** task:

Use the following steps to perform this task:

1. Enter a comma-separated list of hostnames/IP addresses to add to the hostname cache. If empty, no new entries are added.
2. Enter the number of seconds that newly added entries remain valid in the Cache timeout field.

3. If all entries currently in the cache should be refreshed, check Refresh all database entries.

4. Click the Execute and Close button to perform the task.

**Syntax for wrunjob and wruntask**

Use the following arguments, in the order shown, to run this task from the command line or a script using wrunjob or wruntask:

```
wrunjob "Update PDOS Hostname Cache" -l "PDOS Tasks" -a add_entries -a entry_ttl -a refresh
wruntask -t "Update PDOS Hostname Cache" -l "PDOS Tasks" -a add_entries -a entry_ttl -a refresh -h task_endpoint
```

where:

- `add_entries` Indicates which entries to add to the cache. If this value is the empty string, no new entries are added.

- `entry_ttl` Indicates the length of time (in seconds) any newly added cache entries will remain valid. If this value is the empty string, a default value is used.

- `refresh` Indicates whether all cache entries should be refreshed. This value must be either TRUE or FALSE.

- `task_endpoint` Specifies the name of the profile manager, managed node, or endpoint on which to run the task. You can specify more than one name; separate multiple multiple names with spaces.
Auditing

Tivoli Policy Director for Operating Systems provides extensive auditing capabilities that permit you to track authorization access decisions made to protected resources as well as to monitor activity of an administrative nature, such as the starting and stopping of the daemons. This chapter provides information about the types of events that can be audited, the format of the resulting log entries, and how to view the log entries.

Auditing Authorization Decisions

You can audit authorization access decisions for specific resources by enabling resource based auditing. Use Protected Object Policy (POP) access controls to enable resource based auditing. To enable it, do the following steps:

1. Create a POP.
2. Set the audit level attribute to permit, deny, or both.
3. Attach the POP to the resources you want audited.

Audit records for authorization access decisions are also generated if the permit or deny level is set in the global audit level. The auditing levels for the global audit level and the resource audit level are cumulative. For example, if the global audit level is set to deny, and a resource has a POP attached to it with an audit level of permit, every authorization decision for access to that resource will be audited.

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 results in the generation of audit records for all login authorization decisions that permit the login action. Setting the logindeny global audit level results 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 separately from other authorization decisions.

If warning mode is enabled, audit records are generated for authorization access decisions that get changed from deny to permit regardless of the current audit level. Use POP access controls to enable resource based warning mode. Also, similar to auditing, there is a global warning mode that can be turned on. For information about using the `pdoscfg` and `pdosct1` commands to enable the global auditing and warning mode and the `pdadmin` command for setting up POP access controls to enable resource based auditing and warning mode, see "Using Auditing to Verify Policy" on page 78 and "Using Warning Mode to Verify Policy" on page 77.
Auditing Administrative Activity

You can audit administrative activity by setting the admin audit level in the global audit level. The admin audit level causes Tivoli Policy Director for Operating Systems to generate audit records for events such as starting and stopping the Tivoli Policy Director for Operating Systems daemons, loss of connectivity with the Tivoli Policy Director User Registry, TCB-related activity such as a file being marked untrusted by the TCB monitoring function, and the detection of invalid policy. The admin audit level also causes the generation of audit records for events related to a user login account being enabled or disabled when login activity policy is being enforced.

Auditing Trace Events

Tivoli Policy Director for Operating Systems supports the auditing of 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 results in the generation of an audit record for each exec() system call. These records are generated regardless of whether the program being executed is protected by Tivoli Policy Director for Operating Systems policy or not. Setting the trace_file global audit level results in the generation of an audit record for each access to a file system resource that is protected by Tivoli Policy Director for Operating Systems policy.

Note that trace_exec and trace_file audit records are generated only for processes that descend from a login event that was detected by Tivoli Policy Director for Operating Systems. The following processes do not generate trace_exec or trace_file audit records:

- Processes that are started or descended from the UNIX init process during system boot.
- Processes that are active before Tivoli Policy Director for Operating Systems and its processes are started.
- Processes that are running programs that are registered as Immune-Programs in the Trusted Computing Base (TCB).

Note that the immunity of an Immune-Program listed in the TCB is not inherited by other programs that the immune program execs. However, a program made exempt using the pdosexempt command can pass on its immunity to its child processes. This immunity allows a script or program to bypass Tivoli Policy Director for Operating Systems policy enforcement. Care should be taken when using either Immune-Programs or the pdosexempt command to avoid recording trace audit events.

In addition, trace_exec and trace_file audit records are only generated if the request is handled at the operating system service level. If an operation is handled at the application level, such as within a command shell, Tivoli Policy Director for Operating Systems might not be aware of the activity and would not generate an audit record for it.

Global Audit Levels

The type of auditing information collected can be tailored based on your needs. The following global audit levels are supported.

Table 41. Global Audit Levels

<table>
<thead>
<tr>
<th>Audit Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>Turns off all auditing. This is the default value.</td>
</tr>
</tbody>
</table>
### Table 41. Global Audit Levels (continued)

<table>
<thead>
<tr>
<th>Audit Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>permit</td>
<td>Tracks all authorization decisions that permit access to a protected resource.</td>
</tr>
<tr>
<td>deny</td>
<td>Tracks all authorization decisions that deny access to a protected resource.</td>
</tr>
<tr>
<td>loginpermit</td>
<td>Tracks all login authorization decisions that permit the login.</td>
</tr>
<tr>
<td>logindeny</td>
<td>Tracks all login authorization decisions that deny the login.</td>
</tr>
</tbody>
</table>
| admin         | Tracks activity of an administrative nature. For example, if the global audit level has the admin level set, a log entry is created each time one of the Tivoli Policy Director for Operating Systems daemons is started or stopped.  
| trace_exec    | Tracks program invocations initiated by exec() that occur in processes that descend from a login event that was detected by Tivoli Policy Director for Operating Systems. |
| trace_file    | Tracks all accesses to protected files. Tracking occurs whether or not  
|               | - resource auditing is enabled, or  
|               | - global permit or deny auditing is enabled  
|               | Tracking only occurs for those processes that descend from a login event that was detected by Tivoli Policy Director for Operating Systems. |
| all           | Enables all of the following audit levels:  
|               | permit  
|               | deny  
|               | loginpermit  
|               | logindeny  
|               | admin  
| info          | Tracks actions that are done automatically, such as receiving valid policy updates.             |
| verbose       | Enables all of the following audit levels:  
|               | permit  
|               | deny  
|               | loginpermit  
|               | logindeny  
|               | admin  
|               | info  

### The Audit Log File

The PDOSAUDITD daemon manages the Tivoli Policy Director for Operating Systems audit log file. Details on the operation and configuration of the daemon can be found in "The PDOSAUDITD Audit Daemon" on page 56.

The active audit log file is /var/pdos/audit/audit.log. Audit records are written to the audit log in binary format. Based on the settings of the PDOSAUDITD daemon, the audit log is archived when it reaches a configured maximum size and logging continues in a new audit.log file in the same directory. The name of the archived file has a timestamp appended to it, audit.log/YYYY-MM-DD-HH-MM-SS, and resides in the same directory as the active log file.
The audit.log file is the input to the PDOSTECD Tivoli Enterprise Console daemon. If the file is not available, the PDOSTECD daemon shuts down. After making the audit.log file available again, restart the daemon. For more information, see “The PDOSTECD Tivoli Enterprise Console Daemon” on page 59.

Viewing Audit Logs

Because audit logs are written to disk in binary format, the Audit View Tool, pdosaudview, must be used to view them. The complete syntax of the command can be found in “pdosaudview” on page 148. By default, the Audit View Tool writes its output to a text file named text.log in the /var/pdos/audit directory.

The Audit View Tool displays the records in the audit log in one of three formats: concise, keyvalue, and verbose. The content of the records produced in these three formats is described later in this chapter, in “Audit Log Record Types” on page 137.

Concise Format

In concise format, the output consists of one physical line of output per log record with the data separated by commas. The fields are positional and if a field does not have a value or if the field does not pertain to the particular event then just a comma is displayed. There are no field or column headings. Concise output would look similar to the following. Note that the command output illustrated here might be truncated to fit the page.

Mon 29 Oct 2001 04:35:27 PM CST,28,P,1,TraceFile,ossyes,ossyes,Trace,wr,,/export/home/ossyes,.sh_history,1235,
Mon 29 Oct 2001 04:35:27 PM CST,7,P,1,File,ossyes,ossyes,Check Access,wr,34,bvt/File/export/home/ossyes,.sh_hist...
Mon 29 Oct 2001 04:35:38 PM CST,7,P,1,NetOutgoing,ossyes,ossyes,Check Access,C,34,bvt,NetOutgoing/*/tcp/te...
Mon 29 Oct 2001 04:35:44 PM CST,17,A,1,Policy,root,root,Apply,,,,,,,,,,,831,,,,,,,,,14711,S,,0
Mon 29 Oct 2001 04:35:44 PM CST,17,A,1,Policy,root,root,Apply,,,,,,,,,,,831,opt/pdos/bin/pdosd/opt/pdos/bin/
Mon 29 Oct 2001 04:35:45 PM CST,6,P,1,Logout,ossyes,,Logout,1235,goblue.tivoli.com,0
Mon 29 Oct 2001 04:35:45 PM CST,7,P,1,File,root,root,Check Access,r,34,bvt,File/opt/pdos,/usr/lib/liblpm.so

Use the Fixed Position column in the audit record format tables to locate information on what each comma-delimited field represents.

Keyvalue Format

In keyvalue format, the output consists of one physical line of output per log record, as in concise format, however each field is preceded by a 1 to 4 character keyword and equal sign (=) identifying it. In other words, the output is provided in keyword=value format. If a field does not apply to a particular event, it is not shown in the output. Keyvalue output would look similar to the following. Note that the command output illustrated here might be truncated to fit the page.

TS=Mon 29 Oct 2001 04:35:27 PM CST,E=28,V=P,R=1,RT=TraceFile,AN=ossyes,AEN=ossyes,A=Trace,P=wr,PRS=/export/home/ossyes,.sh_history,1235,
TS=Mon 29 Oct 2001 04:35:27 PM CST,E=7,V=P,R=1,RT=File,AN=ossyes,AEN=ossyes,A=Check Access,P=wr,Q=34,PBN=bvt,PON=
TS=Mon 29 Oct 2001 04:35:38 PM CST,E=7,V=P,R=1,RT=NetOutgoing,AN=ossyes,AEN=ossyes,A=Check Access,P=C,Q=34,PBN=
TS=Mon 29 Oct 2001 04:35:44 PM CST,E=17,V=A,R=1,RT=Policy,AN=root,AEN=root,A=Apply,APID=831,PVN=14711,O=S,UQ=
TS=Mon 29 Oct 2001 04:35:44 PM CST,E=17,V=A,R=1,RT=Policy,AN=root,AEN=root,A=Apply,APID=831,RPDN=/opt/pdos/bin/
TS=Mon 29 Oct 2001 04:35:45 PM CST,E=6,V=P,R=1,RT=Logout,AN=ossyes,A=Logout,APID=1235,LL=goblue.tivoli.com,UQ=
TS=Mon 29 Oct 2001 04:35:45 PM CST,E=7,V=P,R=1,RT=File,AN=root,AEN=root,A=Check Access,P=r,Q=34,PBN=bvt,PON=F

Use the Keyword column in the audit record format tables to determine what the indicated field represents.

This is the default format of the pdosaudview command unless the output is written to stdout using the -l option.

Verbose Format

In verbose format, the output consists of several lines of output per log record with each value preceded with a descriptive label and the values interpreted and fully expanded, if
possible. For example, the Audit Event Field would be a text string describing the event instead of an integer value. The start of each record is indicated by the text string

***START OF NEW RECORD***

and the field headings and values are displayed on multiple lines in the output. If a field does not apply to a particular event, it is not displayed.

Verbose mode would look similar to the following:

*** START OF NEW RECORD ***

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Mon 29 Oct 2001 04:35:27 PM CST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Event</td>
<td>TRACE File access</td>
</tr>
<tr>
<td>Audit View</td>
<td>Permit</td>
</tr>
<tr>
<td>Audit Reason</td>
<td>Global Audit</td>
</tr>
<tr>
<td>Audit Resource Type</td>
<td>TraceFile</td>
</tr>
<tr>
<td>Accessor Name</td>
<td>ossyes</td>
</tr>
<tr>
<td>Accessor Effective Name</td>
<td>ossyes</td>
</tr>
<tr>
<td>Audit Action</td>
<td>Trace</td>
</tr>
<tr>
<td>Audit Permissions</td>
<td>write read</td>
</tr>
<tr>
<td>Protected Resource Specification</td>
<td>/export/home/ossyes</td>
</tr>
<tr>
<td>Accessed Resource Specification</td>
<td>.sh_history</td>
</tr>
<tr>
<td>Accessor Process ID</td>
<td>1235</td>
</tr>
<tr>
<td>Running Program System Resource Name</td>
<td>/usr/bin/ksh</td>
</tr>
<tr>
<td>Audit Uniqifier</td>
<td>6</td>
</tr>
</tbody>
</table>

*** START OF NEW RECORD ***

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Mon 29 Oct 2001 04:35:27 PM CST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Event</td>
<td>An authorization decision was made.</td>
</tr>
<tr>
<td>Audit View</td>
<td>Permit</td>
</tr>
<tr>
<td>Audit Reason</td>
<td>Global Audit</td>
</tr>
<tr>
<td>Audit Resource Type</td>
<td>File</td>
</tr>
<tr>
<td>Accessor Name</td>
<td>ossyes</td>
</tr>
<tr>
<td>Accessor Effective Name</td>
<td>ossyes</td>
</tr>
<tr>
<td>Audit Action</td>
<td>Check Access</td>
</tr>
<tr>
<td>Audit Permissions</td>
<td>write read</td>
</tr>
<tr>
<td>Audit Qualifier</td>
<td>All resource policy checks permitted access.</td>
</tr>
<tr>
<td>Policy Branch Name</td>
<td>bvt</td>
</tr>
<tr>
<td>Protected Object Name</td>
<td>File/export/home/ossyes</td>
</tr>
<tr>
<td>System Resource Name</td>
<td>.sh_history</td>
</tr>
<tr>
<td>Accessor Process ID</td>
<td>1235</td>
</tr>
<tr>
<td>Running Program System Resource Name</td>
<td>/usr/bin/ksh</td>
</tr>
<tr>
<td>Audit Outcome</td>
<td>Success</td>
</tr>
<tr>
<td>Audit Uniqifier</td>
<td>7</td>
</tr>
</tbody>
</table>

*** START OF NEW RECORD ***

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Mon 29 Oct 2001 04:35:38 PM CST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Event</td>
<td>An authorization decision was made.</td>
</tr>
<tr>
<td>Audit View</td>
<td>Permit</td>
</tr>
<tr>
<td>Audit Reason</td>
<td>Global Audit</td>
</tr>
<tr>
<td>Audit Resource Type</td>
<td>NetOutgoing</td>
</tr>
<tr>
<td>Accessor Name</td>
<td>ossyes</td>
</tr>
<tr>
<td>Accessor Effective Name</td>
<td>ossyes</td>
</tr>
<tr>
<td>Audit Action</td>
<td>Check Access</td>
</tr>
<tr>
<td>Audit Permissions</td>
<td>connect</td>
</tr>
<tr>
<td>Audit Qualifier</td>
<td>All resource policy checks permitted access.</td>
</tr>
<tr>
<td>Policy Branch Name</td>
<td>bvt</td>
</tr>
<tr>
<td>Protected Object Name</td>
<td>NetOutgoing/*/tcp/telnet</td>
</tr>
<tr>
<td>Network Remote Host Identifier</td>
<td>dfstest08.austin.lab.tivoli.com</td>
</tr>
<tr>
<td>Network Protocol</td>
<td>tcp</td>
</tr>
<tr>
<td>Network Service</td>
<td>23</td>
</tr>
<tr>
<td>Accessor Process ID</td>
<td>1239</td>
</tr>
<tr>
<td>Running Program System Resource Name</td>
<td>/usr/bin/telnet</td>
</tr>
</tbody>
</table>
### Viewing Audit Logs

<table>
<thead>
<tr>
<th>Audit Outcome</th>
<th>Success</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Uniqifier</td>
<td>0</td>
</tr>
</tbody>
</table>

*** START OF NEW RECORD ***

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Mon 29 Oct 2001 04:35:44 PM CST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Event</td>
<td>The policy version has been set in the Kernel Policy Cache.</td>
</tr>
<tr>
<td>Audit View</td>
<td>Admin</td>
</tr>
<tr>
<td>Audit Reason</td>
<td>Global Audit</td>
</tr>
<tr>
<td>Audit Resource Type</td>
<td>Policy</td>
</tr>
<tr>
<td>Accessor Name</td>
<td>root</td>
</tr>
<tr>
<td>Accessor Effective Name</td>
<td>root</td>
</tr>
<tr>
<td>Audit Action</td>
<td>Apply</td>
</tr>
<tr>
<td>Accessor Process ID</td>
<td>831</td>
</tr>
<tr>
<td>Policy Version Number</td>
<td>14711</td>
</tr>
<tr>
<td>Audit Outcome</td>
<td>Success</td>
</tr>
<tr>
<td>Audit Uniqifier</td>
<td>0</td>
</tr>
</tbody>
</table>

*** START OF NEW RECORD ***

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Mon 29 Oct 2001 04:35:44 PM CST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Event</td>
<td>Logout occurred.</td>
</tr>
<tr>
<td>Audit View</td>
<td>Permit</td>
</tr>
<tr>
<td>Audit Reason</td>
<td>Global Audit</td>
</tr>
<tr>
<td>Audit Resource Type</td>
<td>Logout</td>
</tr>
<tr>
<td>Accessor Name</td>
<td>ossyes</td>
</tr>
<tr>
<td>Accessor Effective Name</td>
<td>Logout</td>
</tr>
<tr>
<td>Accessor Process ID</td>
<td>1235</td>
</tr>
<tr>
<td>Login Location Identifier</td>
<td>goblue.tivoli.com</td>
</tr>
<tr>
<td>Audit Uniqifier</td>
<td>0</td>
</tr>
</tbody>
</table>

*** START OF NEW RECORD ***

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Mon 29 Oct 2001 04:35:45 PM CST</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit Event</td>
<td>An authorization decision was made.</td>
</tr>
<tr>
<td>Audit View</td>
<td>Permit</td>
</tr>
<tr>
<td>Audit Reason</td>
<td>Global Audit</td>
</tr>
<tr>
<td>Audit Resource Type</td>
<td>File</td>
</tr>
<tr>
<td>Accessor Name</td>
<td>root</td>
</tr>
<tr>
<td>Accessor Effective Name</td>
<td>root</td>
</tr>
<tr>
<td>Audit Action</td>
<td>Check Access</td>
</tr>
<tr>
<td>Audit Permissions</td>
<td>read</td>
</tr>
<tr>
<td>Audit Qualifier</td>
<td>All resource policy checks permitted access.</td>
</tr>
<tr>
<td>Policy Branch Name</td>
<td>bvt</td>
</tr>
<tr>
<td>Protected Object Name</td>
<td>File/opt/pdos</td>
</tr>
<tr>
<td>System Resource Name</td>
<td>/usr/lib/liblpm.so</td>
</tr>
</tbody>
</table>
This is the default format of the `pdosaudview` command if the `-I` option is specified.

**Audit Log Record Types**

Audit log records are divided into three distinct types based on their content: *general*, *trace*, or *logout*. The information contained in the record varies based not only on the record type, but also on the type of resource being audited.

The content of the three types of audit log records is described first, and then the method for viewing the log records is discussed next.

**General Audit Event Record Type**

Most audit events use the general audit event record type. These include:

- login related events
- authorization decision events
- admin events
- informational events

The content of a general audit event is described in [Table 42].

**Table 42. General Audit Event Record Type**

<table>
<thead>
<tr>
<th>Fixed Position</th>
<th>Keyword</th>
<th>Field Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TS</td>
<td>Timestamp</td>
<td>Date and time audit record was generated.</td>
</tr>
<tr>
<td>2</td>
<td>E</td>
<td>Audit Event Identifier</td>
<td>Type of event that occurred. The audit event identifiers are enumerated in [Table 43 on page 141].</td>
</tr>
<tr>
<td>3</td>
<td>V</td>
<td>Audit View</td>
<td>Audit view associated with the event.</td>
</tr>
<tr>
<td>4</td>
<td>R</td>
<td>Audit Reason</td>
<td>Reason why audit record was generated.</td>
</tr>
<tr>
<td>5</td>
<td>RT</td>
<td>Audit Resource Type</td>
<td>Resource type. One of the following: Process, TCB, Cred, Policy, Login, File, NetIncoming, NetOutgoing, Surrogate, or Sudo.</td>
</tr>
<tr>
<td>6</td>
<td>AN</td>
<td>Accessor Name</td>
<td>Accessing user’s name</td>
</tr>
<tr>
<td>7</td>
<td>AEN</td>
<td>Accessor Effective Name</td>
<td>Accessing user’s effective name</td>
</tr>
</tbody>
</table>
Table 42. General Audit Event Record Type (continued)

<table>
<thead>
<tr>
<th>Fixed Position</th>
<th>Keyword</th>
<th>Field Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>A</td>
<td>Audit Action</td>
<td>The action for the audit event. One of the following: Check Access, Add, Delete, Change, Retrieve, Apply, Trust, Untrust, Start, Stop, Register, Trace, Isolated, Not Isolated, Login, Logout, Enable, or Disable.</td>
</tr>
<tr>
<td>9</td>
<td>P</td>
<td>Audit Permissions</td>
<td>If the Audit Action field value is Check Access, this field contains the specific actions associated with the access request. C connect, D chdir, G surrogate, K kill, L login, N create, R rename, U utime, d delete, l readdr, o chown, p chmod, r read, w write, x execute</td>
</tr>
<tr>
<td>10</td>
<td>Q</td>
<td>Audit Qualifier</td>
<td>Additional information for the audit event. See Table 44 on page 142 for details.</td>
</tr>
<tr>
<td>11</td>
<td>PBN</td>
<td>Policy Branch Name</td>
<td>Policy Branch Name. Only provided if the Protected Object Name field is filled in.</td>
</tr>
<tr>
<td>12</td>
<td>PON</td>
<td>Protected Object Name</td>
<td>Protected Object Name associated with the audit event. For events with Audit Action of Check Access: Tail of the Protected Object Name used to determine if access is allowed. For events with Audit Resource Type of Policy and the Audit Action is Apply: Protected Object Name that the policy was applied to.</td>
</tr>
<tr>
<td>13</td>
<td>SRN</td>
<td>System Resource Name</td>
<td>If Audit Resource Type is File: System name of the file being accessed. If Audit Resource Type is TCB and the Audit Action is Trust or Untrust: The name of the TCB resource that was marked trusted or untrusted. If Audit Resource Type is Login and the Audit View is Admin, and the Audit Action is Disable or Enable: The name of the user account that was enabled or disabled for login.</td>
</tr>
</tbody>
</table>
### Table 42. General Audit Event Record Type (continued)

<table>
<thead>
<tr>
<th>Fixed Position</th>
<th>Keyword</th>
<th>Field Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>SN</td>
<td>Surrogate Name</td>
<td>If the Audit Resource Type is Surrogate, the user name or ID of the target user or the group name or ID of the target group.</td>
</tr>
<tr>
<td>15</td>
<td>NRH</td>
<td>Network Remote Host Identifier</td>
<td><strong>If the Audit Resource Type is NetIncoming</strong>&lt;br&gt;The name of the remote host where access originated.&lt;br&gt;&lt;br&gt;<strong>If the resource type is NetOutgoing</strong>&lt;br&gt;The name of the remote host being accessed.&lt;br&gt;This field will be a host name if the address can be converted; otherwise, it is an IP address.</td>
</tr>
<tr>
<td>16</td>
<td>NP</td>
<td>Network Protocol</td>
<td>If the Audit Resource Type is NetIncoming or NetOutgoing, contains the protocol being used in the access.</td>
</tr>
<tr>
<td>17</td>
<td>NS</td>
<td>Network Service</td>
<td><strong>If the Audit Resource Type is NetIncoming</strong>&lt;br&gt;Service name or port number for the local service being accessed.&lt;br&gt;&lt;br&gt;<strong>If the Audit Resource Type is NetOutgoing</strong>&lt;br&gt;The service name or port number of the remote network service being accessed.</td>
</tr>
<tr>
<td>18</td>
<td>LL</td>
<td>Login Location Identifier</td>
<td>If the Audit Resource Type is Login and the login occurred from a local terminal, this is the terminal name. If the login occurred on a remote system, this is either the hostname or the IP address of the remote system.</td>
</tr>
<tr>
<td>19</td>
<td>APID</td>
<td>Accessor Processor ID</td>
<td>Process Identifier</td>
</tr>
<tr>
<td>20</td>
<td>RPPN</td>
<td>Running Program Protected Name</td>
<td>If the running program is registered in the Trusted Computing Base (TCB), the name the program is registered as appears here.</td>
</tr>
<tr>
<td>21</td>
<td>RPSN</td>
<td>Running Program System Resource Name</td>
<td>Name of the running program as executed.</td>
</tr>
<tr>
<td>22</td>
<td>SC</td>
<td>Sudo Command and Arguments</td>
<td>If the Audit Resource Type is Sudo, contains the target command name and arguments, if they are relevant to the Sudo policy.</td>
</tr>
<tr>
<td>23</td>
<td>SU</td>
<td>Sudo User Name</td>
<td>If the Audit Resource Type is Sudo, contains the target user name that the Sudo command will be executed as, if relevant to the Sudo policy.</td>
</tr>
<tr>
<td>24</td>
<td>SF</td>
<td>Sudo Flags</td>
<td>If the Audit Resource Type is Sudo, this field indicates with the Sudo policy dictated that the invoker password, target user password, or both were required before the target command could be executed. Otherwise this field contains no value.</td>
</tr>
<tr>
<td>25</td>
<td>AP</td>
<td>Additional Parameters</td>
<td>Additional information related to the particular audit event.</td>
</tr>
</tbody>
</table>
### Table 42. General Audit Event Record Type (continued)

<table>
<thead>
<tr>
<th>Fixed Position</th>
<th>Keyword</th>
<th>Field Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>CDAF</td>
<td>TCB Changed Data Attr Flags</td>
<td>Additional information related to Trusted Computing Base (TCB) resources.</td>
</tr>
<tr>
<td>27</td>
<td>PE</td>
<td>Policy Epoch</td>
<td>Additional information related to Policy resources.</td>
</tr>
<tr>
<td>28</td>
<td>PVN</td>
<td>Policy Version Number</td>
<td>Additional information related to Policy resources.</td>
</tr>
<tr>
<td>29</td>
<td>O</td>
<td>Audit Outcome</td>
<td>If the audit record was generated as a result of action taken due to an error condition, this field contains Failure (F). Otherwise, the field contains Success (S).</td>
</tr>
<tr>
<td>30</td>
<td>FS</td>
<td>Audit Fail Status</td>
<td>If the Audit Outcome field is Failure, this field contains an error code indicating the error that occurred.</td>
</tr>
<tr>
<td>31</td>
<td>UQ</td>
<td>Audit Uniqifier</td>
<td>Integer field that uniquely identifies audit records that occur within the same second. The value starts at 0 (for the first record recorded in the second) and is incremented for subsequent records written in that second.</td>
</tr>
<tr>
<td>Audit Event Identifier (E)</td>
<td>Description</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>A login related authorization decision was made.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>User account was disabled (locked), preventing future logins.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>User account was disabled (suspended), preventing future logins.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>User account was enabled for login.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>The password change time was modified by an administrator.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Logout occurred. (See “Logout Audit Event Record Type” on page 144 for a description of the audit record used for this event.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>An authorization decision was made.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>An authorization decision API failure occurred.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Access granted to a file marked untrusted in the TCB database.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>PDOS kernel lost contact with PDOSD. Accesses are being denied by default.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>PDOS kernel has regained contact with PDOSD. Accesses are determined by PDOS policy.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Policy Director user registry is unavailable (isolation mode).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Policy Directory user registry is now available.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Credential acquired.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Policy not applied for an invalid protected object name.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Policy applied for a protected object name.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Policy version set in the Kernel Policy Cache.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Kernel Policy Cache epoch updated.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>A file has been added to the TCB database</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>A file has been removed from the TCB database</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>A file has been marked untrusted</td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>A file has been marked trusted</td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>A PDOS process has started</td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td>A PDOS process has stopped</td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>A PDOS process has been adopted into the watchdog set</td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td>A kosseal_register call was made to acquire privileged access.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>TRACE Exec program (See “Trace Audit Event Record Type” on page 142 for a description of the audit record used for this event.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>TRACE File access (See “Trace Audit Event Record Type” on page 142 for a description of the audit record used for this event.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>Password change has occurred.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 44. Description of Audit Qualifiers

<table>
<thead>
<tr>
<th>Audit Qualifier (Q)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Login Related Qualifiers</strong></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>User account is locked</td>
</tr>
<tr>
<td>2</td>
<td>The user password has expired and no further grace logins remain.</td>
</tr>
<tr>
<td>3</td>
<td>Maximum number of concurrent logins reached.</td>
</tr>
<tr>
<td>4</td>
<td>Lock time interval has not elapsed.</td>
</tr>
<tr>
<td>5</td>
<td>Minimum time interval required between password changes has not elapsed.</td>
</tr>
<tr>
<td>6</td>
<td>User account was unlocked because lock time interval has elapsed.</td>
</tr>
<tr>
<td>7</td>
<td>Maximum number of failed logins reached.</td>
</tr>
<tr>
<td>8</td>
<td>Maximum inactive days has elapsed.</td>
</tr>
<tr>
<td>9</td>
<td>Maximum time interval since last password change has elapsed.</td>
</tr>
<tr>
<td>10</td>
<td>Checking login location access control policy.</td>
</tr>
<tr>
<td>11</td>
<td>Checking Access-Restrictions associated with login location access control policy.</td>
</tr>
<tr>
<td>12</td>
<td>Checking login holiday access control policy.</td>
</tr>
<tr>
<td>13</td>
<td>Checking Access-Restrictions associated with login holiday access control policy.</td>
</tr>
<tr>
<td>14</td>
<td>Checking time of day login access control policy.</td>
</tr>
<tr>
<td>15</td>
<td>Unknown user attempted login.</td>
</tr>
<tr>
<td>16</td>
<td>Login denied by native authentication method.</td>
</tr>
<tr>
<td>17</td>
<td>User account modified by administrative action.</td>
</tr>
<tr>
<td>18</td>
<td>All login policy checks permitted access.</td>
</tr>
<tr>
<td><strong>General Resource Related Qualifiers</strong></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>Checking resource access control policy.</td>
</tr>
<tr>
<td>31</td>
<td>Checking Access-Restrictions associated with resource access control policy.</td>
</tr>
<tr>
<td>32</td>
<td>Checking trust state for TCB resource.</td>
</tr>
<tr>
<td>33</td>
<td>Error occurred reading the request message data.</td>
</tr>
<tr>
<td>34</td>
<td>All resource policy checks permitted access.</td>
</tr>
</tbody>
</table>

Additional qualifiers will be defined as needed.

Trace Audit Event Record Type

Trace audit event records record when an exec() is done or when a file access occurs. The content of a trace audit event record is described in Table 45.

Table 45. Trace Audit Event Record Type

<table>
<thead>
<tr>
<th>Fixed Position</th>
<th>Keyword</th>
<th>Field Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TS</td>
<td>Timestamp</td>
<td>Date and time audit record was generated.</td>
</tr>
<tr>
<td>2</td>
<td>E</td>
<td>Audit Event Identifier</td>
<td>Type of event that occurred.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>27 TRACE Exec program</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>28 TRACE File access</td>
</tr>
</tbody>
</table>
### Table 45. Trace Audit Event Record Type (continued)

<table>
<thead>
<tr>
<th>Fixed Position</th>
<th>Keyword</th>
<th>Field Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>V</td>
<td>Audit View</td>
<td>Audit view associated with the event.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>D           Deny</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>P           Permit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>T           Trace</td>
</tr>
<tr>
<td>4</td>
<td>R</td>
<td>Audit Reason</td>
<td>Reason why audit record was generated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1           Global Audit</td>
</tr>
<tr>
<td>5</td>
<td>RT</td>
<td>Audit Resource Type</td>
<td>Resource type</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>TraceExec</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>TraceFile</td>
</tr>
<tr>
<td>6</td>
<td>AN</td>
<td>Accessor Name</td>
<td>Accessing user’s name</td>
</tr>
<tr>
<td>7</td>
<td>AEN</td>
<td>Accessor Effective Name</td>
<td>Accessing user’s effective name</td>
</tr>
<tr>
<td>8</td>
<td>A</td>
<td>Audit Action</td>
<td>Trace</td>
</tr>
<tr>
<td>9</td>
<td>P</td>
<td>Audit Permissions</td>
<td>This field contains the specific actions associated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>with the access request.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>D           chdir</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>K           kill</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>N           create</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>R           rename</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>U           utime</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>d           delete</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>l           readdir</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>o           chown</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>p           chmod</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>r           read</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>w           write</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>x           execute</td>
</tr>
<tr>
<td>10</td>
<td>Q</td>
<td>Audit Qualifier</td>
<td>Additional information for the audit event. See</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><a href="#">Table 44 on page 142</a> for details</td>
</tr>
<tr>
<td>11</td>
<td>PRS</td>
<td>Protected Resource</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specification</td>
<td></td>
</tr>
</tbody>
</table>
### Table 45. Trace Audit Event Record Type (continued)

<table>
<thead>
<tr>
<th>Fixed Position</th>
<th>Keyword</th>
<th>Field Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>ARS</td>
<td>Accessed Resource Specification</td>
<td>If the Audit Resource Type is TraceFile: The name of the file resource used in the access. If the Audit Resource Type is TraceExec: The name of the file resource as it was specified in the exec() operation. If the file is a setuid program, then a [SU] token follows the name. If the file is a setgid program, then a [SG] token follows the name. If the file is both a setuid and setgid program, then a [SUG] token follows the name. The argv string provided in the exec() call (which normally reflects what command line arguments were specified) follows enclosed in parentheses. For example: `/usr/bin/ps [SG] (ps -elf</td>
</tr>
<tr>
<td>13</td>
<td>APID</td>
<td>Accessor Processor ID</td>
<td>Process Identifier</td>
</tr>
<tr>
<td>14</td>
<td>RPSN</td>
<td>Running Program System Resource Name</td>
<td>Name of the running program as executed.</td>
</tr>
<tr>
<td>15</td>
<td>UQ</td>
<td>Audit Uniqifier</td>
<td>Integer field that uniquely identifies audit records that occur within the same second. The value starts at 0 (for the first record recorded in the second) and is incremented for subsequent records written in that second.</td>
</tr>
</tbody>
</table>

### Logout Audit Event Record Type

Logout audit event records are used for user logout events. Table 46 describes the content of the logout audit event record type.

### Table 46. Logout Audit Event Record Type

<table>
<thead>
<tr>
<th>Fixed Position</th>
<th>Keyword</th>
<th>Field Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>TS</td>
<td>Timestamp</td>
<td>Date and time audit record was generated.</td>
</tr>
<tr>
<td>2</td>
<td>E</td>
<td>Audit Event Identifier</td>
<td>Type of event that occurred. Logout Occurred</td>
</tr>
<tr>
<td>3</td>
<td>V</td>
<td>Audit View</td>
<td>Audit view associated with the event. Permit</td>
</tr>
<tr>
<td>4</td>
<td>R</td>
<td>Audit Reason</td>
<td>Reason why audit record was generated. Global Audit</td>
</tr>
<tr>
<td>5</td>
<td>RT</td>
<td>Audit Resource Type</td>
<td>Resource type. Logout</td>
</tr>
<tr>
<td>6</td>
<td>AN</td>
<td>Accessor Name</td>
<td>Logout user name</td>
</tr>
</tbody>
</table>
Effectively Using the Audit View Tool

Use the Audit View Tool to search the audit log files for information and parse that information into a readable text format. You can filter the log records by a number of parameters such as resource type, authorization decision, timestamp, and accessor type. When you define a search using the Audit View Tool, the tool parses the binary data from the audit log into a text file containing all the records that matched your search. By default this file is called `text.log` and is stored in the same directory where the `audit.log` file is stored.

Every time you execute a search, the `text.log` file is replaced with the records matching that search. You also can view the filtered records immediately on screen by issuing `pdosaudview` with the `-l` option.

The Audit View Tool is run on the command line. The command and filter options for the Audit View Tool are defined in “pdosaudview” on page 148. Several examples of the command are provided in the next section.

Sample Searches

Here are some sample uses of the Audit View Tool.

1. To display all audit records that were generated as a result of an access attempt that was denied:
   
   ```bash
   pdosaudview -w deny
   ```

2. To display denied login attempts that occurred today for user ID `maggie`:
   
   ```bash
   pdosaudview -s today -e today -g login -w deny -n maggie
   ```

3. To display audit records recorded in the last 30 minutes:
   
   ```bash
   pdosaudview -s now-30
   ```

4. To write, in concise format, audit records associated with denied file accesses for user ID `bjones` between October 25, 2001 and October 31, 2001 to a file called `/tmp/audout/bjones`:
   
   ```bash
   pdosaudview -F concise -s 2001-10-25-00:00 \ 
   -e 2001-10-31-23:59 -g file \ 
   -w deny -n bjones -f /tmp/audout/bjones
   ```
5. To display audit records that were written in the last minute:
   `pdosaudview -s now`
This chapter provides an overview of the commands available in Tivoli Policy Director for Operating Systems.

Several of the commands require that the user be a Tivoli Policy Director for Operating Systems runtime administrator. A runtime administrator is any user that is a member of both of the following groups.

- osseal-admin group in the Tivoli Policy Director user registry
- osseal group in UNIX

The `pdosaudview` command requires that the user be a Tivoli Policy Director for Operating Systems auditor. An auditor is any user that is a member of both of the following groups.

- osseal-auditors group in the Tivoli Policy Director user registry
- ossaudit group in UNIX

Default policy has been established to ensure that the commands operate successfully and securely. Changes to the default policy affecting these commands might compromise the security of your system or render the commands inoperative. Refer to Chapter 2, “Policy” on page 5 for more detailed information on the default policy.

**Note:** The `-t trace-string` option available on many of the commands is intended for use by Tivoli Customer Support personnel only. The contents of the `trace-string` is not described in this document.
pdosaudview

Purpose

Parses the binary audit log produced by Tivoli Policy Director for Operating Systems into a number of readable formats.

Syntax

pdosaudview [-h] [-?] [-V]
[ -l ] [ prints output to screen ]
[ -g resource type]
[ -z azn decision type]
[ -p pid]
[ -w audit view]
[ -a action]
[ -r reason]
[ -o outcome]
[ -n accessor name | accessor uid]
[ -c accessor effective name | accessor effective uid]
[ -s [YYYY-MM-DD[(-hh:mm:ss)]] | today [-n] | now [-n] ]
[ -e [YYYY-MM-DD[(-hh:mm:ss)]] | today [-n] | now [-n] ]
[ -R YYYY-MM-DD-hh:mm:ss n]
[ -f filename]
[ -i audit log filename]
[ -F concise | keyvalue | verbose]
[ -M keyword | event | view | permission | qualifier | outcome | all]

Description

The pdosaudview command is used to process a binary audit file produced by Tivoli Policy Director for Operating Systems and convert it into readable text. The resulting output can be viewed, printed, or analyzed by scripts and other programs.

The output format of the pdosaudview command can be one of the following: concise, keyvalue, and verbose. A description of these formats can be found in "Viewing Audit Logs" on page 134.

A variety of filtering options are provided on the command to limit the amount of output produced. Audit records can be selected based on such factors as type of event, time of event, outcome of the event, and type of resource affected.

By default, all audit logs in the /var/pdos/audit directory are processed by the command. To limit the processing to a specific file, use the -i option.

See Chapter 6, “Auditing” on page 131 for a complete overview of auditing.

You must be a Tivoli Policy Director for Operating Systems auditor to use this command.

Options

-V Displays the version information.
-h Displays the usage message.
-? Displays the usage message.
-l Indicates command output should be sent to the screen (stdout). If the -F option is not specified, the records are written in verbose format.
-g Resource type (azn, daemon, tcb, cred, policy, login, logout, trace_exec, trace_file)
In addition to the above values, the values for the -z option can be specified here as well.

-z azn_decision type: (file, netincoming, netoutgoing, login, surrogate, sudo)
-p Identifies the process that generated the audit event. The possible values are KERNEL, PDOSD, WATCHDOG, AUDITD, and GENERAL. This field is no longer displayed in the output of the pdosaudview command. This option, maintained for backward compatibility, allows you to show only the audit events generated by a specific component.

-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)
-r Reason (global_audit, resource_audit, global_warning, resource_warning)
-o Outcome (success, failure, trace_event, trace_permit, trace_deny)
-n Accessor name | accessor uid
-c Accessor effective name | accessor effective uid
-s Start time. Can be specified as a timestamp in the form of YYYY-MM-DD[-hh:mm:ss] or by using the special qualifiers of today and now to represent the current day and the current minute, respectively. Optionally when using the special qualifiers, an integer value, n, can be specified to specify the previous n days or the previous n minutes. Only records logged at or after the specified start time are formatted.
-e End time. Can be specified as a timestamp in the form of YYYY-MM-DD[-hh:mm:ss] or by using the special qualifiers of today and now to represent the current day and the current minute, respectively. Optionally when using the special qualifiers, an integer value, n, can be specified to specify the previous n days or the previous n minutes. Only records logged before or at the end time are formatted.
-R Selects a specific audit record given its timestamp (YYYY-MM-DD-hh:mm:ss) and its audit uniqifier (n).
-f Filename - create ASCII output
-i File name of a specific audit log filename to process. If this option is omitted, all audit logs in the /var/pdos/audit directory are processed by the command.
-F Formatting style of audit records. The default is keyvalue format unless the -l option is used. If the -l option is specified without the -F option, records are displayed in verbose format.
-M Display mapping of audit record fields.

Exit Status

0 The command completed successfully.
1 An error occurred.
Examples

1. To display audit records with a resource type of login:
   pdosaudview -g login

2. To display audit records for surrogate accesses that were permitted yesterday:
   pdosaudview -s today-1 -e today-1 -g surrogate -w permit

3. To display all audit records written within the previous minute to stdout:
   pdosaudview -l -s now-1 -e now-1

More examples can be found in “Effectively Using the Audit View Tool” on page 145.
pdosbkup

Purpose
Backup Tivoli Policy Director for Operating Systems databases and configuration files.

Syntax
pdosbkup [ -Vh?] [-x] [-f filename] [-p directory-path]

Description
The pdosbkup command is used to back up all files and directories listed in the /opt/pdos/etc/pdosbkuplist file or, if the -x option is specified, all files and directories listed in the /opt/pdos/etc/pdosbkuplistx file.

If a directory is specified in the backup list, only files immediately under that directory will be backed up. Sub-directories are traversed. By default the tar file created as the backup file is placed in the /var/pdos/pdosbkup directory with a file name of the form pdosbkupDDMMMYYYY:hh_mm_ss.tar.

The -p option can be used to change the directory where the backup file is stored. Use the -f option to change the name of the file created.

If the pdosbkup command is executed while the Tivoli Policy Director for Operating Systems daemons are running, the state of some of the files can change during the backup.

You must be a Tivoli Policy Director for Operating Systems runtime administrator to use this command.

Options
-V Displays the version information.
-h Displays the usage message.
-? Displays the usage message.
-x Perform extended backup.
-f filename
Specifies the name of the backup file.
-p directory-path
Specifies the name of the directory in which to place the backup file.

Exit Status
0 The command completed successfully.
1 An error occurred.

Examples
The following are examples of pdosbkup usage:

1. To back up critical Tivoli Policy Director for Operating Systems configuration files, enter:
pdosbkup
If the backup was done on December 7, 2001 at 04:30:00, the name of the backup file would be:
/var/pdos/pdosbkup/pdosbkup07Dec2001.04_30_00.tar

2. To do an extended Tivoli Policy Director for Operating Systems backup and store the result in /var/disaster_rcvy/December2001.tar, enter:
   pdosbkup -x -p /var/disaster_rcvy -f December2001.tar
**pdoscfg**

**Purpose**
Configures Tivoli Policy Director for Operating Systems.

**Syntax**

```
pdoscfg [-admin_cred_refresh number_of_minutes]
[-audit_level (all | none | permit | deny | loginpermit | logindeny | admin | verbose | info | trace_exec | trace_file)]
[-audit_log_entries number_of_log_entries]
[-audit_logflush number_of_seconds]
[-audit_logs number_of_logs]
[-audit_log_size number_of_bytes]
[-autostart (on | off)]
[-cred_hold number_of_minutes]
[-delete (comma_delimited_list_of_options)]
[-dns (on | off)]
[-help]
[-kmsg_hnd_threads number_of_threads]
-ldap_ssl_cacert ldap_certificate_file_name
[-login_policy (on | off)]
--branch policy_branch_name
[-operations]
[-pdosd_log_entries number_of_log_entries]
[-pdosd_logs number_of_logs]
[-pdoswdd_log_entries number_of_log_entries]
[-pdoswdd_logs number_of_logs]
[-refresh_interval number_of_minutes]
[-rspfile file_name]
[-sec_master_pwd security_master_password]
[-ssl_listening_port port_to_listen_for_notification]
--suffix policy_director_suffix
[-tcb_ignore_ctime (on | off)]
[-tcb_interval number_of_minutes]
[-tcb_max_file_size number_of_megabytes]
[-tcb_monitor_threads number_of_threads]
[-tcb_nocrc_on_exec (on | off)]
[-uid (on | off)]
[-usage]
[-user_cred_refresh number_of_minutes]
[-version]
[-warning (on | off)]
[-?]```

**Description**

Use the `pdoscfg` command to initially configure Tivoli Policy Director for Operating Systems. After the initial configuration, use `pdoscfg` to modify the configuration attributes. The changes made with `pdoscfg` take effect the next time Tivoli Policy Director for Operating Systems is stopped and then restarted.

You can also use the `pdoscfg` command to delete attributes from the configuration files. The daemons will then use the default values the next time you restart Tivoli Policy Director for Operating Systems.
The policy-branch name and suffix cannot be changed after the initial configuration. You must use the `pdoscfg` command to unconfigure Tivoli Policy Director for Operating Systems and then use the `pdoscfg` command to reconfigure it with a different policy-branch and suffix values.

Stop Tivoli Policy Director for Operating Systems before you issue the `pdoscfg` command to change the SSL listening port or the LDAP SSL CA certificate.

## Options

Options for the configuration command are described in this section. The definition and default, if applicable, for each option is given.

- **admin_credential_refresh**  
  Refresh interval of administrator’s credentials in minutes.  
  Default: 360

- **audit_level**  
  A comma-separated list of audit levels. The levels are all, none, permit, deny, loginpermit, logindeny, admin, verbose, info, trace_exec, or trace_file.  
  Default: none

- **audit_log_entries**  
  Number of PDOSAUDITD log entries before rolling over to a new log. The default of 0 means never roll over to a new log.  
  Default: 0

- **audit_logflush**  
  Interval in seconds to flush the audit log buffers.  
  Default: 5

- **audit_logs**  
  Number of PDOSAUDITD log files to use before recycling log files. A value of 0 indicates that log files should never be recycled. Setting logs to a nonzero value has an effect only if audit_log_entries is nonzero.  
  Default: 0

- **audit_log_size**  
  Maximum size in bytes of log file before the log rolls over to a new log.  
  Default: 1000000

- **autostart**  
  Automatically start Tivoli Policy Director for Operating Systems at system reboot.  
  Default: on

- **cred_hold**  
  Maximum amount of time in minutes that a nonadministrator credential is cached without being accessed. This value must be greater than or equal to the `admin_credential_refresh` value and the `user_credential_refresh` value.  
  Default: 10080

- **delete**  
  Comma-separated list of options to remove from configuration files. Supported options are `admin_credential_refresh`, `audit_level`, `audit_log_entries`, `audit_logflush`,
audit_logs, audit_log_size, cred_hold, dns, kmsg_hnd_threads, pdosd_log_entries, pdosd_logs, pdoswdd_log_entries, pdoswdd_logs, refresh_interval, tcb_interval, tcb_max_file_size, tcb_monitor_threads, uid, user_cred_refresh, and warning.

-dns Enables Tivoli Policy Director for Operating Systems to store the IP address to hostname mapping information.
   Default: on

-help Displays help for all of the options. To display help for one option, type -help -<option>.

-kmsg_hnd_threads
   Number of threads used to handle authorization requests. Must be a positive integer.
   Increasing this value on multi-processor systems with more than 8 processors can reduce the time authorization requests take and improve performance. Specify a value equal to the number of processors in the system or 8, whichever is greater.
   The maximum recommended number of threads at this time is 24.
   Default: 8

-ldap_ssl_cacert
   The CA certificate of the LDAP Server that contains the Tivoli Policy Director user registry. This certificate is required for the mutual authentication that occurs between Tivoli Policy Director for Operating Systems and the LDAP server.

-login_policy
   Enable system login and password restrictions.
   Default: on

-name
   Name of the policy branch to which this machine subscribes.

-operations
   Lists the supported options.

-pdosd_log_entries
   Number of PDOSD log entries to use before rolling over to a new log. The default of 0 means never roll over to a new log.
   Default: 0

-pdosd_logs
   Number of PDOSD log files to use before recycling log files. A value of 0 indicates that log files should never be recycled. Setting logs to a nonzero value has an effect only if pdosd_log_entries is nonzero.
   Default: 0

-pdoswdd_log_entries
   Number of PDOSWDD log entries to use before rolling over to a new log. The default 0 means never roll over to a new log.
   Default: 0

-pdoswdd_logs
   Number of PDOSWDD log files to use before recycling log files. A value of 0 indicates that log files should never be recycled. Setting logs to a nonzero value has an effect only if pdoswdd_log_entries is nonzero.
Default: 0

-refresh_interval
Interval in minutes that the Tivoli Policy Director management server is polled for policy updates, if it has not received any during the interval. A value of 0 indicates that policy database updates are not received by polling. Compare

-ssl_listening_port.

Default: 0

-rspfile
Name of file containing option values for the configuration.

-sec_master_pwd
Tivoli Policy Director security master password.

-ssl_listening_port
Port to listen for policy database update notifications. A value of zero indicates that policy database updates will not be received by notification. Compare

-refresh_interval.

Default: 7134

-suffix
LDAP suffix.

-tcb_ignore_ctime
Causes ctime to be ignored when performing TCB signature comparisons. When this option is enabled, a change in the ctime does not cause the TCB resource to become untrusted.

-tcb_interval
Interval in seconds during which all TCB files are checked for signature changes. The workload is approximately distributed uniformly over this interval.

Default: 1800

-tcb_max_file_size
Maximum number of megabytes of a file considered significant for calculating a checksum. The bytes checked are distributed throughout the file.

Default: 10

-tcb_monitor_threads
Number of threads used to monitor TCB files for changes. Setting this value above one is useful only on multi-processor machines. Must be a positive integer.

Default: 1

-tcb_nocrc_on_exec
Causes the CRC check that normally occurs as part of the authorization check associated with running an executable file to be skipped. Enabling this option avoids performing the CRC validation on large binary files.

-uid
Enables caching of the uid/gid to user/group name mapping information.

Default: off

-usage
Displays help on the command’s usage.
- `--user_cred_refresh`
  Refresh interval of user’s credentials in minutes.
  Default: 720

- `--version`
  Displays the version of the `pdoscfg` utility.

- `--warning`
  Enables global authorization warning mode.
  Default: off

- `--?
  Displays help on the command’s usage.`
pdosctl

Purpose

Sends control messages to selected Tivoli Policy Director for Operating Systems daemons.

Syntax

```
pdosctl -k [daemon [-k daemon ...]]
-s [daemon [-s daemon ...]] [-q]
-w [on|off]
-a [audit-level[:{on|off}]] [-a audit-level[:{on|off}] ...]]
-A [audit-level[:{on|off}]] [-A audit-level[:{on|off}] ...]]
-t [daemon[:trace-string]] [-t daemon[:trace-string] ...]]
[-Vvh?]
[-t trace-string]
```

Description

The `pdosctl` command sends control messages to the specified daemons. The `pdosctl` command is able to shut down an individual daemon, control audit views, control warning mode, set debug trace levels and display daemon status. The daemons that can be controlled are: PDOSD, PDOSAUDITD, and PDOSWDD.

The `-k` option when specified with no arguments shuts down these three Tivoli Policy Director for Operating Systems daemons. The `-k` option may also be used to shut down individual daemons by following it with a daemon name. The `-k` option may be specified multiple times on a single command line.

The `-s` option when specified with no arguments displays the status of each of these three daemons. The `-s` option may also be used to display the status of individual daemons by following it with a daemon name. The `-s` option may be specified multiple times on a single command line.

The `-q` option may be specified with the `-s` option. The `-q` option suppresses the messages generated by the `-s` option and sets the return code to 0 on success and 1 if any of the queried daemons are down.

The `-w` option when specified with no arguments displays the global warning mode for Tivoli Policy Director for Operating Systems. The `-w` option may also be used to set the global warning mode by following it with either the keyword on or off.

The `-a` and `-A` options, when specified with no arguments, display the current global audit level of the daemons. You can also use the `-a` and `-A` options to modify the current global audit level:

- `-A` resets the current global level to the specified value. If multiple `-A` options are specified in a single command line, the global audit level is set to all of the specified values.

- `-a` modifies the global audit level by resetting only the specified audit level. You can specify multiple `-a` options on a single command line.

To reset or modify the global audit level, the `-a` and `-A` options must be followed by an audit level and the keyword on or off separated by a colon (:). Valid values for audit level are: all, none, permit, deny, loginpermit, logindeny, admin, verbose, info, trace_exec, and trace_file.
The -t option when specified with no arguments displays the current trace level of each of
the daemons. The -t option can be followed by a daemon name to display the trace level for
the specified daemon. The -t option can also be used to set the trace level for a specified
daemon. To set the trace level for a daemon, the -t option must be followed by the daemon
name, a colon (:), and then by the trace string. The -t option is used only for Tivoli Policy
Director for Operating Systems support debugging purposes. The format of the trace string is
not documented. The -t option may be specified multiple times on a single command line.
You must be a Tivoli Policy Director for Operating Systems runtime administrator to use
this command.

Options

-\texttt{-V} \quad \text{Displays the version information.}
-\texttt{-v} \quad \text{Displays verbose messages.}
-\texttt{-h} \quad \text{Displays the usage message.}
-\texttt{-?} \quad \text{Displays the usage message.}
-\texttt{-t \ trace-string}
  \quad \text{Sets the trace string for displaying trace messages.}
-\texttt{-k \ [daemon]}
  \quad \text{Send a control message to shut down the specified daemons.}
-\texttt{-s \ [daemon]}
  \quad \text{Send a control message to query the status of the specified daemons.}
-\texttt{-w}
  \quad \text{Send a control message to turn on the global warning level.}
-\texttt{-a \ [audit\ level]}
  \quad \text{Send a control message to modify the global audit level.}
-\texttt{-A \ [audit\ level]}
  \quad \text{Send a control message to modify the global audit level.}
-\texttt{-t \ [daemon]}
  \quad \text{Send a control message to set or display the trace level of the specified daemons.}

Exit Status

\begin{itemize}
  \item [0] \quad \text{The command completed successfully.}
  \item [1] \quad \text{An error occurred.}
\end{itemize}

Examples

The following are examples of \texttt{pdosctl} usage:

1. To shutdown the PDOSD, PDOSAUDITD, and PDOSWDD daemons, enter:
   \begin{verbatim}
   pdosctl -k
   \end{verbatim}
   The output is:
   \begin{verbatim}
   pdosd shutdown
   pdoswdd shutdown
   pdosauditd shutdown
   \end{verbatim}

2. To shutdown only the PDOSWDD daemon, enter:
   \begin{verbatim}
   pdosctl -k pdoswdd
   \end{verbatim}
   The output is:
3. To check the status of Tivoli Policy Director for Operating Systems, enter:

   pdosctl -s

   The output is:
   - pdosd is running normally
   - pdoswdd is running normally
   - pdosauditd is running normally

4. To turn on global warning mode, enter:

   pdosctl -w on

5. To query the global warning mode, enter:

   pdosctl -w

   The output is:
   - The global warning mode setting is on

6. To set the global audit level to grant and deny, enter:

   pdosctl -A permit:on -A deny:on

7. To add the admin audit level to the global audit level, enter:

   pdosctl -a admin:on

8. To query the global audit level, enter:

   pdosctl -a

   The output is:
   - pdosd has the following audit levels on: permit, deny, admin
   - pdoswdd has the following audit levels on: permit, deny, admin
   - pdosauditd has the following audit levels on: permit, deny, admin
pdosdestroy

Purpose
Destroys the Tivoli Policy Director for Operating Systems credentials for the specified users.

Syntax
pdosdestroy [-Vvh?] [-t trace-string] [-u uid] [-u uid ...] [-n name] [-n name ...]

Description
The pdosdestroy command removes the cached credentials for the specified users from the Tivoli Policy Director for Operating Systems Credential Cache. If the -u or -n options are not specified, the credentials of the invoking user are destroyed. If the -u option is specified, the credentials for the user specified by the UID are destroyed. If the -n option is specified, the credentials for the user specified by the name will be destroyed.

If you specify the -u or -n options, you must be a Tivoli Policy Director for Operating Systems runtime administrator. The -u and -n options can be specified multiple times on the same command line and can be used together.

Options
-V Displays the version information.
-v Displays verbose messages.
-h Displays the usage message.
-? Displays the usage message.
-t trace-string Sets the trace string for displaying trace messages.
-u uid Specifies the UID of the user whose credential is to be destroyed.
-n name Specifies the UNIX name of the user whose credential is to be destroyed.

Exit Status
0 The command completed successfully.
1 An error occurred.

Examples
The following are examples of pdosdestroy usage:
1. To destroy the credentials of the invoking user, enter:
   pdosdestroy
2. To destroy the credentials of users anne and riley, whose UID is 300, enter:
   pdosdestroy -n anne -u 300
**pdosexempt**

**Purpose**
Disables Tivoli Policy Director for Operating Systems authorization decisions.

**Attention:** This command disables Tivoli Policy Director for Operating Systems authorization decisions. Remember to revoke the exemption with the `pdosrevoke` command.

**Syntax**
```
pdosexempt [-Vvh?] [-t trace-string] [-i] [pid [pid ...]]
```

**Description**
The `pdosexempt` command disables Tivoli Policy Director for Operating Systems authorization decisions. When the `pdosexempt` command is invoked with no arguments, all processes running under the OSSEAL privileged user (osseal) are exempt from policy. In addition, any new processes running as the OSSEAL privileged user (osseal) are also exempt from policy.

Strong protection should be provided to both the osseal account and the `pdosexempt` command such as permitting access to it through only the following:

- Non-remote terminals
- A stronger authentication mechanism than simple password based authentication
- Highly restrictive ACLs on `pdosexempt`

If a pid or list of pids is specified on the `pdosexempt` command line, the processes represented by those pids are immediately exempt from policy. The list of pids must occur last on the `pdosexempt` command line.

The `-i` option can be specified in conjunction with the list of pids. If the `-i` option is specified, any new children of the processes represented by the specified pids inherit the policy exemption.

The `pdosrevoke` command is used to revoke the PDOS authorization exemption granted by the `pdosexempt` command.

You must be a Tivoli Policy Director for Operating Systems runtime administrator to use this command.

**Options**

- **-V** Displays the version information.
- **-v** Displays verbose messages.
- **-h** Displays the usage message.
- **-?** Displays the usage message.
- **-t trace-string**
  Sets the trace string for displaying trace messages.
- **-i** Causes new child processes of the specified pids to inherit the policy exemption.
Exit Status

0  The command completed successfully.

1  An error occurred.

Examples

The following are examples of `pdosexempt` usage:

1. To make all processes running under the OSSEAL privileged user exempt from Tivoli Policy Director for Operating Systems authorization decisions, enter:
   ```bash
   pdosexempt
   ```
   The output is:
   ```
   User osseal (uid 1444) is now exempt from PDOS policy.
   ```

2. To make a specific process and its children exempt from Tivoli Policy Director for Operating Systems authorization decisions, enter:
   ```bash
   pdosexempt -i 9688
   ```
   The output is:
   ```
   Process 9688 and any future children are now exempt from PDOS policy.
   ```
pdoshla

Purpose

Manages the IP address to Host Name Lookaside Database.

Syntax

```
pdoshla [-Vvh?]
   [-t trace-string]
   [-D DB-path] -F
   [-D DB-path] -f
   [-D DB-path] -r IP-addr
   [-D DB-path] -a IP-addr [-T TTL-secs -H hostname]
   [-D DB-path] -l {all | stale | fresh }
   [-D DB-path] -u
```

Description

The `pdoshla` command adds, deletes, refreshes, and views entries in the IP address to Host Name Lookaside Database.

If the `-D` option is not specified, the default database is used. The default database resides in the `/var/pdos/hla` directory. An entry for a given IP address may be added to the database by using the `-a` option.

If the `-T` option is not specified along with the `-a` option, the Time To Live is set to a default value of 21600 seconds (6 hours).

If the `-H` option is not specified, a DNS lookup is performed to determine the hostname associated with the given IP address.

To remove entries from the database, use:

- `-F` option to flush the entire database
- `-f` option to flush only stale entries
- `-r` option to remove a specific entry

All of the database entries may be refreshed by specifying the `-u` option. This will cause a DNS hostname lookup to occur for each entry found in the database.

Entries in the database can be viewed by using the `-l` option along with the all, stale or fresh qualifiers.

You must be a Tivoli Policy Director for Operating Systems runtime administrator to use this command.

Options

```
-V    Displays the version information.
-v    Displays verbose messages.
-h    Displays the usage message.
-?    Displays the usage message:
   
-t trace-string
    Sets the trace string for displaying trace messages.
```
-D database_path
   Specifies the pathname of the database.

-F
   Specifies that all entries should be flushed from the database.

-f
   Specifies that stale entries should be flushed from the database.

-r IP_address
   Removes an entry from the database.

-a IP_address
   Adds or replaces an entry in the database.

-T TTL_seconds
   Specifies the Time To Live in seconds when creating a new database entry.

-H Hostname
   Specifies the Hostname.

-l
   Lists database entries.

-u
   Refresh all entries in the database.

Exit Status

  0   The command completed successfully.
  1   An error occurred.

Examples

The following are examples of pdoshla usage:

1. To add an entry to the default database for IP address 146.84.107.11, enter:
   pdoshla -a 146.84.107.11

2. To view all of the entries in the default database, enter:
   pdoshla -l all
   The output is:
   # Internet Address Hostname
   9.41.3.101 carlb.austin.lab.tivoli.com
   146.84.107.11 riley.tivoli.com
   9.41.3.123 dfstest13.austin.lab.tivoli.com

3. To view stale entries found in the default database, enter:
   pdoshla -l stale
   The output is:
   # Internet Address Hostname
   9.41.3.123 dfstest13.austin.lab.tivoli.com

4. To flush stale entries from the default database, enter:
   pdoshla -f

5. To refresh all entries found in the default database, enter:
   pdoshla -u
pdoslpadm

Purpose
Perform administrative commands pertaining to the Tivoli Policy Director for Operating Systems Login Activity Database.

Syntax
pdoslpadm [-hvq?]
-r [-f] [-e | -d] [user [user ...]]
-m user [MMDDhhmm[([CC]YY]]]
-c [on | off] [-n {client | server} ]
-p [user [user ...]]
-x user [user ...]
-l user [user ...]
-u [-z] user [user ...]

Description
The pdoslpadm command aids in the administration of Login and Password Activity Policy local to a native UNIX system. After login policy has been configured in Tivoli Policy Director for Operating Systems, 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 system.

Use the -r option to generate a report detailing the status of the native UNIX user accounts that are recorded in the 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.

Note: The rhost name field displayed when using the -r and -f options might appear truncated. This is caused by the way the native login application stored the host information and has no effect on policy enforcement.

Use the -m option to modify the time of the Password Change Date recorded in the 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 MMDDhhmm[([CC]YY]] where:

- MM Month (00-12)
- DD Day (01-31)
- hh Hour (00-23)
- mm Minute (00 - 59)
- CC Century, either 20 or 21. Optional, defaults to current century.
- YY Year (00-99). Optional, defaults to current year.

The -m option is intended primarily for the support of policy which relies on the password change date, such as grace logins and minimum and maximum password age, on systems where password change dates for users are not provided. This situation occurs in
environments with distributed user registries, such as NIS, that do not return the password change date with the POSIX APIs. This situation also occurs on HP-UX systems that have not been configured to be trusted secure systems.

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 Login Activity Database is used only if the native UNIX password change date cannot be retrieved.

When the pdoslpadm command generates a report, the password change date that is currently in effect is displayed. If the date is the value stored in the Login Activity Database, a string is displayed to indicate this. If no date is specified in the user account record from the Tivoli Policy Director for Operating Systems 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 -c option to enable or disable configuration of Login Activity Policy on the local UNIX system. The optional -n option specifies whether the configuration change is occurring on an NIS server or on an NIS client.

The -c option, used in conjunction with the -n option, allows you to configure NIS support of password change dates in a Tivoli Policy Director for Operating Systems environment without having to manually specify password change dates for users using the -m option. To accomplish this, you must enable the support on the NIS server and on all NIS clients with Tivoli Policy Director for Operating Systems and Login Activity Policy enabled.

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 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 Login Activity Database record for the specified user account.

More information on the pdoslpadm command can be found in “Managing Login Activity Policy” on page 81.

Options

- v Displays the version number
- h Displays the usage message
- ? Displays the usage message
- q Run quietly, return only an exit status
- r Report the state of user accounts
- f Specifies a full report
- e Specifies a report of only unlocked (enabled) user accounts.
--- Specifies a report of only locked (disabled) user accounts.
-m Modifies the password change date for a user account to the current time or to the value specified in MMDDDhhssCCYY format.
-c Enable or disable specialized configuration for Login Activity Policy.
-n Used with the -c option to indicate whether the configuration change specified applies to an NIS server or to an NIS client.
-p Displays the policy for a specific exception.
-x Deletes a user record from the database.
-l Locks one or more user accounts
-u Unlocks one or more user accounts.
-z Clears (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 examples of pdoslpadm use:

1. To generate a report of all users in the Tivoli Policy Director for Operating Systems 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 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>
   ------------------------------

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 Login Activity Database, enter:
   
   `pdoslpadm -x anne`
pdosobjsig

Purpose
Manages the Tivoli Policy Director for Operating Systems Object Signature Database.

Syntax
```bash
pdosobjsig [-Vvh?] [-t trace-string] [-D DB-path] -g objname
[-D DB-path] -c objname
[-D DB-path] -u objname -s {trusted | untrusted}
[-D DB-path] -S {trusted | untrusted}
[-D DB-path] [-n] -l {all | trusted | untrusted}
```

Description
The `pdosobjsig` command displays, modifies, and checks the state of objects in the Tivoli Policy Director for Operating Systems Object Signature Database.

If the `-D` option is not specified, the default database is used. The default database resides in the `/var/pdos/tcb` directory. Objects in the database can be viewed by using the `-g` or `-l` options.

The `-g` option displays the state information for a specific object.

The `-l` option lists all objects found in the database according to the all, trusted, or untrusted qualifiers. By default, this produces a detailed listing of objects. Use the `-n` option to have only the names of the objects listed.

The `-u` in combination with the `-s` options or the `-S` option can change the state of objects found in the database. The `-u` option can be used to set the state of a specific object to either trusted or untrusted. The `-S` option can be used to set the state of all objects to either trusted or untrusted.

You cannot set the state of the `pdosobjsig` command to untrusted.

You must be a Tivoli Policy Director for Operating Systems runtime administrator to use this command.

Options
- `-V` Displays the version information.
- `-v` Displays verbose messages.
- `-h` Displays the usage message.
- `?-` Displays the usage message.
- `-t` `trace-string`
  Sets the trace string for displaying trace messages.
- `-g` `objname`
  Displays the state information for the specified object.
- `-c` `objname`
  Checks the state of the specified object.
- `-u` `objname` `-s {trusted | untrusted}`
  Updates the state of a specified object in the database.
-S Updates the state of all objects in the database.
-l Provides a detailed listing of objects in the database.
-n Used in conjunction with the -l option to list only the names of the objects in the database.

**Exit Status**

0 The command completed successfully.
1 An error occurred.

**Examples**

The following are examples of **pdosobjsig** usage:

1. To change the state of the object /anne/usertest in the default database, enter:

   ```
   pdosobjsig -u /anne/usertest -s untrusted
   ```

2. To display detailed information about all untrusted objects found in the default database, enter:

   ```
   pdosobjsig -l untrusted
   ```

   The output is:
   
   Object Name : /anne/usertest
   CRC sum : 279204844
   Inode 289 on device 10/5
   Permissions : rwxr-xr-x
   Owner : 0 : root
   Group : 0 :
   system Size : 6446
   Last status update time : Fri Sep 15 11:04:12 2000
   Last modification time : Fri Sep 15 11:04:12 2000
   State : Untrusted
   Reason : The Administrator changed the state explicitly.

3. To reset the state of the /anne/usertest object in the default database, enter:

   ```
   pdosobjsig -u /anne/usertest -s trusted
   ```

4. To set the state of all objects in the default database to trusted, enter:

   ```
   pdosobjsig -S trusted
   ```

5. To view the object, /anne/usertest, enter:

   ```
   pdosobjsig -g /anne/usertest
   ```

   The output is:
   
   Object Name : /anne/usertest
   State : Trusted
   Reason : The Administrator changed the state explicitly.
pdosrefresh

Purpose
Refreshes the Tivoli Policy Director for Operating Systems credentials for the specified users.

Syntax
```
pdosrefresh [-Vvh?] [-t trace-string] [-u uid] [-u uid ...] [-n name] [-n name ...]
```

Description
The `pdosrefresh` command refreshes the cached Tivoli Policy Director for Operating Systems credentials for the specified users.

If the `-u` or `-n` options are not specified, the credentials of the invoking user are refreshed. If the `-u` option is specified, the credentials for the user specified by the uid will be refreshed.

If the `-n` option is specified, the credentials for the user specified by the name will be refreshed. The `-u` and `-n` options can be specified multiple times on the same command line and can be used together.

You must be a Tivoli Policy Director for Operating Systems runtime administrator to use the `-u` or `-n` options of the `pdosrefresh` command.

Options
- `-V` Displays the version information.
- `-v` Displays verbose messages.
- `-h` Displays the usage message.
- `-?` Displays the usage message.
- `-t` trace-string Sets the trace string for displaying trace messages.
- `-u` uid Specifies the UID of the user whose credential is to be refreshed.
- `-n` name Specifies the UNIX name of the user whose credential is to be refreshed.

Exit Status
- `0` The command completed successfully.
- `1` An error occurred.

Examples
The following are examples of `pdosrefresh` usage:
1. To refresh the credentials of the invoking user, enter:
   `pdosrefresh`
2. To refresh the credentials of users anne and riley, whose UID is 300, enter:
   `pdosrefresh -n anne -u 300`
pdosrevoke

Purpose
Revokes an exemption from Tivoli Policy Director for Operating Systems authorization decisions.

Syntax
pdosrevoke [-Vvh?] [-t trace-string] [pid [pid ...]]

Description
The pdosrevoke command revokes an exemption from Tivoli Policy Director for Operating Systems authorization decisions that was previously granted by the pdosexempt command.

When the pdosrevoke command is invoked with no arguments, all processes running under the OSSEAL privileged user (osseal) lose their exemption from policy. This does not affect processes explicitly made immune by the pdosexempt command invoked with pid parameters.

If a pid or list of pids is specified on the pdosrevoke command line, the processes represented by those pids immediately lose their exemption from policy. The list of pids must occur last on the pdosrevoke command line.

There is no equivalent of the pdosexempt -i command line flag. All exempt processes must have their privilege explicitly revoked.

You must be a Tivoli Policy Director for Operating Systems runtime administrator to use this command.

Options
- V Displays the version information.
- v Displays verbose messages.
- h Displays the usage message.
- ? Displays the usage message.
- t trace-string Sets the trace string for displaying trace messages.

Exit Status
0 The command completed successfully.
1 An error occurred.

Examples
The following are examples of pdosrevoke usage:
1. To revoke the exemption granted to the OSSEAL privileged user by the pdosexempt command, enter:
   pdosrevoke
   The output is:
   User osseal (uid 1444) is no longer exempt from PDOS policy.
The uid might be different in your system.

2. To revoke the exemption granted by the `pdosexempt` command to the pid 9688, enter:
   
   ```
   pdosrevoke 9688
   ```

   The output is:
   
   ```
   Process 9688 is no longer exempt from PDOS policy.
   ```
**pdosrgyimp**

**Purpose**
Imports UNIX users and groups into the Tivoli Policy Director User Registry.

**Syntax**
```bash
```

**Description**
The `pdosrgyimp` command imports UNIX users and groups from the UNIX registry into the Tivoli Policy Director User Registry. All Tivoli Policy Director user accounts are set to valid by default. However, the `-d` option disables or invalidates the accounts. The password for each Tivoli Policy Director user account is set to invalid when it is created.

Command line options control which portions of the UNIX registry are to be imported. The `-u`, `-g` and `-a` options control whether users are imported, groups are imported, or both users and groups are imported. The default is to import both users and groups.

The `-I` option restricts the import to a specific set of users and groups found in the UNIX registry.

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

If an attempt is made to create a Tivoli Policy Director User Registry entry for a user that already exists, that user is excluded from the rest of the import. Any excluded users are not included when populating group memberships. If an attempt is made to create a Tivoli Policy Director User Registry entry for a group that already exists, the existing group is not populated with entries corresponding to the UNIX group membership. Use the `-r` flag to change this behavior.

As a part of importing UNIX groups into the Tivoli Policy Director User Registry, the Tivoli Policy Director group is populated with Tivoli Policy Director users, who are members of the UNIX group, which were not excluded either via command line options or a conflict. Use caution when importing groups separately from users.

The `-S` parameter is required on all imports. It specifies an existing Tivoli Policy Director User Registry suffix that will be used in the distinguished name (dn) for each user and group. Tivoli Policy Director users and groups are created using the following mapping:

- **user name**
  - UNIX-user-name

- **user cn**
  - UNIX-user-name

- **user sn**
  - UNIX-user-name
user dn
cn=pdos user UNIX-user-name, suffix

group name
UNIX-group-name

group cn
UNIX-group-name

group dn
cn=pdos group UNIX-user-name, suffix

The pdosrgyimp command produces two files in the current working directory named pdosrgyimp.import and pdosrgyimp.conflict. A record is written to the pdosrgyimp.import file for each user and group that is created in the Tivoli Policy Director User Registry. If an attempt is made to create a user or group that already exists in the Tivoli Policy Director User Registry, a record of that conflict will be written to the pdosrgyimp.conflict file.

These two files are written in the format of commands that can be sent to the pdadmin tool with comment lines detailing the actions. The pdosrgyimp.conflict file has a comment line explaining the failure followed by the pdadmin command that generated the conflict. For example:

```
# #
# create user failed
#
user create "test1" "cn=pdos user test1,ou=tivoli,o=ibm" "test1" "test1" "s12t"
```

An example taken from a pdosrgyimp.import file is:

```
# #
# create user
#
user create "riley" "cn=pdos user riley,ou=tivoli,o=ibm" "riley" "riley" "3AD4l00u"
user modify "riley" password-valid no
user modify "riley" account-valid yes
#
# create user
#
user create "maggie" "cn=pdos user maggie,ou=tivoli,o=ibm" "maggie" "maggie" "34pkjTaU"
user modify "maggie" password-valid no
user modify "maggie" account-valid yes
#
# create group
#
group create "canine" "cn=pdos group canine,ou=tivoli,o=ibm" "canine"
group modify "canine" add "riley"
group modify "canine" add "maggie"
```

The -n or noaction option generates a list of pdadmin style commands that would be executed had the -n option not been specified.

**Options**

- `-V` Displays the version information.
- `-v` Displays verbose messages.
- `-h` Displays the usage message.
-? Displays the usage message.
-\u Specified that only UNIX users should be imported.
-\g Specified that only UNIX groups should be imported.
-\a Specified that UNIX users and groups should be imported.
-\i Specified that when importing UNIX users and groups, if a matching LDAP entry
   exists, and that entry is not already a Tivoli Policy Director user or group entry, the
   entry should be imported from LDAP.
-\n Specified that no action should be taken. A list of \texttt{pdadmin} commands is generated.
-\r Specified that group membership for existing groups should be refreshed. If a group
   that was requested to be imported already exists in Tivoli Policy Director, any
   non-excluded user entries from the UNIX group will be added to the existing Tivoli
   Policy Director group.
-\d Disable all newly created Tivoli Policy Director user accounts.
-\G \texttt{default-group}
   Specifies the name of a Tivoli Policy Director Group of which all newly imported
   users will be members. If this group does not exist, it is created.
-\S \texttt{suffix-string}
   Specifies the Tivoli Policy Director Suffix that is to be appended to the common
   name when creating a distinguished name in the Tivoli Policy Director User
   Registry. This suffix must exist in the Tivoli Policy Director User Registry.
-\L \texttt{log-directory}
   Specifies the directory where the \texttt{pdosrgyimp.import} and the \texttt{pdosrgyimp.conflict}
   logs will be created.
-\E \texttt{exclude-file}
   Specifies a filename containing a list of UNIX users and groups to exclude from the
   import. The format of entries in the file follows:
   
   \begin{verbatim}
   # Comment characters
   USER UNIX_user_name
   USER UNIX_user_name
   GROUP UNIX_group_name
   GROUP UNIX_group_name
   ...
   \end{verbatim}
-\l \texttt{include-file}
   Specifies a filename containing a list of UNIX users and groups to include in the
   import. The format of entries in the file follows:
   
   \begin{verbatim}
   # Comment characters
   USER UNIX_user_name
   USER UNIX_user_name
   GROUP UNIX_group_name
   GROUP UNIX_group_name
   ...
   \end{verbatim}
-\P \texttt{password}
   Specifies a default password to be used for all Tivoli Policy Director user accounts
   that are created by this import.
Specifies the Tivoli Policy Director Administrator login ID to authenticate as. This user must be a member of the iv-admin group.

Specifies the password of the Tivoli Policy Director Administrator login ID. If you do not specify the password on the command line, you are prompted for it.

Exit Status

<table>
<thead>
<tr>
<th>Code</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>The command completed successfully.</td>
</tr>
<tr>
<td>1</td>
<td>An error occurred.</td>
</tr>
</tbody>
</table>

Examples

The following are examples of `pdosrgyimp` usage:

1. To import all users and groups from the UNIX registry, enter:
   ```bash
   pdosrgyimp -S o=ibm -l sec_master
   ```

2. To import all users and groups from the UNIX registry and refresh group membership for UNIX groups that previously existed in the Tivoli Policy Director User Registry, enter:
   ```bash
   pdosrgyimp -S o=ibm -l sec_master -r
   ```

3. To import all users and groups from the UNIX registry with the exception of those found in the exclude file named `exclude.1`, enter:
   ```bash
   pdosrgyimp -S o=ibm -l sec_master -E exclude.1
   ```

4. To import only those users and groups from the UNIX registry who are listed in the include file named `include.1`, enter:
   ```bash
   pdosrgyimp -S o=ibm -l sec_master -I include.1
   ```

5. To import only the users from the UNIX registry who are listed in the include file named `include.2` and add them as members of the group `default-group`, enter:
   ```bash
   pdosrgyimp -S o=ibm -l sec_master -u -I include.2 -G default-group
   ```

6. To import only the groups from UNIX registry who are listed in the include file named `include.2` and exclude the users listed in the exclude file named `exclude.2` from group membership, enter:
   ```bash
   pdosrgyimp -S o=ibm -l sec_master -g -I include.2 -E exclude.2
   ```
**pdosrstr**

**Purpose**
Restores Tivoli Policy Director for Operating Systems database and configuration files from a backup file.

**Syntax**
```
pdosrstr [-Vh?] -f filename
```

**Description**
The `pdosrstr` command restores Tivoli Policy Director for Operating Systems files that were previously saved using the `pdosbkup` command. Files are restored from the backup file specified by the `-f` option.

You must be a Tivoli Policy Director for Operating Systems runtime administrator to use this command.

**Options**
- `-V` Displays the version information.
- `-h` Displays the usage message.
- `-?` Displays the usage message.
- `-f filename` Specifies the name of the backup file.

**Exit Status**
- `0` The command completed successfully.
- `1` An error occurred.

**Examples**
The following is an example of `pdosrstr` usage:

1. To restore files saved in the `pdosbkup25ct2001.14_32_41.tar` file in the default directory, enter:

   ```
   ```
**pdossudo**

**Purpose**
Invoke a command as the root UNIX user.

**Syntax**

```
pdossudo [-Vvh?] [-t trace-string] command-alias [arg [arg ...]]
```

**Description**

The pdossudo command lets an authorized user invoke a command that would otherwise require UNIX privileges that the invoking UNIX user does not possess. The invoker must pass the following authorization checks before the command is executed:

- The prevailing PDOS user must have permission to surrogate to the target user as specified in the extended attributes of the Sudo protected object.
- The prevailing PDOS user must have execute permission on the specified sudo-command (or matching subordinate argument class if an ACL is present).
- The arguments satisfy any constraints specified in a matching argument class.

You must be a Tivoli Policy Director for Operating Systems runtime administrator to use this command.

**Options**

- `-V` Displays the version information.
- `-v` Displays verbose messages.
- `-h` Displays the usage message.
- `?-` Displays the usage message.
- `-t trace-string`
  Sets the trace string for displaying trace messages.

**Exit Status**

- `0` The command completed successfully.
- `1` An error occurred.

**Examples**

See "An Example of Sudo Usage" on page 43 for an example of setting up a command for pdossudo use.
pdosteccfg

Purpose

Configures PDOSTECD, the Tivoli Enterprise Console Daemon.

Syntax

```
```

Description

The `pdosteccfg` command is used to configure the PDOSTECD daemon.

The PDOSTECD daemon uses the `/var/pdos/audit/audit.log` file as input for its processing. This file must exist and be accessible to the PDOSTECD daemon, otherwise the daemon shuts down. Restart the PDOSTECD daemon after making the `audit.log` file available again.

You must be a Tivoli Policy Director for Operating Systems runtime administrator to use this command.

Options

- `-v` Displays the version information.
- `-h` Displays help for each of the options.
- `-?` Displays the usage message.
- `-autostart` Indicates whether the PDOSTECD daemon should start automatically or not.
- `-burst` Maximum number of events that the daemon should process at a time.
- `-delay` Number of seconds to wait when no events are available.
- `-delete` Deletes the specified options from the current configuration. One or more of the following, separated by commas, can be specified: `burst, delay, interval, log_entries, or logs`.
- `-help` Displays help for each of the options.
- `-interval` Number of seconds to wait after processing events before checking for the arrival of new events.
-log_entries  Number of pdostecd.log entries to use before rolling over to a new log. A value of 0, the default, means never roll over to a new log.

-logs  Number of pdostecd.log files to use before recycling log files. A value of 0 indicates that log files should never be recycled. This option only has an effect if log_entries is nonzero.

-operations  Displays the command options available.

-rspfile  Name of a file containing option values for the configuration. Options specified on the command line override options specified in the response file.

-sec_master_pwd  Tivoli Policy Director security master password.

-usage  Displays the usage message.

-version  Displays the version information.

Exit Status

0  The command completed successfully.

1  An error occurred.

Examples

To have the PDOSTECD daemon start automatically:

dostecfg -autostart on
**pdostecucfg**

**Purpose**
Unconfigures PDOSTECD, the Tivoli Enterprise Console Daemon.

**Syntax**

```
pdostecucfg [-help]
            [-operations]
            [-remove_per_policy (on | off)]
            [-rspfile file_name]
            [-sec_master_pwd Policy_Director_password]
            [-usage]
            [-version]
            [-?]
```

**Description**

The `pdostecucfg` command is used to unconfigure the PDOSTECD daemon. The PDOSTECD daemon must be unconfigured before using the `pdosucfg` command to unconfigure Tivoli Policy Director for Operating Systems.

You must be a Tivoli Policy Director for Operating Systems runtime administrator to use this command.

**Options**

- `--help` Displays help for all of the options. To display help for one option, type `--help --option`.
- `--operations` Lists the supported options.
- `--remove_per_policy` Unregister the policy branch specific Tivoli Policy Director for Operating Systems information this machine is configured to use. Do not specify, if other Tivoli Policy Director for Operating Systems machines are configured under that policy branch. Doing so could make the machine inoperable. If additional policy has been added under that policy branch, you might need to remove it manually.

  Default: off

- `--rspfile` File containing option values for the unconfiguration.

- `--sec_master_pwd` Tivoli Policy Director security master password.

- `--usage` Displays help on the command’s usage.

- `--version` Displays the version.

- `--?` Displays help on the command’s usage.

**Exit Status**

```
0 The command completed successfully.
```
An error occurred.
pdosucfg

Purpose
Unconfigures Tivoli Policy Director for Operating Systems.

Syntax

 :

[pdosucfg | –help]
[–operations]
[–remove_once_only (on | off)]
[–remove_per_policy (on | off)]
[–rspfile file_name]
[–sec_master_pwd Policy_Director_password]
[–usage]
[–version]
[–?]  

Description
The pdosucfg command is used to unconfigure the PDOSD daemon. The PDOSTECD daemon must be unconfigured using the pdostecucfg command before unconfiguring Tivoli Policy Director for Operating Systems. See pdostecucfg on page 183.

You must be a Tivoli Policy Director for Operating Systems runtime administrator to use this command.

Options

–help Displays help for all of the options. To display help for one option, type –help –option.

–operations Lists the supported options.

–remove_once_only
Unregister the Tivoli Policy Director for Operating Systems product policy. Do not specify, if other Tivoli Policy Director for Operating Systems machines are configured to this Tivoli Policy Director server, because it could make the other machines inoperable. If additional policy has been added, you may need to remove it manually.

 Default: off

–remove_per_policy
Unregister the policy branch specific Tivoli Policy Director for Operating Systems information this machine is configured to use. Do not specify, if other Tivoli Policy Director for Operating Systems machines are configured under that policy branch. Doing so could make the machine inoperable. If additional policy has been added under that policy branch, you might need to remove it manually.

 Default: off

–rspfile
File containing option values for the unconfiguration.

–sec_master_pwd
Tivoli Policy Director security master password.
–usage
Displays help on the command’s usage.

–version
Displays the version.

–?
Displays help on the command’s usage.

Exit Status

0  The command completed successfully.
1  An error occurred.
pdosuidprog

Purpose
Identifies setuid or setgid programs on a system so that an administrator can decide whether
they should be included in the Trusted Computing Base (TCB).

Syntax
pdosuidprog

pdosuidprog [-Vvh?]
[-t trace-string]
-l [-H] [-s] [-x dir [-x dir ...]] [directories [directories ...]]
-g [-c class-name][-H][-s] [-p policy-name] [-x dir [-x dir...]] [directories ...]

Description
The pdosuidprog command searches the specified directories for setuid and setgid
programs. If no directories are specified on the command line, the search begins in the
current directory and descends all of the directories under it. This command does not search
the /dev directory on any system nor the /proc directory on Solaris or Linux systems.

Multiple directories can be searched by specifying them on the command line. If directories
are specified they must be last on the command line. Directories that should not be
descended should be specified with the -x option.

The pdosuidprog command relies on the operating system to detect circular linked directory
structures. The command continues to descend through the directory structure until the
operating system denies the request. Circular linked directory structures should be excluded
from the search using the -x option.

The format of the output produced by the pdosuidprog command depends on whether the -l
or the -g option is specified. If the -l option is specified, the pdosuidprog command
generates a list of all of the setuid and setgid programs that were found. The list includes the
filename, the uid for setuid programs and the gid for setgid programs.

If the -H option is specified with the -l option, any duplicate hard links that are found are
not listed.

The -l option cannot be used with the -g option and either -l or -g must be specified. If the
-g option is specified, the pdosuidprog command generates a list of pdadmin commands
that are required to place the setuid and setgid programs in the Trusted Computing Base
(TCB).

If the -H option is specified with the -g option, commands generated for duplicate hard links
are in the form of a comment.

The default class used to generate the Tivoli Policy Director for Operating Systems TCB
entry commands is Secure-Programs. However it can be changed using the -c option
followed by the class name. Valid entries for class-name are:
- Login-Programs
- Secure-Files
- Secure-Programs
- Impersonator-Programs
- Immune-Programs
The default policy branch name used to generate the TCB object create commands is obtained from the osseal.conf file. The policy branch name can be changed by using the -p option.

You must be a Tivoli Policy Director for Operating Systems runtime administrator to use this command.

**Options**

- **-V** Displays the version information.
- **-v** Displays verbose messages.
- **-h** Displays the usage message.
- **-?** Displays the usage message.
- **-t trace-string** Sets the trace string for displaying trace messages.
- **-l** Generate a list of filenames.
- **-g** Generate pdadmin object creation commands.
- **-H** Do not generate duplicates for hard links.
- **-s** Do not traverse symbolic links to other filesystems.
- **-c class-name** Specifies the class name to be used in the pdadmin object creation commands.
- **-p policy-name** Specifies the policy branch name to be used in the pdadmin object creation commands.
- **-x dir** Specifies a directory that should not be descended in the search, the directory name must be a fully-qualified pathname.

**Exit Status**

<table>
<thead>
<tr>
<th>Status Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>The command completed successfully.</td>
</tr>
<tr>
<td>1</td>
<td>An error occurred.</td>
</tr>
</tbody>
</table>

**Examples**

The following are examples of **pdosuidprog** usage:

1. To search the current directory for setuid and setgid programs and generate a list of files, enter:

   ```
   pdosuidprog -l
   ```

   The output is:

   ```
   /opt/pdos/bin/pdosunauth : 1444 : 228
   /opt/pdos/bin/pdosrefresh : 1444 : 228
   /opt/pdos/bin/pdosdestroy : 1444 : 228
   /opt/pdos/bin/pdoswhoami : : 228
   /opt/pdos/bin/pdoswhois : 1444 : 228
   /opt/pdos/bin/pdossudo : 0 : 228
   /opt/pdos/bin/pdosexempt : 1444 : 228
   /opt/pdos/bin/pdosrevoke : 1444 : 228
   /opt/pdos/bin/pdosctl : : 228 /opt/pdos/bin/pdosd : 0 : 228
   /opt/pdos/bin/pdoswdd : 0 : 228
   /opt/pdos/bin/pdosauditd : 0 : 228
   ```
2. To search the /opt directory for setuid and setgid programs without descending /opt/pdos/bin, generating a list of **pdadmin** commands for policy branch testbranch, enter:

```
pdosuidprog -g -x /opt/pdos/bin -p testbranch /opt
```

The output (formatted to fit on the printed page) is:

```
object create \
   /OSSEAL/testbranch/TCB/Secure-Programs /opt/local/bin/ansuprog \n   "" 2 ispolicyattachable yes
```
pdosunauth

**Purpose**
Spawns a shell that executes commands in an unauthenticated environment.

**Syntax**

```
pdosunauth [-Vvh?]
            [-t trace-string]
            [command]
```

**Description**
The `pdosunauth` command spawns a shell that is treated as unauthenticated for the purposes of Tivoli Policy Director for Operating Systems authorization decisions. This command allows a program to be tested in an unauthenticated environment. If a `command` is specified, the shell is spawned to execute only that command.

**Options**

- `-V` Displays the version information.
- `-v` Displays verbose messages.
- `-h` Displays the usage message.
- `-?` Displays the usage message.
- `-t trace-string`
  Sets the trace string for displaying trace messages.

  `command`
  The name of the command to be executed.

**Exit Status**

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>The command completed successfully.</td>
</tr>
<tr>
<td>1</td>
<td>An error occurred.</td>
</tr>
</tbody>
</table>

**Examples**

1. To invoke a shell that can be used to invoke commands as an unauthenticated user, enter:
   ```
pdosunauth
   ```
2. To list the contents of the `/var/pdos/cred` directory as an unauthenticated user, enter:
   ```
pdosunauth ls /var/pdos/cred
   ```
   The output is:
   ```
ls: /var/pdos/cred:
The file access permissions do not allow the specified action.
```
pdosversion

Purpose
Displays the version information for Tivoli Policy Director for Operating Systems.

Syntax
pdosversion

Description
The pdosversion command displays the version information for Tivoli Policy Director for Operating Systems including the versions of the shared libraries.

Exit Status
0 The command completed successfully.
1 An error occurred.

Examples
To display the Tivoli Policy Director for Operating Systems version information, enter:
pdosversion

The output is similar to the following:
Policy Director for Operating Systems 3.8.0
pdosversion 3.8.0.0 (011203a)
libosseald 3.8.0.0 (011203a)
libosseal 3.8.0.0 (011203a)
libkoseal 3.8.0.0 (011203a)
pdoswhoami

Purpose
Displays the Tivoli Policy Director for Operating Systems accessor ID information.

Syntax
pdoswhoami [-Vvh?] [-t trace-string] [-n | a | l]

Description
The pdoswhoami command displays Tivoli Policy Director for Operating Systems accessor information about the invoking user.

With no specified options, the pdoswhoami command displays the invoking user’s Tivoli Policy Director for Operating Systems user name.

The -n option displays the invoking user’s accessor ID.

The -a option displays both the invoking user’s accessor ID and name.

The -l option displays the invoking user’s accessor ID, Tivoli Policy Director for Operating Systems name and the following credential information:
- Tivoli Policy Director for Operating Systems Group membership information
- The time that the credential was last refreshed
- The credential’s refresh expiry
- The time that the credential was last accessed
- The credential’s hold time expiry

Options
-V Displays the version information.
-v Displays verbose messages.
-h Displays the usage message.
-? Displays the usage message.
-t trace-string Sets the trace string for displaying trace messages.
-n Displays the accessor’s UID.
-a Displays the accessor’s UID and name.
-l Displays the accessor’s UID, name and PDOS credential information.

Exit Status
0 The command completed successfully.
1 An error occurred.

Examples
The following are examples of pdoswhoami usage:
1. To display the Tivoli Policy Director for Operating Systems accessor name of the invoking user, enter:
   ```bash
pdoswhoami
   ```
   The output is: riley.

2. To display the Tivoli Policy Director for Operating Systems accessor name and UID of the invoking user, enter:
   ```bash
   pdoswhoami -a
   ```
   The output is: 204 riley.

3. To display the Tivoli Policy Director for Operating Systems accessor name, UID and credential information of the invoking user, enter:
   ```bash
   pdoswhoami -l
   ```
   The output is:
   ```bash
   204 riley
   The credential is associated with the following groups: staff
   The credential was last refreshed at Wed Oct 25 08:21:40 2001
   The credential refresh time expires at Wed Oct 25 08:41:40 2001
   The credential was last accessed at Wed Oct 25 08:31:20 2001
   The credential hold time expires at Wed Oct 25 08:56:20 2001```
**pdoswhois**

**Purpose**
Displays Tivoli Policy Director for Operating Systems accessor ID information associated with the specified process ids.

**Syntax**

```
pdoswhois [-Vvh?]  
[-t trace-string]  
[-l] pid [pid [pid ...]]
```

**Description**

The `pdoswhois` command displays the Tivoli Policy Director for Operating Systems accessor ID information about the specified process ID list. The list of pids must occur last on the `pdoswhois` command line. The Tivoli Policy Director for Operating Systems accessor ID and accessor user ID for each specified process are displayed.

If the `-l` option is specified, the `pdoswhois` command also displays the following credential information for each specified process:

- Tivoli Policy Director for Operating Systems Group membership information
- The time that the credential was last refreshed
- The credential’s refresh expiry
- The time that the credential was last accessed
- The credential’s hold time expiry

**Options**

- `-V`  Displays the version information.
- `-v`  Displays verbose messages.
- `-h`  Displays the usage message.
- `?-` Displays the usage message.
- `-t trace-string`  
  Sets the trace string for displaying trace messages.
- `-l`  Displays the Tivoli Policy Director for Operating Systems accessor UID, accessor name and credential information associated with each specified process.

**Exit Status**

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>The command completed successfully.</td>
</tr>
<tr>
<td>1</td>
<td>An error occurred.</td>
</tr>
</tbody>
</table>

**Examples**

1. To display the Tivoli Policy Director for Operating Systems accessor ID information for a single process, enter:

   `pdoswhois 170358`

   The output is:

   Pid, 170358, is running under the uid = 204, user name = riley
2. To display the Tivoli Policy Director for Operating Systems accessor ID information for multiple processes, enter:

```
pdoswhois 170358 53804 219134
```

The output is:

```
Pid, 170358, is running under the uid = 204, user name = riley.
The process with pid, 53804, is running as unauthenticated.
Pid, 219134, is running under the uid = 0, user name = root.
```

3. To display the Tivoli Policy Director for Operating Systems accessor ID information for multiple processes along with the credential information, enter:

```
pdoswhois -l 170358 219134
```

The output (formatted to fit the printed page) is:

```
Pid, 170358, is running under the uid = 204, user name = riley.
The credential is associated with the following groups: staff
The credential was last refreshed at Wed Oct 25 08:56:39 2000
The credential was last accessed at Wed Oct 25 08:40:12 2000
The credential hold time expires at Wed Oct 25 09:05:12 2000

Pid, 219134, is running under the uid = 0, user name = root.
The credential is associated with the following groups:
  osseal-admin osseal-auditors
The credential was last refreshed at Wed Oct 25 08:59:05 2000
The credential refresh time never expires.
The credential was last accessed at Wed Oct 25 09:00:51 2000
The credential hold time never expires.
```
Integrating with Tivoli Enterprise Console

Tivoli Policy Director for Operating Systems provides the ability to generate Tivoli Enterprise Console events. This chapter provides an overview of auditing in the UNIX environment and provides information about how to configure the Tivoli Enterprise Console logfile adapter to send Tivoli Enterprise Console events for Tivoli Policy Director for Operating Systems. For more information about Tivoli Enterprise Console, and the list of supported operating system platforms, see the *Tivoli Enterprise Console Users’s Guide*.

### Auditing Overview

Tivoli Policy Director for Operating Systems handles auditing tasks and generates Tivoli Enterprise Console events. To integrate Tivoli Policy Director for Operating Systems with the functionality of Tivoli Enterprise Console, the Tivoli Policy Director for Operating Systems Enterprise Console Integration product must be installed on the following machines:

- The Tivoli management region server
- The Tivoli Enterprise Console event server
- Any managed node that is a gateway to a machine running Tivoli Policy Director for Operating Systems

Additionally, the Tivoli Enterprise Console logfile adapter for Tivoli Policy Director for Operating Systems must be installed on the endpoints that have Tivoli Policy Director for Operating Systems installed. For information about installing Tivoli Policy Director for Operating Systems Enterprise Console Integration, see the *Tivoli Policy Director for Operating Systems Installation Guide*. For information about installing the Tivoli Enterprise Console logfile adapter, refer to the following section.

**Note:** Refer to the Tivoli Enterprise Console documentation to determine the system requirements that must be met to run Tivoli Enterprise Console on a given operating system platform. The Tivoli Policy Director for Operating Systems Enterprise Console Integration component can be installed on any supported Tivoli Enterprise Console system.

After Tivoli Policy Director for Operating Systems Enterprise Console Integration has been installed, the PDOSTECD daemon must be configured and started. The endpoints and the event server must be configured to send and receive Tivoli Enterprise Console events for Tivoli Policy Director for Operating Systems. If this configuration is not done, events from Tivoli Policy Director for Operating Systems will not be received.
Notes:

1. If no auditing is being done, no events will be generated, regardless of whether required software has been installed and configured. By default, however, resource access failures are audited.

2. The Tivoli Enterprise Console event server may be configured to receive and process one or both Tivoli Enterprise Console events and Tivoli Risk Manager events from Tivoli Policy Director for Operating Systems endpoints. However, each Tivoli Policy Director for Operating Systems endpoint can only be configured to send either Tivoli Enterprise Console events or Tivoli Risk Manager events.

3. The /var/pdos/audit/audit.log file is the source for the PDOSTECD daemon. If this file is removed or becomes unavailable, the PDOSTECD daemon shuts down and no further events are processed. After making the file available again, restart the PDOSTECD daemon to resume the processing of events.

Installing and Configuring the Logfile Adapter

The Tivoli Enterprise Console logfile adapter for Tivoli Policy Director for Operating Systems executables and other files are installed on the endpoint through the Adapter Configuration Facility.

Notes:

1. The logfile adapter for Tivoli Policy Director for Operating Systems can be installed only on endpoints. To generate events from a managed node, you must make the managed node an endpoint as well.

2. Refer to the Tivoli Enterprise Console documentation to determine the system requirements that must be met to run Tivoli Enterprise Console on a given operating system platform. The Tivoli Policy Director for Operating Systems Enterprise Console Integration component can be installed on any supported Tivoli Enterprise Console system.

3. The root user has to be defined as a Tivoli Policy Director for Operating Systems runtime administrator during distribution of the PDOS-ACPROF profile for the setup to complete successfully.

The process of installing Tivoli Policy Director for Operating Systems Enterprise Console Integration creates an adapter configuration profile (PDOS-ACPROF) in the PDOS profile manager and adds a tecad_logfile_pdos record to that profile. For more information on the Adapter Configuration Facility, refer to the Tivoli Enterprise Console User’s Guide.

Use the following steps to complete the integration process:

1. Distribute PDOS-ACPROF to all the Tivoli Policy Director for Operating Systems endpoints on which you want to generate Tivoli Enterprise Console events.
   After this profile has been successfully distributed, the Tivoli Enterprise Console logfile adapter for Tivoli Policy Director for Operating Systems will be started automatically.

2. Use the Setup TEC Event Server for PDOS job to set up the event server so that it can receive and process Tivoli Enterprise Console events for Tivoli Policy Director for Operating Systems.
   For more information, see “Setup TEC Event Server for PDOS” on page 122.
3. Configure and start the PDOSTECD daemon. See “The PDOSTECD Tivoli Enterprise Console Daemon” on page 59 for details.

After the Setup TEC Event Server for PDOS job has been successfully executed, the Tivoli Enterprise Console event console will start receiving Tivoli Policy Director for Operating Systems events. All the Tivoli Policy Director for Operating Systems audit events are accessible through the LOGFILE event source.

To stop the Tivoli Enterprise Console logfile adapter for Tivoli Policy Director for Operating Systems, go to the /etc/Tivoli/tecad/pdos/bin directory and run stop_tecad_pdos. Or, you can use the Stop TEC Adapter job. To restart the logfile adapter, run start_tecad_config_pdos from the same directory. Or, you can use the Start TEC Adapter job. The Tivoli Enterprise Console logfile adapter subsequently restarts automatically on system reboot.

For more information, see “Start TEC Adapter” on page 128 and “Stop TEC Adapter” on page 128.
Integrating with Tivoli Risk Manager

Tivoli Policy Director for Operating Systems provides the ability to generate Tivoli Risk Manager events. This chapter provides an overview of auditing in the UNIX environment and provides information about how to configure the Tivoli logfile adapter to send Tivoli Risk Manager events for Tivoli Policy Director for Operating Systems. For more information about Tivoli Risk Manager, see the *Tivoli Risk Manager User’s Guide*.

**Auditing Overview**

Tivoli Policy Director for Operating Systems handles auditing tasks and generates Tivoli Risk Manager events. To integrate Tivoli Policy Director for Operating Systems with the functionality of Tivoli Risk Manager, the Tivoli Policy Director for Operating Systems Enterprise Console Integration must be installed on the following machines:

- The Tivoli management region server
- The Tivoli Enterprise Console event server
- Any managed node that is a gateway for a machine running Tivoli Policy Director for Operating Systems

Additionally, the Tivoli logfile adapter for Tivoli Policy Director for Operating Systems must be installed on the endpoints that have Tivoli Policy Director for Operating Systems installed. For information about installing Tivoli Policy Director for Operating Systems Enterprise Console Integration, see the *Tivoli Policy Director for Operating Systems Installation Guide*. Information about installing the Tivoli logfile adapter is contained in the next section of this document.

After Tivoli Policy Director for Operating Systems Enterprise Console Integration has been installed, the endpoints and the event server must be configured to send and receive Tivoli Risk Manager events for Tivoli Policy Director for Operating Systems. If this configuration is not done, events from Tivoli Policy Director for Operating Systems will not be received.

**Notes:**

1. If no auditing is being done, no events will be generated, regardless of whether required software has been installed and configured. By default, however, resource access failures are audited.

2. The Tivoli Enterprise Console event server may be configured to receive and process one or both Tivoli Enterprise Console events and Tivoli Risk Manager events from Tivoli Policy Director for Operating Systems endpoints. However, each Tivoli Policy Director for Operating Systems endpoint can only be configured to send either Tivoli Enterprise Console events or Tivoli Risk Manager events.
3. The /var/pdos/audit/audit.log file is the source for the PDOSTECD daemon. If this file is removed or becomes unavailable, the PDOSTECD daemon shuts down and no further events are processed. After making the file available again, restart the PDOSTECD daemon to resume the processing of events.

Installing and Configuring the Logfile Adapter to Integrate with Tivoli Risk Manager

The Tivoli logfile adapter for Tivoli Policy Director for Operating Systems executables and other files are installed on the endpoint through the Adapter Configuration Facility.

Notes:

1. The Tivoli logfile adapter for Tivoli Policy Director for Operating Systems can be installed only on endpoints. To generate events from a managed node, you must make the managed node an endpoint as well.

2. Refer to the Tivoli Enterprise Console documentation to determine the system requirements that must be met to run Tivoli Enterprise Console on a given operating system platform. The Tivoli Policy Director for Operating Systems Enterprise Console Integration component can be installed on any supported Tivoli Enterprise Console system.

3. The root user has to be defined as a Tivoli Policy Director for Operating Systems runtime administrator during distribution of the PDOS-RISKMGR-ACPROF profile for the setup to complete successfully.

The process of installing Tivoli Policy Director for Operating Systems Enterprise Console Integration creates an adapter configuration profile (PDOS-RISKMGR-ACPROF) in the PDOS profile manager and adds a tecad_logfile_pdos_riskmgr record to that profile. For more information on the Adapter Configuration Facility, refer to the Tivoli Enterprise Console User’s Guide.

Use the following steps to complete the integration process:

1. Distribute PDOS-RISKMGR-ACPROF to all the Tivoli Policy Director for Operating Systems endpoints from which you want to send Tivoli Risk Manager events. After this profile has been successfully distributed, the Tivoli logfile adapter for Tivoli Policy Director for Operating Systems will be started automatically.

2. Use the Setup TEC Event Server for PDOS job to set up the event server so that it can receive and process Tivoli Risk Manager events for Tivoli Policy Director for Operating Systems. For more information, see “Setup TEC Event Server for PDOS” on page 122.

3. If the Tivoli Enterprise Console event server in your environment is running on a Microsoft Windows NT system, you must customize the $BINDIR/RISKMGR/corr/riskmgr_baroc.lst file to include the pdosrm.baroc file. Include the pdos.baroc file also if the event server should send events to the Tivoli Enterprise Console as well. Make your changes effective by entering the following commands in a bash shell from the event server after running this task:

   cd $BINDIR/RISKMGR/corr
cp ../../generic_unix/TME/PDOSTASKS/pdosrm.baroc ./tec
cp ../../generic_unix/TME/PDOSTASKS/pdos.baroc ./tec
./rmcorr_cfg -update
After the **Setup TEC Event Server for PDOS** job has been successfully executed, the Tivoli Enterprise Console event console will start receiving Tivoli Policy Director for Operating Systems events. All the Tivoli Policy Director for Operating Systems audit events are accessible through the LOGFILE event source.

To stop the Tivoli logfile adapter for Tivoli Policy Director for Operating Systems, go to the `/etc/Tivoli/tecad/pdos/bin` directory and run `stop_tecad_pdos`, or you can use the **Stop TEC Adapter** job. To restart the logfile adapter, run `start_tecad_config_pdos` from the same directory, or you can use the **Start TEC Adapter** job. The Tivoli logfile adapter for Tivoli Policy Director for Operating Systems will restart automatically on system reboot.

For more information, see “**Start TEC Adapter**” on page 128 and “**Stop TEC Adapter**” on page 128.
### Table 47. System Resources and Corresponding Tivoli Policy Director for Operating Systems Resource Types

<table>
<thead>
<tr>
<th>Resource Type</th>
<th>Resource Type Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>File system resources</td>
<td>File</td>
</tr>
<tr>
<td>Network Resources</td>
<td>NetIncoming</td>
</tr>
<tr>
<td></td>
<td>NetOutgoing</td>
</tr>
<tr>
<td>Login Resources</td>
<td>Login/Terminal/Local</td>
</tr>
<tr>
<td></td>
<td>Login/Terminal/Remote</td>
</tr>
<tr>
<td></td>
<td>Login/Holidays</td>
</tr>
<tr>
<td>Surrogate Resources</td>
<td>Surrogate</td>
</tr>
<tr>
<td>Sudo Resources</td>
<td>Sudo</td>
</tr>
<tr>
<td>Trusted Computing Base Resources</td>
<td>TCB/Login-Programs</td>
</tr>
<tr>
<td></td>
<td>TCB/Secure-Files</td>
</tr>
<tr>
<td></td>
<td>TCB/Secure-Programs</td>
</tr>
<tr>
<td></td>
<td>TCB/Impersonator-Programs</td>
</tr>
<tr>
<td></td>
<td>TCB/Immune-Programs</td>
</tr>
</tbody>
</table>

### Table 48. Tivoli Policy Director for Operating Systems Permissions Defined in the [OSSEAL] Action Group

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
<th>Tivoli Policy Director for Operating Systems resource type</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>Connect</td>
<td>NetIncoming and NetOutgoing</td>
</tr>
<tr>
<td>D</td>
<td>Change directory</td>
<td>File</td>
</tr>
<tr>
<td>G</td>
<td>Surrogate</td>
<td>Surrogate</td>
</tr>
<tr>
<td>K</td>
<td>Kill program</td>
<td>File</td>
</tr>
<tr>
<td>L</td>
<td>Login</td>
<td>Login</td>
</tr>
<tr>
<td>N</td>
<td>Create</td>
<td>File</td>
</tr>
<tr>
<td>R</td>
<td>Rename</td>
<td>File</td>
</tr>
<tr>
<td>U</td>
<td>Update timestamp</td>
<td>File</td>
</tr>
<tr>
<td>d</td>
<td>Delete</td>
<td>File</td>
</tr>
<tr>
<td>l</td>
<td>List directory</td>
<td>File</td>
</tr>
<tr>
<td>o</td>
<td>Change ownership</td>
<td>File</td>
</tr>
<tr>
<td>p</td>
<td>Change permission</td>
<td>File</td>
</tr>
<tr>
<td>r</td>
<td>Read</td>
<td>File</td>
</tr>
<tr>
<td>w</td>
<td>Write</td>
<td>File</td>
</tr>
<tr>
<td>x</td>
<td>Execute</td>
<td>File and Sudo</td>
</tr>
</tbody>
</table>
Table 49. Policy Director Primary Actions Used for Policy Management

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>a</td>
<td>Attach an ACL or POP</td>
</tr>
<tr>
<td>b</td>
<td>Browse object space and see object names</td>
</tr>
<tr>
<td>c</td>
<td>Control or modify an ACL</td>
</tr>
<tr>
<td>d</td>
<td>Delete an object</td>
</tr>
<tr>
<td>m</td>
<td>Modify an object’s attributes</td>
</tr>
<tr>
<td>v</td>
<td>View the attributes of an object</td>
</tr>
</tbody>
</table>

Table 50. Policy Director Primary Actions Used for Policy Decisions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>Bypass time-of-day restriction</td>
</tr>
<tr>
<td>T</td>
<td>Traverse</td>
</tr>
</tbody>
</table>
The wildcard character set expressions comply with the POSIX Regular Expression (RE) bracket expression definition. Table 51 summarizes this definition.

**Table 51. Special Elements of Wildcard Character Set**

<table>
<thead>
<tr>
<th>Character Set Element</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>^ (circumflex)</td>
<td>A circumflex introduces a set of characters to exclude from the character set. Characters following it will not match the character set. The circumflex character only has this special meaning if it is the first character in the character set. Otherwise it simply represents the circumflex character itself.</td>
<td>^[a-z] matches everything except lower case ASCII characters. [ab^] matches 'a', 'b' or '^'.</td>
</tr>
<tr>
<td>] (right bracket)</td>
<td>The right bracket character normally terminates the character set. When it appears as the first character in the character set it represents the right bracket character.</td>
<td>[] matches the ']' character. [a] is an invalid expression.</td>
</tr>
<tr>
<td>[.collating-symbol.]</td>
<td>The [..] brackets allow specification of a collating symbol that does not consist of a single character. For example [.ch.]. If the string enclosed in the [..] brackets is not a valid collating symbol the expression will be treated as invalid.</td>
<td>[[.ch.]]+c matches the string &quot;chchc&quot; but not &quot;hc&quot; or &quot;cc&quot;. [[.qx.]] is an invalid expression</td>
</tr>
<tr>
<td>[=equivalence-class=]</td>
<td>The [= =] brackets allow specification of a character equivalence class. A character's equivalence class consists of all characters matching independent of case, umlauts, graves, and so forth.</td>
<td>[[=a=]] matches 'a', 'A', 'A' and other A characters.</td>
</tr>
</tbody>
</table>
Table 51. Special Elements of Wildcard Character Set (continued)

<table>
<thead>
<tr>
<th>Character Set Element</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>[:character-class:]</td>
<td>The [:] brackets allow specification of an entire class of characters. Valid character classes are those characters relevant to the LC_CTYPE category of the locale in which policy is being enforced. The character classes valid in all locales are shown in Table 52. Character classes specific to the locale in which PDOSD is running are also supported.</td>
<td>[[:digit:]] matches any digit. [[:lower:]] is equivalent to [a-z] in the C locale but will, for example, include characters such as the cedilla (,) in French locales.</td>
</tr>
</tbody>
</table>

Table 52. Wildcard Character Set Character Classes Valid for all Locales

<table>
<thead>
<tr>
<th>Character Class</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>[:alnum:]</td>
<td>Alphabetic characters and decimal digits</td>
<td>'a', 'A', '6'</td>
</tr>
<tr>
<td>[:alpha:]</td>
<td>Alphabetic characters</td>
<td>'a', 'A', 'Z'</td>
</tr>
<tr>
<td>[:blank:]</td>
<td>Blank characters</td>
<td>space, tab, newline</td>
</tr>
<tr>
<td>[:cntrl:]</td>
<td>ASCII control characters</td>
<td>^A, ^C</td>
</tr>
<tr>
<td>[:digit:]</td>
<td>Decimal digits</td>
<td>'0', '1', '2', '3'</td>
</tr>
<tr>
<td>[:graph:]</td>
<td>Graphical characters</td>
<td></td>
</tr>
<tr>
<td>[:lower:]</td>
<td>Lower case characters</td>
<td>'a', 'b', 'c'</td>
</tr>
<tr>
<td>[:print:]</td>
<td>Printable characters</td>
<td>Anything matching [:alnum:], [:graph:], [:punct:] or the space character and that do not match [:cntrl:]</td>
</tr>
<tr>
<td>[:punct:]</td>
<td>Punctuation characters</td>
<td>, , .</td>
</tr>
<tr>
<td>[:space:]</td>
<td>White space characters: space and tab</td>
<td>space, tab</td>
</tr>
<tr>
<td>[:upper:]</td>
<td>Uppercase characters</td>
<td>'A', 'B', 'C'</td>
</tr>
<tr>
<td>[:xdigit:]</td>
<td>Hexadecimal digits</td>
<td>'0', '3', 'A', 'F'</td>
</tr>
</tbody>
</table>
Tivoli Enterprise Console Events

Tivoli Policy Director for Operating Systems uses the Tivoli Enterprise Console logfile adapter to send information about critical UNIX security system events to security administrators. The adapter formats and forwards events to Tivoli Enterprise Console. Also, a set of rules and associated actions is defined for the supported events. This chapter describes the events and associated information that are sent to Tivoli Enterprise Console by the logfile adapter.

The following Tivoli Policy Director for Operating Systems events are monitored:

- Login (permit/deny/warning)
- Login deny due to:
  - Login disabled
  - Login locked
  - Login suspended
- Login enabled
- Login password change
- Logout
- Credential acquired
- Process start (success/failure)
- Process stop (success/failure)
- Process adopt (success/failure)
- Contact lost
- Contact restored
- Register (success/failure)
- LDAP server (up/down)
- Set group (deny/warning)
- Trusted Computing Base add (success/failure)
- Trusted Computing Base remove (success/failure)
- Policy (valid/not valid)
- Policy set (success/failure)
- Outgoing network connection (warning/deny)
- Incoming network connection (warning/deny)
- Untrusted program execution (success/failure)
- File access (warning/deny)
- Untrusted file accessed
- User `su` (permit/deny/warning)
- User switches groups (success/failure)

For information about how to install and configure the Tivoli Enterprise Console logfile adapter to receive and process Tivoli Policy Director for Operating Systems events, see Chapter 8, “Integrating with Tivoli Enterprise Console” on page 197. For more information about Tivoli Enterprise Console, see the Tivoli Enterprise Console User’s Guide.
<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Event Name</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDOS Process Started Successfully. Process: <em>PDOS_run_srn</em></td>
<td>A Tivoli Policy Director for Operating Systems daemon was successfully started.</td>
<td>PDOS_ProcessStartSuccess</td>
<td>Harmless</td>
</tr>
<tr>
<td>PDOS Process Start Failed. Process: <em>PDOS_run_srn</em></td>
<td>An attempt to start a Tivoli Policy Director for Operating Systems daemon was not successful.</td>
<td>PDOS_ProcessStartFail</td>
<td>Critical</td>
</tr>
<tr>
<td>PDOS Process Stopped Successfully. Process: <em>PDOS_run_srn</em></td>
<td>A Tivoli Policy Director for Operating Systems daemon was successfully stopped.</td>
<td>PDOS_ProcessStopSuccess</td>
<td>Harmless</td>
</tr>
<tr>
<td>PDOS Process Stop Failed. Process: <em>PDOS_run_srn</em></td>
<td>An attempt to stop a Tivoli Policy Director for Operating Systems daemon was not successful.</td>
<td>PDOS_ProcessStopFail</td>
<td>Critical</td>
</tr>
<tr>
<td>PDOS Process Adopted Successfully. Process: <em>PDOS_run_srn</em></td>
<td>A Tivoli Policy Director for Operating Systems daemon was successfully adopted into the set of watched processes.</td>
<td>PDOS_ProcessAdoptSuccess</td>
<td>Harmless</td>
</tr>
<tr>
<td>PDOS Process Adopt Failed. Process: <em>PDOS_run_srn</em></td>
<td>An attempt to adopt a Tivoli Policy Director for Operating Systems daemon into the set of watched processes was not successful.</td>
<td>PDOS_ProcessAdoptFail</td>
<td>Minor</td>
</tr>
<tr>
<td>PDOS Authorization Decision API Failed.</td>
<td>An authorization API encountered an unexpected error.</td>
<td>PDOS_AznApiFailure</td>
<td>Warning</td>
</tr>
<tr>
<td>Kernel lost contact with PDOSD</td>
<td>Communications between the PDOS kernel and the PDOSD daemon have been lost. Authorization cannot be enforced.</td>
<td>PDOS_LostContact</td>
<td>Critical</td>
</tr>
<tr>
<td>Kernel has regained contact with PDOSD.</td>
<td>Communications between the PDOS kernel and the PDOSD daemon have been restored.</td>
<td>PDOS_ContactRestored</td>
<td>Warning</td>
</tr>
<tr>
<td>A kosseal_register call was made to acquire privileged access.</td>
<td>A Tivoli Policy Director for Operating Systems process has gained privileged access.</td>
<td>PDOS_RegisterSuccess</td>
<td>Harmless</td>
</tr>
<tr>
<td>Message</td>
<td>Description</td>
<td>Event Name</td>
<td>Severity</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------------------</td>
<td>----------</td>
</tr>
<tr>
<td>A kosseal_register call failed to acquire privileged access.</td>
<td>A Tivoli Policy Director for Operating Systems process was unable to gain privileged access.</td>
<td>PDOS_RegisterFail</td>
<td>Critical</td>
</tr>
<tr>
<td>Policy Director user registry is available.</td>
<td>The Tivoli Policy Director user register is now available. Policy updates can be downloaded.</td>
<td>PDOS_LdapServerUp</td>
<td>Harmless</td>
</tr>
<tr>
<td>Policy Director user register is unavailable (isolation mode).</td>
<td>The Tivoli Policy Director user registry is not available. Policy cannot be updated at this time.</td>
<td>PDOS_LdapServerDown</td>
<td>Minor</td>
</tr>
</tbody>
</table>
### Table 54. File Related Tivoli Enterprise Console Events

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Event Name</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed File Access. File <code>PDOS_acc_name</code></td>
<td>Access to a file was denied.</td>
<td><code>PDOS_FileAccessDeny</code></td>
<td>Warning</td>
</tr>
<tr>
<td>Program: <code>PDOS_run_srn</code></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Action: <code>PDOS_permission</code></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Warning File Access. File <code>PDOS_acc_name</code></td>
<td>Access to a file was allowed only because policy is set to warn instead of deny.</td>
<td><code>PDOS_FileAccessWarning</code></td>
<td>Warning</td>
</tr>
<tr>
<td>Program: <code>PDOS_run_srn</code></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Action: <code>PDOS_permission</code></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message</td>
<td>Description</td>
<td>Event Name</td>
<td>Severity</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------------</td>
<td>----------</td>
</tr>
<tr>
<td>Failed Incoming Network Connection. From Host: PDOS_ipaddress Services: PDOS_port</td>
<td>Access to an incoming network connection was denied.</td>
<td>PDOS_IncomingNetConnDeny</td>
<td>Warning</td>
</tr>
<tr>
<td>Warning Incoming Network Connection. From Host: PDOS_ipaddress Services: PDOS_port</td>
<td>Access to an incoming network connection was allowed only because policy is set to warn instead of deny.</td>
<td>PDOS_IncomingNetConnWarning</td>
<td>Warning</td>
</tr>
<tr>
<td>Failed Outgoing Network Connection. To Host: PDOS_ipaddress User: PDOS_acc_name Program: PDOS_run_sr</td>
<td>Access to an outgoing network connection was denied.</td>
<td>PDOS_OutgoingNetConnDeny</td>
<td>Warning</td>
</tr>
<tr>
<td>Warning Outgoing Network Connection. To Host: PDOS_ipaddress User: PDOS_acc_name Program: PDOS_run_sr</td>
<td>Access to an outgoing network connection was allowed only because policy is set to warn instead of deny.</td>
<td>PDOS_OutgoingNetConnWarning</td>
<td>Warning</td>
</tr>
<tr>
<td>Message</td>
<td>Description</td>
<td>Event Name</td>
<td>Severity</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------------</td>
<td>----------</td>
</tr>
<tr>
<td>Successful Sudo operation. User: $PDOS_acc_name$ Program: $PDOS_exe$</td>
<td>Sudo operation was successful.</td>
<td>PDOS_SudoPermit</td>
<td>Harmless</td>
</tr>
<tr>
<td>Failed Sudo operation. User: $PDOS_acc_name$ Program: $PDOS_exe$</td>
<td>Sudo operation was unsuccessful.</td>
<td>PDOS_SudoDeny</td>
<td>Warning</td>
</tr>
<tr>
<td>Warning Sudo operation. User: $PDOS_acc_name$ Program: $PDOS_exe$</td>
<td>Sudo operation was allowed only because policy is set to warn instead of deny</td>
<td>PDOS_SudoWarning</td>
<td>Warning</td>
</tr>
<tr>
<td>Message</td>
<td>Description</td>
<td>Event Name</td>
<td>Severity</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Failed Substitution to User. To User: PDOS_asname From User: PDOS_acc_name Program: PDOS_exe</td>
<td>Substitute user failed.</td>
<td>PDOS_SetUserDeny</td>
<td>Harmless</td>
</tr>
<tr>
<td>Warning Substitution to User. To User: PDOS_asname From User: PDOS_acc_name Program: PDOS_exe</td>
<td>Substitute user was allowed only because policy is set to warn instead of deny</td>
<td>PDOS_SetUserWarning</td>
<td>Warning</td>
</tr>
</tbody>
</table>
**Table 58. Set(Group) Related Tivoli Enterprise Console Events**

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Event Name</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed Substitution to Group. To Group: PDOS_asname From User: PDOS_acc_name Program: PDOS_exe</td>
<td>Substitute group failed.</td>
<td>PDOS_SetGroupDeny</td>
<td>Harmless</td>
</tr>
<tr>
<td>Warning Substitution to Group. To Group: PDOS_asname From User: PDOS_acc_name Program: PDOS_exe</td>
<td>Substitute group was allowed only because policy is set to warn instead of deny</td>
<td>PDOS_SetGroupWarning</td>
<td>Warning</td>
</tr>
</tbody>
</table>

**Table 59. TCB Related Tivoli Enterprise Console Events**

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Event Name</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access allowed to untrusted file. File: PDOS_asrn User: PDOS_acc_name Program: PDOS_exe</td>
<td>Access to an untrusted file was allowed.</td>
<td>PDOS_AccessUntrust</td>
<td>Minor</td>
</tr>
<tr>
<td>Access allowed to a TCB file in an unknown state. File: PDOS_asrn User: PDOS_acc_name Program: PDOS_exe</td>
<td>Access to a Trusted Computing Base (TCB) file in an unknown trust state was allowed.</td>
<td>PDOS_AccessUnknownTrustState</td>
<td>Warning</td>
</tr>
<tr>
<td>A file has been marked trusted. File: PDOS_asrn User: PDOS_acc_name Program: PDOS_exe</td>
<td>A file has been successfully marked as trusted.</td>
<td>PDOS_TrustSuccess</td>
<td>Harmless</td>
</tr>
<tr>
<td>PDOS failed to mark a file trusted. File: PDOS_asrn User: PDOS_acc_name Program: PDOS_exe Fail_Status: PDOS_fail_status</td>
<td>Tivoli Policy Director for Operating Systems was unable to mark a file trusted.</td>
<td>PDOS_TrustFail</td>
<td>Warning</td>
</tr>
<tr>
<td>A file has been marked untrusted. File: PDOS_asrn User: PDOS_acc_name Program: PDOS_exe</td>
<td>Tivoli Policy Director for Operating Systems was marked a file as untrusted.</td>
<td>PDOS_UntrustSuccess</td>
<td>Warning</td>
</tr>
<tr>
<td>PDOS failed to mark a file untrusted. File: PDOS_asrn User: PDOS_acc_name Program: PDOS_exe Fail_Status: PDOS_fail_status</td>
<td>Tivoli Policy Director for Operating Systems was unable to mark a file untrusted.</td>
<td>PDOS_UntrustFail</td>
<td>Warning</td>
</tr>
<tr>
<td>Message</td>
<td>Description</td>
<td>Event Name</td>
<td>Severity</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>------------</td>
<td>----------</td>
</tr>
<tr>
<td>New file added to TCB database. File: <code>PDOS_srn</code> User: <code>PDOS_acc_name</code></td>
<td>A file has been successfully added to the Trusted Computing Base (TCB) database.</td>
<td>PDOS_TcbAddSuccess</td>
<td>Harmless</td>
</tr>
<tr>
<td>PDOS failed to add new file to TCB database. File: <code>PDOS_srn</code> User: <code>PDOS_acc_name</code> Fail_Status: <code>PDOS_fail_status</code></td>
<td>Tivoli Policy Director for Operating Systems was unable to add a file to the Trusted Computing Base (TCB) database.</td>
<td>PDOS_TcbAddFail</td>
<td>Warning</td>
</tr>
<tr>
<td>File removed from TCB database. File: <code>PDOS_srn</code> User: <code>PDOS_acc_name</code></td>
<td>A file has been successfully removed from the Trusted Computing Base (TCB) database.</td>
<td>PDOS_TcbRemoveSuccess</td>
<td>Warning</td>
</tr>
<tr>
<td>PDOS failed to remove a file from TCB database. File: <code>PDOS_srn</code> User: <code>PDOS_acc_name</code> Fail_Status: <code>PDOS_fail_status</code></td>
<td>Tivoli Policy Director for Operating Systems was unable to remove a file from the Trusted Computing Base (TCB) database.</td>
<td>PDOS_TcbRemoveFail</td>
<td>Warning</td>
</tr>
</tbody>
</table>
### Table 60. Policy Related Tivoli Enterprise Console Events

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Event Name</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy applied for a protected object name. Name: <strong>PDOS_pon</strong></td>
<td></td>
<td>PDOS_PolicyValid</td>
<td>Harmless</td>
</tr>
<tr>
<td>Policy not applied for an invalid protected object name. Name: <strong>PDOS_pon</strong></td>
<td></td>
<td>PDOS_PolicyInvalid</td>
<td>Warning</td>
</tr>
<tr>
<td>Policy kernel version set in Kernel Policy Cache.</td>
<td></td>
<td>PDOS_PolicySetSuccess</td>
<td>Warning</td>
</tr>
<tr>
<td>Failed to set policy.</td>
<td></td>
<td>PDOS_PolicySetFail</td>
<td>Warning</td>
</tr>
</tbody>
</table>

### Table 61. Login Related Tivoli Enterprise Console Events

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Event Name</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login successful. User: <strong>PDOS_acc_name</strong> From Host: <strong>PDOS_login_location</strong> Program: <strong>PDOS_exe</strong></td>
<td>User login permitted.</td>
<td>PDOS_LoginPermit</td>
<td>Harmless</td>
</tr>
<tr>
<td>Login Failed. User: <strong>PDOS_acc_name</strong> From Host: <strong>PDOS_login_location</strong> Program: <strong>PDOS_exe</strong></td>
<td>User login was denied.</td>
<td>PDOS_LoginDeny</td>
<td>Warning</td>
</tr>
<tr>
<td>Login Warning. User: <strong>PDOS_acc_name</strong> From Host: <strong>PDOS_login_location</strong> Program: <strong>PDOS_exe</strong></td>
<td>User login was allowed only because policy is set to warn instead of deny</td>
<td>PDOS_LoginWarning</td>
<td>Warning</td>
</tr>
<tr>
<td>User Account <strong>PDOS_acc_name</strong> enabled for login.</td>
<td>The specified user account was enabled for login.</td>
<td>PDOS_LoginEnabled</td>
<td>Warning</td>
</tr>
<tr>
<td>User Account <strong>PDOS_acc_name</strong> disabled for login.</td>
<td>The specified user account has been disabled for login.</td>
<td>PDOS_LoginDisabled</td>
<td>Warning</td>
</tr>
<tr>
<td>User Account <strong>PDOS_acc_name</strong> locked for login.</td>
<td>The specified user account has been locked for login.</td>
<td>PDOS_LoginLocked</td>
<td>Warning</td>
</tr>
<tr>
<td>User Account <strong>PDOS_acc_name</strong> suspended for login.</td>
<td>The specified user account has been suspended for login.</td>
<td>PDOS_LoginSuspended</td>
<td>Warning</td>
</tr>
<tr>
<td>Password change time was modified by administrator. User: <strong>PDOS_acc_name</strong></td>
<td>The password change time associated with this user account has been changed by the administrator.</td>
<td>PDOS_LoginAdm</td>
<td>Warning</td>
</tr>
<tr>
<td>Password successfully changed. User: <strong>PDOS_acc_name</strong></td>
<td>The password associated with this user account has been changed.</td>
<td>PDOS_LoginPwdChange</td>
<td>Warning</td>
</tr>
</tbody>
</table>
Table 61. Login Related Tivoli Enterprise Console Events (continued)

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Event Name</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logout occurred. User: PDOS_acc_name</td>
<td>The specified user has logged off.</td>
<td>PDOS_Logout</td>
<td>Harmless</td>
</tr>
</tbody>
</table>

Table 62. Credential Related Tivoli Enterprise Console Events

<table>
<thead>
<tr>
<th>Message</th>
<th>Description</th>
<th>Event Name</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obtained credential. User: PDOS_acc_name</td>
<td>Credential successfully obtained.</td>
<td>PDOS_GetCredSuccess</td>
<td>Harmless</td>
</tr>
<tr>
<td>Failed to obtain credential. User: PDOS_acc_name</td>
<td>Tivoli Policy Director for Operating Systems was unable to obtain credential.</td>
<td>PDOS_GetCredFail</td>
<td>Warning</td>
</tr>
</tbody>
</table>
This appendix describes the messages provided by Tivoli Policy Director for Operating Systems.

0x340b4001 failed to allocate kernel memory!
Explanation: The operating system failed to allocate memory in the kernel.
Action: Check the amount of system page space available as well as the amount of available memory. You also might consider rebooting the system. If the problem persists, contact IBM Customer Support.

0x340b4002 unexpected error
Explanation: An unexpected error occurred during PDOS kernel processing.
Action: Use the error code in the message to determine the cause of the error and correct it. If the problem persists, contact IBM Customer Support.

0x340b4003 internal error
Explanation: An unexpected error occurred in the PDOS kernel logic.
Action: If the problem persists, contact IBM Customer Support. Diagnostic data for use by IBM Customer Support can be obtained by running the following script and redirecting its output to a file: /opt/pdos/kernel/kossdump.sh.

0x340b4004 lost contact with pdosd, err
Explanation: The PDOS kernel has lost communication with the pdosd process.
Action: Verify that the pdosd process is running. Restart the process if necessary. If the problem persists, contact IBM Customer Support. Diagnostic data for use by IBM Customer Support can be obtained by running the following script and redirecting its output to a file: /opt/pdos/kernel/kossdump.sh.

0x340b4005 still can not contact pdosd, err
Explanation: The PDOS kernel is unable to regain communication with the pdosd process.

0x340b4006 regained contact with pdosd
Explanation: Communication between the PDOS kernel and the pdosd process has been restored.
Action: No immediate action is required. If this message occurs frequently, contact IBM Customer Support. Diagnostic data for use by IBM Customer Support can be obtained by running the following script and redirecting its output to a file: /opt/pdos/kernel/kossdump.sh.

0x340b4007 cannot contact pdosauditd, err
Explanation: The PDOS kernel failed to communicate with the pdosauditd process.
Action: Verify that the pdosauditd process is running. Restart the process if necessary. If the problem persists, contact IBM Customer Support. Diagnostic data for use by IBM Customer Support can be obtained by running the following script and redirecting its output to a file: /opt/pdos/kernel/kossdump.sh.

0x340b4008 cannot enforce protected file object:
Explanation: PDOS cannot enforce security on the indicated file system resource.
Action: Contact IBM Customer Support. Diagnostic data for use by IBM Customer Support can be obtained by running the following script and redirecting its output to a file: /opt/pdos/kernel/kossdump.sh.

0x340b4009 cannot enforce accessed file object:
Explanation: PDOS was unable to enforce security on an accessed file system resource.
Action: Contact IBM Customer Support. Diagnostic data for use by IBM Customer Support can be obtained by running the following script and redirecting its output to a file:
/opt/pdos/kernel/kossdump.sh.

0x35787080  Failed to process audit message: %d: %s
Explanation: An internal service failed to process an audit record message.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35787081  Failed to extract audit common event data message: %d: %s
Explanation: An internal message processing routine failed to read all the data for an audit record from a message channel. An audit record was not processed successfully.
Action: Use the returned error status to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35787082  Failed to extract audit common data message: %d: %s
Explanation: An internal message processing routine failed to read all the data for an audit record from a message channel. An audit record was not processed successfully.
Action: Use the returned error status to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35787084  Failed to extract Running Program Protected Object Name: %d: %s
Explanation: An internal message processing routine failed to read all the data for an audit record from a message channel. An audit record was not processed successfully.
Action: Use the returned error status to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35787086  Failed to extract Protected Object Name: %d: %s
Explanation: An internal message processing routine failed to read all the data for an audit record from a message channel. An audit record was not processed successfully.
Action: Use the returned error status to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35787087  Failed to extract System Resource Name: %d: %s
Explanation: An internal message processing routine failed to read all the data for an audit record from a message channel. An audit record was not processed successfully.
Action: Use the returned error status to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35787088  Failed to extract audit parameters: %d: %s
Explanation: An internal message processing routine failed to read all the data for an audit record from a message channel. An audit record was not processed successfully.
Action: Use the returned error status to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x3578708a  Failed to extract network data extension: %d: %s
Explanation: An internal message processing routine failed to read all the data for an audit record from a message channel. An audit record was not processed successfully.
Action: Use the returned error status to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x3578708b  Failed to extract TCB data extension: %d: %s
Explanation: An internal message processing routine failed to read all the data for an audit record from a message channel. An audit record was not processed successfully.
Action: Use the returned error status to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.
0x3578708c Failed to extract policy data extension: %d: %s
Explanation: An internal message processing routine failed to read all the data for an audit record from a message channel. An audit record was not processed successfully.
Action: Use the returned error status to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x3578708d Failed to extract sudo data extension: %d: %s
Explanation: An internal message processing routine failed to read all the data for an audit record from a message channel. An audit record was not processed successfully.
Action: Use the returned error status to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35787184 Failed to extract Branch Name: %d: %s
Explanation: An internal message processing routine failed to read all the data for an audit record from a message channel. An audit record was not processed successfully.
Action: Use the returned error status to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35787185 Failed to extract local terminal: %d: %s
Explanation: An internal message processing routine failed to read all the data for an audit record from a message channel. An audit record was not processed successfully.
Action: Use the returned error status to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35787186 Failed to extract Surrogate Name: %d: %s
Explanation: An internal message processing routine failed to read all the data for an audit record from a message channel. An audit record was not processed successfully.
Action: Use the returned error status to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35787187 Failed to extract Surrogate Name Length: %d: %s
Explanation: An internal message processing routine failed to read all the data for an audit record from a message channel. An audit record was not processed successfully.
Action: Use the returned error status to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35787188 Failed to extract Surrogate ID: %d: %s
Explanation: An internal message processing routine failed to read all the data for an audit record from a message channel. An audit record was not processed successfully.
Action: Use the returned error status to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35787189 Failed to extract remote terminal: %d: %s
Explanation: An internal message processing routine failed to read all the data for an audit record from a message channel. An audit record was not processed successfully.
Action: Use the returned error status to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x3578718a Failed to extract Accessor Name: %d: %s
Explanation: An internal message processing routine failed to read all the data for an audit record from a message channel. An audit record was not processed successfully.
Action: Use the returned error status to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x3578718b Failed to extract Accessor Effective Name: %d: %s
Explanation: An internal message processing routine failed to read all the data for an audit record from a message channel. An audit record was not processed successfully.
Action: Use the returned error status to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35794005 PDOSAUDITD tried to generate an unexpected audit event.
Explanation: An internal service attempted to audit an event that is not recognized by the PDOSAUDITD auditing service.
Action: If the problem persists, contact IBM Customer Support.

0x35794006 Usage: pdosauditd [-fhlvV?] [-t trace-string]
-f run daemon on in foreground -v display verbose messages -V display version information and terminate -[h?] display this usage message -t specify initial trace level
Explanation: pdosauditd usage statement.
Action: None
**0x357940cb** Unable to read configuration file %s: %d: %s

**Explanation:** The PDOSAUDITD daemon received an error when it attempted to read the specified configuration file.

**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

**0x357940cc** Configuration value of [%s:%s]: %s

**Explanation:** The PDOSAUDITD daemon displays current configuration values when started with the verbose flag.

**Action:** None

**0x357940cd** Configuration value of [%s:%s]: %d

**Explanation:** The PDOSAUDITD daemon displays current configuration values when started with the verbose flag.

**Action:** None

**0x357940cf** Unable to initialize Message Handler service: %d: %s

**Explanation:** An error occurred when the PDOSAUDITD daemon attempted to initialize the message handling service.

**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

**0x357940d0** Unable to shutdown Message Handler service: %d: %s

**Explanation:** An error occurred when the PDOSAUDITD daemon attempted to shut down the message handling service.

**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

**0x357940d1** Message Handler service initialized

**Explanation:** The PDOSAUDITD daemon has initialized the message handler service.

**Action:** None

**0x357940d2** Message Handler service shutdown

**Explanation:** The PDOSAUDITD daemon has shut down the message handler service.

**Action:** None

**0x357940d4** PDOSAUDITD terminating cleanly

**Explanation:** The PDOSAUDITD daemon is terminating normally.

**Action:** None

**0x357940d5** PDOSAUDITD successfully shutdown

**Explanation:** The PDOSAUDITD daemon has shut down successfully.

**Action:** None

**0x357940d6** Redirecting output to: %s

**Explanation:** The PDOSAUDITD daemon is redirecting output to the location specified.

**Action:** None

**0x357940da** Could not perform daemon cleanup: %x: %s

**Explanation:** During PDOSAUDITD daemon shut down, an error occurred while cleaning up resources.

**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

**0x357940db** Could not get the hostname of the machine PDOSAUDITD is running on

**Explanation:** During initialization, the PDOSAUDITD daemon encountered an error when attempting to determine the host name of the current machine.

**Action:** If the problem persists, contact IBM Customer Support.

**0x357940dd** Error auditing unknown event ID 0x%x.

**Explanation:** An internal service attempted to audit an event that is not recognized by the PDOSAUDITD auditing service.

**Action:** Restart the PDOSAUDITD daemon and report the error to IBM Customer Support.

**0x357940de** Error allocating audit record for event %s (0x%x). The error status is 0x%x: %s

**Explanation:** An error occurred when the PDOSAUDITD daemon attempted to allocate storage for a data structure to store an audit record.

**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.
0x357940df Error auditing event %s (0x%x). The error status is 0x%x: %s.
Explanation: An error occurred when the PDOSAUDITD daemon attempted to generate an audit record.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35794fa1 PDOSAUDITD could not set the kernel audit level. status: %d
Explanation: The PDOSAUDITD daemon encountered an error attempting to set the current audit level in the PDOS Kernel service.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35794fa2 PDOSAUDITD set the kernel audit level to: %d
Explanation: Indicates that the audit level in the PDOS Kernel service has been set to the specified value.
Action: None

0x35794fa4 Could not get the IP address of the machine PDOSAUDITD is running on
Explanation: During initialization, the PDOSAUDITD daemon encountered an error trying to determine the IP address of the current machine.
Action: If the problem persists, contact IBM Customer Support.

0x357b1001 The Object Signature Database is already initialized
Explanation: Internal error indicating that the Object Signature Database is already initialized.
Action: None.

0x357b1002 The Object Signature Database is not yet initialized
Explanation: An attempt was made to access the Object Signature Database before it was initialized.
Action: Restart the PDOS daemons. If the error persists, contact IBM Customer Support.

0x357b1003 Failed to open the Object Signature Database.
Explanation: An unexpected error occurred when attempting to open the Object Signature Database.
Action: Contact IBM Customer Support.

0x357b1004 Failed to create the Object Signature Database.
Explanation: An unexpected error occurred when creating the Object Signature Database.
Action: None.

0x357b1005 Failed to close the Object Signature Database.
Explanation: An unexpected error occurred when closing the Object Signature Database.
Action: Restart the PDOS daemons.

0x357b1006 The specified object is already in the untrusted state.
Explanation: An attempt was made to change an object to the untrusted state that was already untrusted.
Action: None.

0x357b1007 Attempt to lock file failed
Explanation: Internal status code
Action: None.

0x357b1008 Attempt to unlock file failed
Explanation: Internal status code
Action: None.

0x357b1009 Could not read header file
Explanation: Internal status code
Action: None.

0x357b100a Could not write header file
Explanation: Internal status code
Action: None.
**0x357b100b**  Header is truncated

**Explanation:** Internal status code

**Action:** None.

---

**0x357b100c**  File seek failed

**Explanation:** Internal status code

**Action:** None.

---

**0x357b1080**  Unable to store the version number in the database : %s : %d

**Explanation:** Failed to store the version number in the Object Signature Database headers.

**Action:** Check previous errors in the error log to determine the cause of the error. Correct the problem and restart the PDOS daemons. If the error persists, contact IBM Customer Support.

---

**0x357b1081**  Unable to get the version number from the database : %s : %d

**Explanation:** Unable to fetch the version number from the Object Signature Database header.

**Action:** Check previous errors in the error log to determine the cause of the error. Correct the problem and restart the PDOS daemons. If the problem persists, contact IBM Customer Support.

---

**0x357b1082**  Unable to store the time stamp in the database : %s : %d

**Explanation:** Unable to store the last update time in the Object Signature Database header.

**Action:** Check previous errors in the error log to determine the cause of the error. Correct the problem and restart the PDOS daemons. If the problem persists, contact IBM Customer Support.

---

**0x357b1083**  Unable to get the time stamp from the database : %s : %d

**Explanation:** Unable to get the time stamp from the Object Signature Database headers.

**Action:** Check previous errors in the error log to determine the cause of the error. Correct the problem and restart the PDOS daemons. If the problem persists, contact IBM Customer Support.

---

**0x357b1084**  An error occurred while getting the information about the file: File : %s : %s : %d

**Explanation:** An unexpected error occurred when obtaining information about the specified file.

**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

---

**0x357b1085**  An error occurred while opening the file.

**Filename : message : error:** %s : %s : %d

**Explanation:** An unexpected error occurred when attempting to open the specified file.

**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

---

**0x357b1086**  An error occurred while reading the file:

**Name : %s : %s : %d**

**Explanation:** An unexpected error occurred when reading the specified file.

**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

---

**0x357b1087**  Could not read header file: %d: %s

**Explanation:** An error occurred attempting to read the Object Signature Database header file.

**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

---

**0x357b1088**  Could not write header file: %d: %s

**Explanation:** An unexpected error occurred when writing the specified file.

**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

---

**0x357b1089**  Could not open the header file: %d: %s

**Explanation:** An unexpected error occurred when opening the Object Database header file.

**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.
0x357b108a  Attempt to lock file with flags %x failed: %d: %s
Explanation: An unexpected error occurred attempting to lock the specified file.
Action: Verify that the specified file has the proper file permissions set. Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x357b108b  Attempt to unlock file failed: %d: %s
Explanation: An unexpected error occurred attempting to unlock the specified file. The error code displayed is the value returned by the system.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x357b108c  File seek in %s to %llu failed: %d: %s
Explanation: An unexpected error occurred during file seek in the specified file.
Action: Use the returned error code to diagnose during file seek in the specified file. Also check the availability of general system resources, such as disk space, paging space, memory usage.

0x357b108d  Maximum checksum size %llu not in the range %llu to %llu - using %llu.
Explanation: The max-checksum-file-size parameter specified in the PDOS configuration file is not within the specified range.
Action: Correct the value of the max-checksum-file-size parameter so that it falls within the proper range. The proper range is displayed as part of the message.

0x357b1100  Failed to initialize Object Signature Database hashing subsystem.
Explanation: Internal status code.
Action: None.

0x357b1101  There are no entries in the database matching the file.
Explanation: Internal status code
Action: None.

0x357b1104  Invalid record version
Explanation: Internal status code.
Action: None.

0x357b1105  Record read failed
Explanation: Internal status code.
Action: None.

0x357b1106  Record write failed
Explanation: Internal status code.
Action: None.

0x357b1107  Record truncated
Explanation: Internal status code.
Action: None.

0x357b1108  seek failed
Explanation: An unexpected error occurred reading the hash file.
Action: See additional messages in the error log to determine the cause of the error. Correct the problem and restart the PDOS daemons. If the problem persists, contact IBM Customer Support.

0x357b1109  readdir failed
Explanation: An unexpected error occurred when reading the directory.
Action: See additional messages in the error log to determine the cause of the error. Correct the problem and restart the PDOS daemons. If the problem persists, contact IBM Customer Support.

0x357b110a  stat failed
Explanation: An unexpected error occurred running the stat command on the file.
Action: See additional messages in the error log to determine the cause of the error. Correct the problem and restart the PDOS daemons. If the problem persists, contact IBM Customer Support.
<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
</table>
| 0x357b110b mkdir failed | **Explanation:** An unexpected error occurred attempting to create a directory.  
**Action:** Check the permissions on the directory to be created. See additional messages in the error log to determine the cause of the error. Correct the problem and restart the PDOS daemons. If the problem persists, contact IBM Customer Support. |
| 0x357b110c Could not create record file | **Explanation:** An unexpected error occurred when creating an entry in the Object Signature Database for the protected resource.  
**Action:** See additional messages in the error log to determine the cause of the error. Correct the problem and restart the PDOS daemons. If the problem persists, contact IBM Customer Support. |
| 0x357b110d Could not rename record file | **Explanation:** An unexpected error occurred when attempting to rename the record file.  
**Action:** See additional messages in the error log to determine the cause of the error. Correct the problem and restart the PDOS daemons. If the problem persists, contact IBM Customer Support. |
| 0x357b110e Could not delete record file | **Explanation:** An unexpected error occurred when trying to delete an entry from the Object Signature Database.  
**Action:** See additional messages in the error log to determine the cause of the error. Correct the problem and restart the PDOS daemons. If the problem persists, contact IBM Customer Support. |
| 0x357b1180 Could not open hash directory %s; %d: %s | **Explanation:** An error occurred attempting to open the Trusted Computing Base (TCB) hash directory.  
**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support. |
| 0x357b1181 Could not close hash directory %s; %d: %s | **Explanation:** An error occurred attempting to close the Trusted Computing Base (TCB) hash directory.  
**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support. |
| 0x357b1182 Could not read object signature record name length: %d: %s | **Explanation:** An unexpected error occurred when attempting to read the object signature record name length.  
**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support. |
| 0x357b1183 Could not write object signature record name length: %d: %s | **Explanation:** An unexpected error occurred when writing the object signature record name length.  
**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support. |
| 0x357b1184 Could not read object signature record name: %d: %s | **Explanation:** An unexpected error occurred when attempting to read the object signature record name.  
**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support. |
| 0x357b1185 Could not write object signature record name: %d: %s | **Explanation:** An unexpected error occurred when writing the object signature record name.  
**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support. |
| 0x357b1186 Could not read object signature record signature: %d: %s | **Explanation:** An unexpected error occurred when attempting to read the object signature record signature.  
**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support. |
| 0x357b1187 Could not write object signature record signature: %d: %s | **Explanation:** An unexpected error occurred when writing the object signature record signature.  
**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support. |
D. Messages

0x357b1188  Could not read object signature record
version: %d: %s

Explanation:  An unexpected error occurred when attempting
to read the version of the object signature record.

Action:  Use the returned error code and error text to diagnose
and correct the problem. If the problem persists, contact IBM
Customer Support.

0x357b1189  Could not write object signature record
version: %d: %s

Explanation:  An unexpected error occurred when writing the
object signature version.

Action:  Use the returned error code and error text to diagnose
and correct the problem. If the problem persists, contact IBM
Customer Support.

0x357b118a  Invalid record version: %d

Explanation:  The record version is not valid. This condition
could indicate a corrupt Object Signature Database.

Action:  Shut down the PDOS daemons. Delete all the entries
in the Object Signature Database, which is located in the
/var/pdos/tcb directory. Restart the PDOS daemons. If the
problem persists, contact IBM Customer Support.

0x357b118b  seek failed: %d: %s

Explanation:  Seek in signature file in the Object Signature
Database failed.

Action:  Use the returned error code and error text to diagnose
and correct the problem. If the problem persists, contact IBM
Customer Support.

0x357b118c  Could not open TCB signature file %s: %d: %s

Explanation:  An unexpected error occurred when attempting
to open a file in the Object Signature Database.

Action:  Use the returned error code and error text to diagnose
and correct the problem. If the problem persists, contact IBM
Customer Support.

0x357b118d  Match failed searching TCB signature file
%s/%s: 0x%x: %s

Explanation:  Match failed searching TCB signature file.

Action:  Use the returned error code and error text to diagnose
and correct the problem. If the problem persists, contact IBM
Customer Support.

0x357b118e  Unable to read hash directory: %d: %s

Explanation:  An unexpected error occurred when attempting
to read hash directory in the Object Signature Database.

Action:  Use the returned error code and error text to diagnose
and correct the problem. If the problem persists, contact IBM
Customer Support.

0x357b118f  Unable to stat directory entry %s: %d: %s

Explanation:  Stat failed on file name in the Object Signature
Database.

Action:  Use the returned error code and error text to diagnose
and correct the problem. If the problem persists, contact IBM
Customer Support.

0x357b1190  Unable to create directory %s: %d: %s

Explanation:  Could not create a directory to store hashed
Object Signature Database entries.

Action:  Use the returned error code and error text to diagnose
and correct the problem. If the problem persists, contact IBM
Customer Support.

0x357b1191  Unable to determine maximum entry size in
root hash directory %s: %d: %s

Explanation:  Unable to determine the maximum entry size in
the root hash directory.

Action:  See the errno returned and the associated error text to
determine cause of the error. Correct the problem. If the
problem persists, contact IBM Customer Support.

0x357b1192  Unable to create record file %s: %d: %s

Explanation:  Unable to create a hash file for the Trusted
Computing Base (TCB) entry in the Object Signature Database.

Action:  Use the returned error code and error text to diagnose
and correct the problem. If the problem persists, contact IBM
Customer Support.

0x357b1193  Unable to rename temporary record file %s
to %s: %d: %s

Explanation:  Unable to rename a temporary file used by the
Object Signature Database.

Action:  Use the returned error code and error text to diagnose
and correct the problem. If the problem persists, contact IBM
Customer Support.
Unable to delete record file %s: %d: %s
Explanation: Unable to delete the hashed file in the Object Signature Database.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

There are no objects whose state needs to be updated. Either there are no objects in the database or all the objects are already in the specified state.
Explanation: Informational Message.
Action: None.

The state of the specified object is changed successfully.
Explanation: Internal status code.
Action: None.

Unallocated Inode.
Explanation: Internal status code indicating an unallocated inode.
Action: None.

Directory
Explanation: Internal status code indicating the type of device
Action: None.

Block Device
Explanation: Internal status code indicating the type of device
Action: None.

Character Device
Explanation: Internal status code indicating the type of device
Action: None.

File
Explanation: Internal status code indicating the type of device
Action: None.

Set UID
Explanation: Informational Message.
Action: None.

Set GID
Explanation: Informational status code.
Action: None.

Sticky
Explanation: Informational status code.
Action: None.

State : Trusted
Explanation: Indicates the state of the trusted object.
Action: None.

State : Untrusted
Explanation: Indicates the state of the trusted object.
Action: None.

State : Invalid
Explanation: Informational status code.
Action: None.

State : Trusted (should not exist and does not exist)
Explanation: Indicates that a trusted object has been deleted but the policy for the object still exists.
Action: Check to see if the object was deleted in error. If not evaluate if the policy protecting the non-existent resource is valid.

State : Untrusted (should not exist but does exist)
Explanation: Informational status code.
Action: None.

Reason : The object is a new object.
Explanation: Informational message.
Action: None.
0x357b1210 Reason: The Administrator changed the state explicitly.
Explanation: Informational message.
Action: None.

0x357b1211 Reason: The access state changed.
Explanation: Informational message.
Action: None.

0x357b1212 Reason: The signature check failed.
Explanation: Informational message.
Action: Verify that the signature of the trusted object changed for a valid reason.

0x357b1213 Reason: The reason is invalid.
Explanation: Informational Message.
Action: None.

0x357b1214 Attribute caused the signature failure: CRC checksum
Explanation: Informational Message.
Action: None.

0x357b1215 Attribute caused the signature failure: Owner
Explanation: Informational Message.
Action: None.

0x357b1216 Attribute caused the signature failure: Group
Explanation: Informational Message.
Action: None.

0x357b1217 Attribute caused the signature failure: Size
Explanation: Informational Message.
Action: None.

0x357b1218 Attribute caused the signature failure: Last Inode update time
Explanation: Informational Message.
Action: None.

0x357b1219 Attribute caused the signature failure: Last modification time
Explanation: Informational Message.
Action: None.

0x357b121a Attribute caused the signature failure: Permissions
Explanation: Informational Message.
Action: None.

0x357b121b Attribute caused the signature failure: Inode number
Explanation: Informational Message.
Action: None.

0x357b121c Attribute caused the signature failure: Device number
Explanation: Informational Message.
Action: None.

0x357b121d Attribute caused the signature failure: Invalid
Explanation: Informational Message.
Action: None.

0x357b121e One or more required options are missing.
Explanation: One or more required options are missing from the command.
Action: Verify the command syntax. Correct the problem and retry the operation.

0x357b121f The specified object cannot be set to untrusted state.
Explanation: Informational Message.
Action: None.

0x357b1280 Object Name: %s
Explanation: Informational Message.
Action: None.
0x357b1281 CRC sum : %u
Explanation: Informational Message.
Action: None.

0x357b1282 Inode %lld on device %d/%d
Explanation: Informational Message.
Action: None.

0x357b1283 Owner : %u : %s
Explanation: Informational Message.
Action: None.

0x357b1284 User : %u : Unknown
Explanation: Unknown user. Check file permissions to make sure the file is owned by a valid user.
Action: Check file permissions to determine if the trusted file is owned by a valid user.

0x357b1285 Group : %u : %s
Explanation: Informational Message.
Action: None.

0x357b1286 Group : %u : Unknown
Explanation: Unknown Group.
Action: Check group ownership of the trusted file.

0x357b1287 Size : %lld
Explanation: Informational Message.
Action: None.

0x357b1288 Last status update time : %s
Explanation: Informational Message.
Action: None.

0x357b1289 Last modification time : %s
Explanation: Informational Message.
Action: None.

0x357b128a Permissions : %s
Explanation: Informational Message.
Action: None.

0x357b128b Major Device Number : %d Minor Device Number : %d
Explanation: Informational Message.
Action: None.

0x357b128c Type %o file
Explanation: Informational Message.
Action: None.

0x357b128d Last state transition time: %s
Explanation: Informational Message.
Action: None.

0x357b128e Unable to initialize the Object Signature Database : %s : %d
Explanation: Unable to initialize the Object Signature Database.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x357b128f Unable to get the state of the object : %s : %d
Explanation: Unable to get the state of the object in the Object Signature Database.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x357b1290 Unable to check the state of the object : %s : %d
Explanation: Unable to check the state of the object in the Object Signature Database.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.
0x357b1291 Unable to set the state of the object: %s: %d
Explanation: Unable to set the trust state of the object. See accompanying error message for cause and action.
Action: See message text for cause and action.

0x357b1292 There is a signature change detected for the object, %s, which caused state to change to untrusted.
Explanation: Informational Message.
Action: None.

0x357b1293 Error occurred while updating the state of all objects: %s: %d
Explanation: Unable to update the state of all objects.
Action: See other error messages in the error logs to determine which objects state could not be updated. Correct the problem and retry the operation. If the problem persists, contact IBM Customer Support.

0x357b1294 There are no objects in the database or there are no objects in the specified state.
Explanation: Informational Message.
Action: None.

0x357b1295 Unable to shutdown the Object Signature Database: %s: %d
Explanation: An unexpected error occurred attempting to shut down the Object Signature Database.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x357b1296 Usage: To get the state of an object
pdosobjsig [-D DB-path] -g objname To check the state of an object
pdosobjsig [-D DB-path] -c objname To update the state of an object
pdosobjsig [-D DB-path] -u objname -s [trusted | untrusted] To update the state of all objects
pdosobjsig [-D DB-path] -s [trusted | untrusted] To list all the objects satisfying the given filter
pdosobjsig [-D DB-path] [-n] -l [all | trusted | untrusted] To display the version information
pdosobjsig -V Other optional flags
Explanation: Usage statement.
Action: None.

0x357b1297 Argument to -%c must be an object name. "%s" is invalid.
Explanation: Invalid argument.
Action: Check usage syntax, correct the problem and repeat the operation.

0x357b1298 Unable to read PDOSD configuration file %s: 0x%x: %s
Explanation: Unable to read the PDOSD configuration file.
Action: Check that the PDOSD configuration file exists, that the file permissions are set appropriately, and the policy set correctly on the file.

0x357b1299 The object, %s, cannot be set to untrusted state.
Explanation: Informational Message.
Action: None.

0x357b129a The state of the object, %s, is changed successfully.
Explanation: Informational Message.
Action: None.

0x357b129b %s
Explanation: Informational Message.
Action: None.

0x357b1500 Setting Object Signature Database timestamp failed: 0x%x: %s
Explanation: Setting the last check time in the database failed.
Action: See previous messages in the error log to determine the cause of the error. Correct the problem and restart the PDOS daemons. If the error persists, contact IBM Customer Support.

0x357b1501 Setting Object Signature Database version failed: 0x%x: %s
Explanation: Unable to set the version number in the Object Signature Database headers.
Action: See previous messages in the error log to determine the cause of the error. Correct the problem and restart the PDOS daemons. If the error persists, contact IBM Customer Support.
0x357b1502  Getting object signature state for TCB file
%s failed: 0x%x: %s

Explanation: An unexpected error occurred attempting to
obtain the signature state for the specified Trusted Computing
Base (TCB) file.
Action: Use the returned error code and error text to diagnose
and correct the problem. If the problem persists, contact IBM
Customer Support.

0x357b1503  Unable to add TCB file %s to the Object
Signature Database: 0x%x: %s

Explanation: Unable to add the Trusted Computing Base
(TCB) file to the Object Signature Database.
Action: Use the returned error code and error text to diagnose
and correct the problem. If the problem persists, contact IBM
Customer Support.

0x357b1504  Unable to enumerate contents of Object
Signature Database: 0x%x: %s

Explanation: Unable to enumerate contents of the Object
Signature Database.
Action: Use the returned error code and error text to diagnose
and correct the problem. If the problem persists, contact IBM
Customer Support.

0x357b1505  Unable to remove stale TCB file %s from
Object Signature Database: 0x%x: %s

Explanation: Unable to remove an old Trusted Computing
Base (TCB) entry from the Object Signature Database.
Action: Use the returned error code and error text to diagnose
and correct the problem. If the problem persists, contact IBM
Customer Support.

0x357b1506  Unable to remove TCB file %s from Object
Signature Database: 0x%x: %s

Explanation: Unable to delete a Trusted Computing Base
(TCB) file from the Object Signature Database.
Action: Use the returned error code and error text to diagnose
and correct the problem. If the problem persists, contact IBM
Customer Support.

0x357b1507  Unable to add TCB file %s to Object
Signature Database: 0x%x: %s

Explanation: Unable to add a Trusted Computing Base (TCB)
file to the Object Signature Database.
Action: Use the returned error code and error text to diagnose
and correct the problem. If the problem persists, contact IBM
Customer Support.

0x357b1508  TCB monitor instructed to both add and
remove TCB file %s from the Object
Signature Database

Explanation: The Trusted Computing Base (TCB) monitor
was instructed to both add and remove the TCB file from the
Object Signature Database. No change was made to the Object
Signature Database.
Action: None.

0x357b1509  TCB monitor unable to initialize the Object
Signature Database for database file %s:
0x%x: %s

Explanation: The Trusted Computing Base (TCB) monitor
was unable to initialize the Object Signature Database for the
database file.
Action: Use the returned error code and error text to diagnose
and correct the problem. If the problem persists, contact IBM
Customer Support.

0x357b150a  TCB monitor unable to check the state of the
database object in database file %s: 0x%x:
%s

Explanation: The Trusted Computing Base (TCB) monitor
was not able to check the state of the database object.
Action: Use the returned error code and error text to diagnose
and correct the problem. If the problem persists, contact IBM
Customer Support.

0x357b150b  TCB monitor instructed to add entry %s to
Object Signature Database but it is already
present.

Explanation: The Trusted Computing Base (TCB) monitor
was asked to add an entry to the Object Signature Database that
already exists.
Action: No action is necessary. The entry already exists in the
database.

0x357b150c  TCB monitor interval too short. Interval
expired with %d of %d entries still to check.

Explanation: The Trusted Computing Base (TCB) monitor
was unable to check all entries in the Object Signature
Database because the monitor interval was too short.
Action: Edit the PDOS configuration files and increase the
TCB monitor interval.
0x357b1580  TCB monitor audit logging unexpected event for %s: 0x%x state 0x%x
Explaination: The Trusted Computing Base (TCB) monitor encountered an unexpected event. This is an internal coding error.
Action: Contact IBM Customer Support.

0x357b1581  Unable to allocate audit record 0x%x:0x%x event on %s: 0x%x: %s
Explaination: Unable to allocate memory for audit record.
Action: See status message indicating why the audit record could not be allocated. Correct the error and retry the operation which generated this audit record.

0x357b1582  Unable to queue audit record 0x%x:0x%x event on %s: 0x%x: %s
Explaination: Unable to queue audit record.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x357b1f80  Reason : The object was created.
Explaination: Informational Message.
Action: None.

0x357b1f81  Reason : The object was deleted.
Explaination: Informational Message.
Action: None.

0x357d5002  ------- Policy Director context -------
Explaination: Information only.
Action: None.

0x357d5003  
Explaination: This dot will print during time consuming processes.
Action: None.

0x357d5007  The unconfiguration process did not complete successfully. See %s for more details.
Explaination: Information only.
Action: None.

0x357d500a  The drvconfig command failed. The devlinks command will not be attempted.
Explaination: The process failed before the devlinks command could be run.
Action: Run devlinks command manually from command line after fixing the problems.

0x357d500e  Enter the security master password:
Explaination: Prompts for the password.
Action: None.

0x357d500f  Enter the security master verification password:
Explaination: Prompts for the password again for verification.
Action: None.

0x357d5010  The security master password does not match the security master verification password.
Explaination: Enter the same password for security master password and the security master verification password.
Action: None.

0x357d5011  %s has begun.
Explaination: This indicates the beginning of the process.
Action: None.

0x357d5012  Following is the command line:
Explaination: This indicates the beginning of the command line logging.
Action: None.

0x357d5013  The unconfiguration process did not complete successfully. See %s for details.
Explaination: Errors occurred during the process.
Action: See the log file for details of each error.

0x357d5014  The file %s did not exist. Unable to change attributes.
Explaination: Information only.
Action: None required.
0x357d5015  The configuration process did not complete successfully. See %s for details.
Explanation: Errors occurred during the process.
Action: See the log file for details of each error.

0x357d5016  The pdoslpadm process completed successfully.
Explanation: The pdoslpadm process completed with no errors.
Action: None.

0x357d5017  See %s for more details.
Explanation: Tells the user the name of the log file.
Action: None.

0x357d5018  If additional policy information has been added, it will need to be removed manually.
Explanation: Additional user-added policy information should be removed by the user.
Action: Manually remove any policy information that was added without the configuration process.

0x357d5019  Unregistering Policy Director and policy-specific information.
Explanation: Any policy information just added will now be removed due to an error.
Action: None.

0x357d501a  The file %s was renamed to %s.
Explanation: Information only.
Action: None.

0x357d513c  File %s could not be removed.
Explanation: The file could not be removed.
Action: Check if the file exists and has the right permissions.

0x357d513f  File %s could not be removed since it does not exist.
Explanation: The file does not exist.
Action: None.

0x357d5515  The value specified, %s, must be a positive integer.
Explanation: The value is invalid due to non-numeric characters.
Action: Change the value to a positive integer and restart the process.

0x357d5516  The value for cred_hold must be greater than the values of both admin_cred_refresh and user_cred_refresh.
Explanation: The cred_hold value specified must be greater than the admin_cred_refresh and the user_cred_refresh.
Action: Modify the value of one or all three options and restart the process.

0x357d5517  All of the slots at positions 70-78, 82, or 83 in name_to_sysnum are already taken. Policy Director for Operating Systems needs one of these slots.
Explanation: Unable to locate an unused slot in the name_to_sysnum file.
Action: Free an item in range of 70-78, 82 or 83.

0x357d5518  Registering with Policy Director failed with error code %d.
Explanation: Could not run the registration command successfully.
Action: Fix the problem and reissue the command.

0x357d5519  Opening the configuration file failed with error code %d.
Explanation: Could not open necessary configuration file.
Action: Refer to the log file, check file permissions and paths.

0x357d551a  Stanza %s could not be added to configuration file %s.
Explanation: Unable to add a stanza to the configuration file.
Action: Check the file and directory permissions.

0x357d551b  Entry %s could not be deleted from configuration file %s.
Explanation: Unable to delete an entry from the configuration file.
Action: Check the file and directory permissions.
<table>
<thead>
<tr>
<th>Code</th>
<th>Message</th>
<th>Explanation</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x357d551c</td>
<td>Option %s is required and its value cannot be deleted.</td>
<td>The required items may not be deleted.</td>
<td>Remove the required items from the delete list.</td>
</tr>
<tr>
<td>0x357d551d</td>
<td>The value for option %s cannot be deleted.</td>
<td>The items specified cannot be deleted.</td>
<td>Remove the item from the delete list.</td>
</tr>
<tr>
<td>0x357d551e</td>
<td>Entry %s in stanza %s could not be added to configuration file %s.</td>
<td>Unable to add a stanza options the configuration file.</td>
<td>Check the file and directory permissions.</td>
</tr>
<tr>
<td>0x357d5520</td>
<td>Unknown password requirement found.</td>
<td>Internal error - unable to map password requirements.</td>
<td>Contact your service representative.</td>
</tr>
<tr>
<td>0x357d5522</td>
<td>Autostart feature could not be disabled.</td>
<td>There was an error using the /etc/inittab file.</td>
<td>Check file and directory permissions.</td>
</tr>
<tr>
<td>0x357d5523</td>
<td>Autostart feature could not be enabled.</td>
<td>There was an error using the /etc/inittab file.</td>
<td>Login as root, check file and directory permissions.</td>
</tr>
<tr>
<td>0x357d5524</td>
<td>Line %s could not be added to file %s.</td>
<td>There was an error using the /etc/inittab file.</td>
<td>Check the file and directory permissions.</td>
</tr>
<tr>
<td>0x357d5525</td>
<td>The option %s cannot be changed with a reconfiguration. In order to change this value, unconfigure and then configure with the new value.</td>
<td>Once the initial configuration has set this value, it cannot be changed.</td>
<td>To change this option, unconfigure and then configure.</td>
</tr>
<tr>
<td>0x357d5526</td>
<td>The option %s is required.</td>
<td>The option is required.</td>
<td>Reissue the command specifying the option.</td>
</tr>
<tr>
<td>0x357d5527</td>
<td>The quotation marks in %s are mismatched.</td>
<td>There is an unsupported number of quotation marks in the text.</td>
<td>Contact your service representative.</td>
</tr>
<tr>
<td>0x357d5528</td>
<td>The option %s requires a length of %d or less.</td>
<td>The length of the value needs to be shorter.</td>
<td>Reissue the command specifying a value with a shorter length.</td>
</tr>
<tr>
<td>0x357d5529</td>
<td>The option %s requires an integral value.</td>
<td>The option requires an integral value.</td>
<td>Reissue the command specifying an integral value.</td>
</tr>
<tr>
<td>0x357d552a</td>
<td>The option %s needs to be between %d and %d inclusive.</td>
<td>The option had a value out of range.</td>
<td>Reissue the command specifying a valid value.</td>
</tr>
<tr>
<td>0x357d552b</td>
<td>The option %s requires a value of 'on' or 'off'.</td>
<td>The option requires 'on' or 'off'</td>
<td>Reissue the command specifying a valid value.</td>
</tr>
<tr>
<td>0x357d552c</td>
<td>Setting the working directory to %s failed.</td>
<td>The directory could not be accessed.</td>
<td>Check the permissions and directory path.</td>
</tr>
<tr>
<td>0x357d552d</td>
<td>Memory could not be allocated.</td>
<td>Unable to allocate memory for processing data.</td>
<td>Contact your service representative.</td>
</tr>
<tr>
<td>0x357d552e</td>
<td>Response file option could not be mapped.</td>
<td>Could not map response file options.</td>
<td>Contact your service representative.</td>
</tr>
</tbody>
</table>
0x357d552f  Policy Director for Operating Systems daemon failed with error code %d.

Explanation:  Could not run Policy Director for Operating Systems daemon successfully.
Action:  Contact your service representative.

0x357d5530  The terminal state could not be saved.
Explanation:  Could not prepare the terminal for password prompting.
Action:  Contact your service representative.

0x357d5531  Echo mode could not be turned off.
Explanation:  Could not prepare the terminal for password prompting.
Action:  Contact your service representative.

0x357d5532  Password prompt could not be displayed.
Explanation:  Could not prompt for password.
Action:  Contact your service representative.

0x357d5533  The security master password is required.
Explanation:  Could not obtain a password from the user.
Action:  Reissue the command supplying the security master password.

0x357d5534  The option %s requires a value to be specified.
Explanation:  The option specified requires a value.
Action:  Reissue the command specifying a value for the option.

0x357d5535  The option %s has been specified more than once.
Explanation:  The option has been specified more than once.
Action:  Reissue the command specifying the option only once.

0x357d5536  The file %s could not be read.
Explanation:  Read access is required for the file specified in the response file.
Action:  Check the file permissions and reissue the command.

0x357d5537  The file %s does not exist.
Explanation:  The response file specified a file name that does not exist.
Action:  Check the spelling or path of the file name and reissue the command.

0x357d5538  The option %s is either an invalid option or is not unique.
Explanation:  The option specified is either not unique or is not valid.
Action:  Reissue the command specifying valid options.

0x357d5539  File %s could not be renamed to %s.
Explanation:  An error occurred renaming a file.
Action:  Check the permissions of the file and directory and check amount of disk space.

0x357d553a  This command must be run by the root user.
Explanation:  This command must be run by the root user because operations will be performed that require root authority.
Action:  Login as the root user and then reissue this command.

0x357d553b  %s failed.
Explanation:  An error occurred while executing a configuration command.
Action:  Contact your service representative.

0x357d553c  File %s could not be opened.
Explanation:  The process was unable to open file.
Action:  Check the file permissions and path.

0x357d553d  The -delete option requires a comma separated list.
Explanation:  A comma-delimited list could not be found after the -delete command line argument.
Action:  Add a list of items to delete or do not use the -delete option.

0x357d553e  %s was not a member of the set.
Explanation:  The policy file entry could be invalid.
Action:  Contact your service representative.
<table>
<thead>
<tr>
<th>Code</th>
<th>Message</th>
<th>Explanation</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x357d553f</td>
<td>Line %s could not be parsed.</td>
<td>The policy file entry could be invalid.</td>
<td>Contact your service representative.</td>
</tr>
<tr>
<td>0x357d5540</td>
<td>User %s could not be located in the passwd file.</td>
<td>Could not retrieve the user id from passwd file.</td>
<td>Contact your service representative.</td>
</tr>
<tr>
<td>0x357d5541</td>
<td>Group %s could not be located in the group file.</td>
<td>Could not retrieve the group id from group file.</td>
<td>Contact your service representative.</td>
</tr>
<tr>
<td>0x357d5542</td>
<td>Initialization for password generation failed.</td>
<td>Unable to create a password for the user or initialize parameters.</td>
<td>Contact your service representative.</td>
</tr>
<tr>
<td>0x357d5543</td>
<td>Random password could not be generated.</td>
<td>Unable to generate a random password for the user.</td>
<td>Contact your service representative.</td>
</tr>
<tr>
<td>0x357d5544</td>
<td>The devlinks command failed.</td>
<td>An error occurred while running the devlinks command.</td>
<td>Run devlinks manually from the command line.</td>
</tr>
<tr>
<td>0x357d5545</td>
<td>The drvconfig command failed.</td>
<td>An error occurred while executing the drivconfig command.</td>
<td>See log file for details.</td>
</tr>
<tr>
<td>0x357d5546</td>
<td>User creation in Policy Director failed.</td>
<td>Information only.</td>
<td>None required.</td>
</tr>
<tr>
<td>0x357d5547</td>
<td>Group creation in Policy Director failed.</td>
<td>Information only.</td>
<td>None required.</td>
</tr>
<tr>
<td>0x357d5548</td>
<td>Policy Director context could not be established.</td>
<td>An error occurred when trying to establish context.</td>
<td>Contact your service representative.</td>
</tr>
<tr>
<td>0x357d5549</td>
<td>Policy Director command %s failed.</td>
<td>An error occurred when trying to run a Policy Director command.</td>
<td>Contact your service representative.</td>
</tr>
<tr>
<td>0x357d554a</td>
<td>The line %s in file %s is invalid.</td>
<td>The policy file entry was invalid.</td>
<td>Contact your service representative.</td>
</tr>
<tr>
<td>0x357d554c</td>
<td>Parsing the Policy Director command information in file %s failed.</td>
<td>The policy file entry could be invalid.</td>
<td>Contact your service representative.</td>
</tr>
<tr>
<td>0x357d554d</td>
<td>Parsing line %s for roll back information failed.</td>
<td>The policy file entry could be invalid.</td>
<td>Contact your service representative.</td>
</tr>
<tr>
<td>0x357d554e</td>
<td>The Policy Director command could not be determined.</td>
<td>Could not identify the Policy Director command.</td>
<td>Contact your service representative.</td>
</tr>
<tr>
<td>0x357d554f</td>
<td>The ACL modify command could not be determined.</td>
<td>Could not identify the Policy Director ACL command.</td>
<td>Contact your service representative.</td>
</tr>
<tr>
<td>Error Code</td>
<td>Description</td>
<td>Explanation</td>
<td>Action</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>0x357d5550</td>
<td>The group modify command could not be determined.</td>
<td>Could not identify the Policy Director group command.</td>
<td>Contact your service representative.</td>
</tr>
<tr>
<td>0x357d5551</td>
<td>The account modify command could not be determined.</td>
<td>Could not identify the Policy Director account command.</td>
<td>Contact your service representative.</td>
</tr>
<tr>
<td>0x357d5552</td>
<td>The option whose value was to be deleted could not be determined.</td>
<td>The process could not understand the items specified for deletion.</td>
<td>Validate the items to be deleted and reissue the command.</td>
</tr>
<tr>
<td>0x357d5553</td>
<td>Policy Director has not been properly configured. Configuration values in pd.conf have not been set.</td>
<td>The pd.conf file is missing values necessary for configuration.</td>
<td>Run the Policy Director configuration process and re-start the process.</td>
</tr>
<tr>
<td>0x357d5554</td>
<td>The option -ldap_ssl_cacert must be specified during an initial configuration.</td>
<td>The process requires the -ldap_ssl_cacert option.</td>
<td>Issue the required options and restart the process.</td>
</tr>
<tr>
<td>0x357d5555</td>
<td>The option -ldap_ssl_cacert can only be specified on the initial configuration.</td>
<td>This value cannot be changed during a reconfiguration.</td>
<td>If these value needs to be changed, unconfigure first and then reconfigure.</td>
</tr>
<tr>
<td>0x357d5556</td>
<td>The Policy Director for Operating Systems daemon is running. Issue the &quot;rc.osseal stop&quot; command to stop it, then re-issue the command.</td>
<td>The pdosd daemon cannot be running during a configuration or unconfiguration process.</td>
<td>Issue the &quot;rc.osseal stop&quot; command and then try again.</td>
</tr>
<tr>
<td>0x357d5557</td>
<td>Unregistering with Policy Director failed with error code %d.</td>
<td>Could not unregister with Policy Director.</td>
<td>Fix the problem, then try again.</td>
</tr>
<tr>
<td>0x357d5558</td>
<td>The login_policy option was not detected.</td>
<td>The login_policy option is missing and should have been detected in the pdosd.conf file.</td>
<td>No action required, however, if pdoslpadm needs to be run, specify the option and reconfigure.</td>
</tr>
<tr>
<td>0x357d5559</td>
<td>The pdoslpadm process does not exist.</td>
<td>The configuration process could not run the pdoslpadm process.</td>
<td>Contact your service representative.</td>
</tr>
<tr>
<td>0x357d555a</td>
<td>The pdoslpadm process did not complete successfully.</td>
<td>An error occurred while running pdoslpadm. See the log for details.</td>
<td>Fix the error and restart the process.</td>
</tr>
<tr>
<td>0x357d555b</td>
<td>Error creating kdb and sth files with pdoscakdb.</td>
<td>An error occurred while running pdoscakdb. See the log for details.</td>
<td>Fix the error and restart the process.</td>
</tr>
<tr>
<td>0x357d555c</td>
<td>Unable to copy %s to %s.</td>
<td>The file could not be copied.</td>
<td>Check the permissions on the directory and file.</td>
</tr>
<tr>
<td>0x357d555d</td>
<td>Unable to locate necessary configuration files. Policy Director for Operating Systems may already be unconfigured.</td>
<td>The pdosd.conf or osseal.conf files could not be located.</td>
<td>Policy Director for Operating Systems may have already been unconfigured. If not, make sure the configuration files are in the /opt/pdos/etc directory.</td>
</tr>
</tbody>
</table>

240

Version 3.8
Unable to locate necessary configuration file values to initialize Policy Director context. The configuration files may be corrupt.

Explaination: The pdosd.conf or osseal.conf files did not contain all of the required information.
Action: Check the integrity of the configuration files and reissue the command.

The configuration files could be corrupt or missing required information. The %s will not be performed.

Explaination: The pdosd.conf or osseal.conf files did not contain all of the required information.
Action: Check the integrity of the configuration files and reissue the command.

Removal of objectspace, %s, failed. This process cannot clean up the objectspace.

Explaination: If the specified objectspace still exists, it should be cleaned manually.
Action: Run the pdadmin command to remove the objectspace manually.

The value of %s is invalid for the option %s.

Explaination: The user specified a value that is not valid for this option.
Action: Reissue the command and specify an appropriate value. See the option’s help for more details.

The security master password specified was invalid.

Explaination: The user specified the wrong password and the process failed.
Action: Reissue the command and specify the correct password.

Directory %s could not be opened.

Explaination: The program could not open a directory.
Action: Check if the directory exists and has the right permissions.

File %s could not be opened.

Explaination: The file could not be opened.
Action: Check permissions on the file or directory.

Temporary file %s could not be created.

Explaination: The file could not be created.
Action: Check permissions on the file or directory.

Calling stat for %s failed.

Explaination: The stat call failed.
Action: Check permissions on the file or directory.

The option %s is a required option.

Explaination: Missing command line option.
Action: Please specify the required option.

The key database file name could not be generated.

Explaination: The key database file name could not be generated from the certificate name.
Action: Contact your service representative.

The current time could not be determined.

Explaination: The current time on the machine could not be determined.
Action: Contact your service representative.

The password could not be generated.

Explaination: A password could not be generated.
Action: Contact your service representative.

Initializing the encryption toolkit failed with return code %d.

Explaination: The encryption toolkit could not be initialized.
Action: Contact your service representative.

Reading the certificate file %s failed with return code %d.

Explaination: The certificate file could not be read.
Action: Check the permissions on the certificate file and make sure it is not corrupted.
Creating the key database file with default certificates failed with return code.

Explanation: The key database file could not be created with default certificates.
Action: Contact your service representative.

Creating the stash file failed with return code.

Explanation: The stash file could not be created.
Action: Contact your service representative.

Storing the certificate in the key database file failed with return code.

Explanation: The certificate could not be stored in the key database file.
Action: Contact your service representative.

Closing the key database file failed with return code.

Explanation: The key database file could not be closed.
Action: Contact your service representative.

Creating the key database file and stash file was not successful. See the log for details.

Explanation: The key database file and stash file was not created successfully.
Action: Correct the problem and reissue the command.

The PDOS Credential Service is already initialized.

Explanation: The PDOS Credential Service is currently initialized in a valid state and an attempt was made to initialize again to the same state.
Action: Restart the daemons and report the error to IBM Customer Support.

The PDOS Credential Service is not yet initialized.

Explanation: An internal service attempted to retrieve credential information from the PDOS Credential Service before the service was available.
Action: Restart the daemons and report the error to IBM Customer Support.

Policy Director user registry is unavailable (isolation mode).

Explanation: The PDOS Credential Service is unable to communicate with the Policy Director user registry. PDOS continues to operate but is unable to retrieve any new credentials until connectivity is once again established.
Action: Verify that network connectivity exists to the Policy Director user registry and correct any communication problems. Check that the user registry itself is in a valid state and correct any errors.

Policy Director user registry is available.

Explanation: The PDOS Credential Service is able to communicate with the Policy Director user registry to obtain new credentials.
Action: None

unauthenticated user

Explanation: Informational message indicating that a user has unauthenticated credentials. Local UNIX users without corresponding Policy Director user IDs have unauthenticated credentials.
Action: None

Initialization of the PDOS Credential Service Memory Cache failed

Explanation: An error occurred when the PDOS Credential Service attempted to initialize its Memory Cache.
Action: This message is preceded by one or more error messages from the Memory Cache. Correct the cause of the failure, then restart the daemons.

Initialization of the PDOS Credential Service Disk Cache failed

Explanation: An error occurred when the PDOS Credential Service attempted to initialize its Disk Cache.
Action: This message is preceded by one or more error messages from the Disk Cache. Correct the cause of the failure, then restart the daemons.

Initialization of the PDOS Credential Service UUID Cache failed

Explanation: An error occurred when the PDOS Credential Service attempted to initialize its UUID Cache.
Action: This message is preceded by one or more error messages from the UUID Cache. Correct the cause of the failure, then restart the daemons.
0x357e2009  The credential’s expiration time has passed

Explanation:  An attempt was made to cache a credential that has already expired. This error may occur when the PDOS Credential Service is unable to communicate with the Policy Directory user registry. When the PDOS Credential Service is operating in this mode, credentials are retrieved from the Disk Cache and may be stored in the Memory Cache. If the refresh time expires between the time the credential is retrieved from the Disk Cache but before it is stored in the Memory Cache, this error occurs.

Action:  None

0x357e200a  The requested credential was not found in the cache

Explanation:  The PDOS Credential Service was unable to find a credential for a user in either the Memory Cache or the Disk Cache. This is usually a normal condition. If this message appears in an error message, it may be an indication that the cache is corrupted.

Action:  Restart the daemons and report this error to IBM Customer Support.

0x357e200b  No login policy is cached for unauthenticated users.

Explanation:  The Disk Cache contains no login policy time-of-day restrictions for unauthenticated users.

Action:  None

0x357e200c  No Admin Group Information is cached.

Explanation:  The Disk Cache contains no osseal-admin group information. This is a normal condition during Disk Cache initialization.

Action:  None

0x357e200d  The requested credential is unauthenticated

Explanation:  A PDOS Credential Service cache entry was found for the user indicating that the user has unauthenticated credentials.

Action:  None

0x357e200e  The PDOS Credential Service Memory Cache is full

Explanation:  All entries in the PDOS Credential Service Memory Cache are in use.

Action:  No action is required. Old entries in the cache that are eligible for deletion are automatically reused when new credentials must be cached.

0x357e200f  The PDOS Credential Service Memory Cache is full and the LRU list contains no entries that may be deleted

Explanation:  All entries in the PDOS Credential Service Memory Cache are in use and there are no entries eligible for deletion. Because the credentials for administrative users are not eligible for deletion, this condition can occur when a large number of administrative users are defined.

Action:  No action is required. The PDOS Credential Service Memory Cache automatically increases the number of entries in the cache. To prevent this message from occurring on subsequent restarts, reduce the number of administrative users defined in the osseal-admin group.

0x357e2010  Failed to open the PDOS Credential Service Disk Cache Directory

Explanation:  The PDOS Credential Service was unable to open the directory containing the Disk Cache using the opendir system call.

Action:  Verify that the /var/pdos/cred directory exists and that both the UNIX permissions and PDOS policy permit pdosd to read that directory.

0x357e2011  Failed to close the PDOS Credential Service Disk Cache Directory

Explanation:  The PDOS Credential Service was unable to close the directory containing the Disk Cache using the closedir system call.

Action:  Verify that the /var/pdos/cred directory exists.

0x357e2012  invalid pointer

Explanation:  An internal service passed a bad pointer to an internal function.

Action:  Restart the daemons and report the error to IBM Customer Support.

0x357e2013  invalid buffer size specified

Explanation:  An internal service specified an incorrect data size to an internal function.

Action:  Restart the daemons and report the error to IBM Customer Support.

0x357e2014  credential needs a refresh

Explanation:  The requested credential was found in the PDOS Credential Service Disk Cache but it should be refreshed by the PDOS Credential Service, if possible.

Action:  No action is required. If the PDOS Credential Service is running in isolation mode, the credential will be refreshed when PDOS comes out of isolation. Otherwise, the credential will be refreshed immediately.
0x357e2015  Credential Disk File error

**Explanation:** The PDOS Credential Service was unable to read or write to one of the cache files in the Disk Cache directory.

**Action:** Verify that the `/var/pdos/cred` directory exists, that both the UNIX permissions and PDOS policy permit `pdosd` to read and write to that directory and the files contained within that directory, and that there is sufficient free disk space in the filesystem containing the `/var/pdos/cred` directory.

0x357e2016  Credential Disk File open error

**Explanation:** The PDOS Credential Service was unable to open one of the cache files in the Disk Cache directory.

**Action:** Verify that the `/var/pdos/cred` directory exists, that both the UNIX permissions and PDOS policy permit `pdosd` to read and write to that directory and the files contained within that directory, and that there is sufficient free disk space in the filesystem containing the `/var/pdos/cred` directory.

0x357e2017  Credential Disk File close error

**Explanation:** The PDOS Credential Service was unable to close one of the cache files in the Disk Cache directory.

**Action:** Verify that the `/var/pdos/cred` directory exists.

0x357e2018  The entry already exists

**Explanation:** An attempt was made to cache a credential in the PDOS Credential Service Memory Cache that is already cached.

**Action:** Restart the daemons and report the error to IBM Customer Support.

0x357e2019  The entry does not exist

**Explanation:** An attempt was made to access an entry in the PDOS Credential Service Disk Cache that does not exist.

**Action:** None

0x357e201a  An error occurred while getting the PAC

**Explanation:** An error occurred while the PDOS Credential Service Disk Cache was converting the credential from the internal Policy Director format to the PDOS Credential Service Disk Cache format.

**Action:** Restart the daemons and report the error to IBM Customer Support.

0x357e201b  An error occurred while converting the PAC

**Explanation:** An error occurred while the PDOS Credential Service Disk Cache was converting the credential from the PDOS Credential Service Disk Cache format to the internal Policy Director format.

**Action:** Restart the daemons and report the error to IBM Customer Support.

0x357e201c  The Policy Director registry is not initialized.

**Explanation:** A call to the Policy Director user registry failed because a connection to the user registry does not exist.

**Action:** Check the status of the Policy Director user registry. If the user registry is not functioning properly, shut down and restart the Policy Director user registry server. If the problem persists, contact IBM Customer Support.

0x357e201d  Invalid parameters passed to the Policy Director registry API.

**Explanation:** A call to the Policy Director user registry failed because incorrect parameters were specified.

**Action:** Restart the daemons and report the error to IBM Customer Support.

0x357e201e  The user account is marked as invalid in the Policy Director registry.

**Explanation:** An attempt to get user credentials from the Policy Directory user registry failed because the user account is marked as invalid.

**Action:** Modify the Policy Director user registry to set account-valid to yes for the user account.

0x357e201f  The user is a not a Policy Director user.

**Explanation:** An attempt to get user credentials from the Policy Directory user registry failed because the user account specified is not a valid Policy Director user name.

**Action:** Verify that the user account specified is correct. If it is correct, update the Policy Director user registry.

0x357e2020  The Policy Director user registry is either not responding or is busy. The operation will be retried.

**Explanation:** There are too many requests to the Policy Director user registry pending. The requested operation was not completed. This condition is usually caused by the server being overloaded or inoperative.

**Action:** Verify that the Policy Director user registry is functioning properly. If the problem persists, contact IBM Customer Support.
<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
<th>Explanation</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x357e2021</td>
<td>The Credential Acquisition Service tried to generate an unexpected audit event.</td>
<td>An attempt was made to audit an event that is not recognized by the PDOS Credential Service.</td>
<td>Restart the daemons and report the error to IBM Customer Support.</td>
</tr>
<tr>
<td>0x357e2022</td>
<td>Credential Acquisition Service initialization failed.</td>
<td>An error occurred during the initialization of the PDOS Credential Service.</td>
<td>This message is preceded by one or more error messages. Correct the cause of the failure, then restart the daemons. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x357e2023</td>
<td>There are no admin users found in the UNIX registry.</td>
<td>An error occurred when the PDOS Credential Service tried to cache credentials for members of the osseal-admin group. This error indicates that there are either no members of the group or none of the members of the group are local UNIX users.</td>
<td>Create entries in the UNIX Registry corresponding to one or more members of the osseal-admin group in the Policy Director user registry.</td>
</tr>
<tr>
<td>0x357e2024</td>
<td>Invalid authentication information was presented to Policy Director.</td>
<td>An authentication error occurred when PDOS attempted to communicate with the Policy Director user registry. This error indicates that a problem exists with the bind-dn and bind-pwd entries in the /opt/pdos/etc/pdosd.conf file.</td>
<td>Verify that the bind-dn and bind-pwd entries in the /opt/pdos/etc/pdosd.conf file are correct. The pdadmin command can be used to check the validity of the bind-dn and bind-pwd values are valid. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x357e2025</td>
<td>An error occurred in Policy Director function call.</td>
<td>An error occurred when an internal service attempted to call the Policy Director user registry.</td>
<td>Restart the daemons and report the error to IBM Customer Support.</td>
</tr>
<tr>
<td>0x357e2026</td>
<td>Unable to convert the UUID to group name.</td>
<td>An error occurred when converting a Policy Director user registry group UUID from a users credential into a common name.</td>
<td>Use the pdosrefresh command to refresh the users cached credential.</td>
</tr>
<tr>
<td>0x357e2080</td>
<td>Could not get the members of the admin group,,%s</td>
<td>An error occurred when retrieving the list of members of the osseal-admin group.</td>
<td>Verify that the connection to the Policy Director user registry is functioning properly and that the certificates in /var/pdos/certs are valid.</td>
</tr>
<tr>
<td>0x357e2081</td>
<td>Cannot connect to the LDAP Server. rc = 0x%x</td>
<td>An error occurred when the PDOS Credential Service attempted to communicate with the Policy Director user registry. There are a number of reasons why this communication could fail. The most likely ones are a problem with network connectivity or a problem with the user registry itself. PDOS will continue to function in this state but cannot retrieve any new credentials.</td>
<td>Verify that the connection to the Policy Director user registry is functioning properly and that the certificates in /var/pdos/certs are valid.</td>
</tr>
<tr>
<td>0x357e2082</td>
<td>The Policy Director Registry call failed with the error code of 0x%x</td>
<td>The Policy Director user registry returned the specified error when called by the PDOS Credential Service.</td>
<td>Restart the daemons and report the error to IBM Customer Support.</td>
</tr>
<tr>
<td>0x357e2083</td>
<td>Unable to create a new credential structure for the uid, %lld: major:minor: 0x%x:0x%x</td>
<td>An error occurred when the PDOS Credential Service attempted to allocate a new credential structure using the Policy Director API.</td>
<td>Use the returned major and minor error codes, as well as the error text, to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>Error Code</td>
<td>Description</td>
<td>Explanation</td>
<td>Action</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
<td>-------------</td>
<td>--------</td>
</tr>
<tr>
<td>0x357e2084</td>
<td>Unable to create a new credential structure for the unauth user: major:minor: 0x%x:0x%x</td>
<td>An error occurred when the PDOS Credential Service attempted to allocate a new credential structure using the Policy Director API.</td>
<td>Use the returned major and minor error codes, as well as the error text, to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x357e2085</td>
<td>Unable to get a credential for the uid, %lld : message: major: minor: %s:0x%x:0x%x</td>
<td>An error occurred when the PDOS Credential Service attempted to obtain a credential for the specified user from Policy Director.</td>
<td>Use the returned major and minor error codes, as well as the error text, to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x357e2086</td>
<td>Unable to get unauthenticated credential : major: minor: 0x%x:0x%x</td>
<td>An error occurred when the PDOS Credential Service attempted to obtain a credential for an unauthenticated user from Policy Director.</td>
<td>Use the returned major and minor error codes, as well as the error text, to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x357e2087</td>
<td>Cannot find the time of day login policy for unauthenticated user.</td>
<td>The time of time-of-day login policy for unauthenticated users cannot be found in the Policy Director user registry. The osseal-unauth user is created during initial PDOS configuration. The time-of-day login policy for unauthenticated users is associated with the osseal-unauth user. This error indicates that the osseal-unauth user has been deleted from the user registry.</td>
<td>Re-create the osseal-unauth user in the Policy Director user registry and set the tod-access policy appropriately. To see how the osseal-unauth user was initially created, look at the /opt/pdos/etc/osseal.once-only script.</td>
</tr>
<tr>
<td>0x357e2088</td>
<td>Error waiting for Credential Service initialization. The error status is 0x%x: %s.</td>
<td>An error occurred when one of the PDOS Credential Service threads was waiting for initialization to complete.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x357e2100</td>
<td>Unable to delete the credential: credential handle %d</td>
<td>An error occurred when deleting a cached credential from the PDOS Credential Service Memory Cache.</td>
<td>Restart the daemons and report the error to IBM Customer Support.</td>
</tr>
<tr>
<td>0x357e2101</td>
<td>Unable to get an entry in the memory cache to cache the credential: %d: %s</td>
<td>An error occurred when allocating space to cache a credential in the PDOS Credential Service Memory Cache.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x357e2180</td>
<td>Unable to initialize the Disk Cache: %d: %s</td>
<td>An error occurred when initializing the PDOS Credential Service Disk Cache.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x357e2181</td>
<td>Unable to update access times for Disk Cache Entries: %d: %s</td>
<td>An error occurred during the shut down of a daemon which prevented one or more credential access times from being updated in the PDOS Credential Service Disk Cache.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x357e2182</td>
<td>Unable to cache the credential in the Disk Cache: %d: %s</td>
<td>An error occurred when caching a credential in the PDOS Credential Service Disk Cache.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x357e2183</td>
<td>Unable to lookup the credential in the Disk Cache: %d: %s</td>
<td>An error occurred when retrieving an entry from the PDOS Credential Service Disk Cache.</td>
<td>Restart the daemons and report the error to IBM Customer Support.</td>
</tr>
</tbody>
</table>
Unable to cache the login policy for unauthenticated users in the Disk Cache: %d: %s

Explanation: An error occurred when caching the login policy time-of-day restrictions for unauthenticated users in the PDOS Credential Service Disk Cache.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Unable to retrieve the login policy for unauthenticated users from the Disk Cache: %d: %s

Explanation: An error occurred when retrieving the login policy time-of-day restrictions for unauthenticated users from the PDOS Credential Service Disk Cache.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Unable to cache the Admin Group information in the Disk Cache: %d: %s

Explanation: An error occurred when caching the list of members of the osseal-admin group in the PDOS Credential Service Disk Cache.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Unable to retrieve the Admin Group information from the Disk Cache: %d: %s

Explanation: An error occurred when retrieving the list of members of the osseal-admin group from the PDOS Credential Service Disk Cache.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

An error occurred while reading the credential from the Disk Cache: %d: %s

Explanation: An error occurred when reading a cached credential from the PDOS Credential Service Disk Cache.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

An error occurred while deleting the credential from the Disk Cache: %d: %s

Explanation: An error occurred when deleting a cached credential from the PDOS Credential Service Disk Cache.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

An error occurred while executing the Database Maintenance thread: %d: %s

Explanation: An error occurred when the maintenance thread associated with the PDOS Credential Service Disk Cache was either refreshing cached credentials which have exceeded their refresh interval, deleting cached credentials which have exceeded their hold interval, or updating access times of cached credentials.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Unable to audit a credential related event. Audit event ID 0x%x is unknown.

Explanation: An attempt was made to audit an event that is not recognized by the PDOS Credential Service.

Action: Restart the daemons and report the error to IBM Customer Support.

Error allocating audit record for event %s (0x%x). The error status is 0x%x: %s

Explanation: An error occurred when allocating space for an audit record.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Error auditing event %s (0x%x). The error status is 0x%x: %s.

Explanation: An error occurred when the PDOS Credential Service tried to add an audit event to the audit queue.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.
0x358a3081  One or more required options are missing.

Explanation: One or more required options are missing from the pdoshla command.

Action: Verify the proper syntax of the pdoshla command. Correct the problem and retry the pdoshla command.

0x358a3082  Unable to initialize the Host Look-aside database: %s: %d

Explanation: An error occurred during the initialization of the pdoshla command.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x358a3084  Unable to flush all the entries from the Host Look-aside database: %s: %d

Explanation: An error occurred while the pdoshla command was flushing entries from the database. Some of the entries might have been successfully flushed.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x358a3085  Unable to refresh the contents of Host Look-aside database: %s: %d

Explanation: An error occurred while the pdoshla command was refreshing all of the entries in the database. Some of the entries might have been successfully refreshed.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x358a3087  Usage: To flush all the entries pdoshla [-D DB-path] -F To flush all stale entries pdoshla [-D DB-path] -f To remove an entry pdoshla [-D DB-path] -r <IP-addr> To add/replace an entry pdoshla [-D DB-path] -a <IP-addr> [-T <TTL-secs>] -H <Hostname> To list all the entries satisfying the given filter pdoshla [-D DB-path] -l [all | stale | fresh ] To refresh all the entries pdoshla [-D DB-path] -u To display the version information pdoshla -V Other optional flags pdoshla [-vh?] [-t trace-string]

Explanation: pdoshla command usage statement.

Action: None

0x358a3088  The IP address, %s, was not found in the Host Look-aside database.

Explanation: The specified IP address was not found in the Host Look-aside database.

Action: Retry the command using a network IP address that exists in the Host Look-aside database.

0x358c0001  password parameters have not been initialized

Explanation: An internal service attempted to do password processing prior to initialization.

Action: Contact IBM Customer Support.

0x358c0002  failed getting the Policy Director minimum password length

Explanation: An error occurred while retrieving the password policy for the minimum password length from Policy Director.

Action: Contact IBM Customer Support.

0x358c0003  failed getting the Policy Director minimum password alphabetic characters

Explanation: An error occurred while retrieving the password policy for the minimum number of alphabetic characters from Policy Director.

Action: Contact IBM Customer Support.

0x358c0004  failed getting the Policy Director minimum password non-alphabetic characters

Explanation: An error occurred while retrieving the password policy for the minimum number of non-alphabetic characters from Policy Director.

Action: Contact IBM Customer Support.

0x358c0005  failed getting the Policy Director maximum password repeated characters

Explanation: An error occurred while retrieving the password policy for the maximum number of repeated characters from Policy Director.

Action: Contact IBM Customer Support.

0x358c0006  failed checking if Policy Director allows spaces in passwords

Explanation: An error occurred while retrieving the password policy for spaces in a password from Policy Director.

Action: Contact IBM Customer Support.
The password length is less than the length required by PD

**Explanation:** An error occurred during password verification indicating that the length of the supplied password is less than the minimum password length required by the Policy Director policy.

**Action:** Use the `pdadmin> policy get min-password-length` command to query the password length policy. Retry the command specifying a password which adheres to the Policy Director policy.

The number of alphabetic characters in the password is less than the number required by PD

**Explanation:** An error occurred during password verification indicating that the number of alphabetic characters in the supplied password is less than the minimum number of alphabetic characters required by the Policy Director policy.

**Action:** Use the `pdadmin> policy get min-password-alphas` command to query the password alphas policy. Retry the command specifying a password which adheres to the Policy Director policy.

The number of non-alphabetic characters in the password is less than the number required by PD

**Explanation:** An error occurred during password verification indicating that the number of non-alphabetic characters in the supplied password is less than the minimum number of non-alphabetic characters required by the Policy Director policy.

**Action:** Use the `pdadmin> policy get min-password-non-alphas` command to query the password alphas policy. Retry the command specifying a password which adheres to the Policy Director policy.

No spaces allowed in the password passed to PD

**Explanation:** An error occurred during password verification indicating that the supplied password contains spaces and the Policy Director policy does not allow spaces.

**Action:** Use the `pdadmin> policy get password-spaces` command to query the password spaces policy. Retry the command specifying a password which adheres to the Policy Director policy.

The number of repeated characters in the password is greater than the number allowed by PD

**Explanation:** An error occurred during password verification indicating that the number of repeated characters in the supplied password is greater than the maximum number of repeated characters allowed by the Policy Director policy.

**Action:** Use the `pdadmin> policy get max-password-repeated-chars` command to query the password repeated characters policy. Retry the command specifying a password which adheres to the Policy Director policy.

The following informational message was returned from `ivadmin`: 0x%x: %s

**Explanation:** Policy Director messages have varying levels of severity. This message is informational.

**Action:** Use the returned message code and message text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

The following warning message was returned from `ivadmin`: 0x%x: %s

**Explanation:** Policy Director messages have varying levels of severity. This message is a warning.

**Action:** Use the returned message code and message text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

The following error message was returned from `ivadmin`: 0x%x: %s

**Explanation:** Policy Director messages have varying levels of severity. This message is an error.

**Action:** Use the returned message code and message text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

The following message was returned from `ivadmin`: 0x%x: %s

**Explanation:** Policy Director messages have varying levels of severity. This message is used when we cannot determine the type of the returned message.

**Action:** Use the returned message code and message text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.
0x358cd001  See %s for more details.
Explanation: Information only.
Action: None

0x358cd002  Unable to determine machine type.
Explanation: The script was unable to determine the operating system of the machine.
Action: Ensure that you are running the script for your operating system.

0x358cd003  Tivoli PDOS Installation and Configuration is complete.
Explanation: Installation and configuration of Tivoli Policy Director for Operating Systems is complete.
Action: None

0x358cd004  This script will only work on %s
Explanation: The script is platform dependent and can only be run on the operating system specified.
Action: Either find the appropriate script for your platform, or run the script that failed on the appropriate system.

0x358cd006  You must be the root user to run this process.
Explanation: This script only can be run by the root, or super, user.
Action: Log in as root and retry the operation.

0x358cd007  pkginfo file was not found in %s.
Explanation: The pkginfo file could not be located on the CD.
Action: Contact IBM Customer Support.

0x358cd008  Press ENTER to see the available %s language files:
Explanation: Prompt to the user that the available language files are ready to be displayed.
Action: Press the ENTER key to continue.

0x358cd019  %s in the set %s does not exist.
Explanation: Could not locate an expected file for installation.
Action: The file is skipped and processing continues.

0x358cd01a  Not installing the %s component.
Explanation: Files needed for installing the specified component are missing. The component is not installed.
Action: Contact IBM Customer Support.

0x358cd01c  Press ENTER to begin the installation.
Explanation: See message.
Action: Press the ENTER key to begin the installation.

0x358cd021  Enter a number to modify, or y to begin configuration:
Explanation: Prompts the user to enter a number of the configuration option to modify. Enter y to accept the current configuration values and continue with the installation.
Action: Enter the number of the configuration option you wish to modify or enter y to continue with the installation without further modifications.

0x358cd022  Enter the LDAP Server Hostname:
Explanation: Prompts the user to enter the host name of the LDAP server.
Action: Enter the host name of the LDAP server.

0x358cd023  Enter the LDAP Server Port Number:
Explanation: Prompts the user to enter the port number of the LDAP server.
Action: Enter the port number for the LDAP server.

0x358cd024  Enter the Policy Director Manager Hostname:
Explanation: Prompts the user to enter the host name of the Tivoli Policy Director Management Server machine.
Action: Enter the host name of the Tivoli Policy Director Management Server machine.

0x358cd025  Enter the Policy Director Certificate Filename:
Explanation: Prompts the user to enter the name of the certificate file.
Action: Enter the name of the certificate file.
Enter the SSL listening port used by PDMgr:
Explanation: Prompts the user to enter the SSL listening port used by the Tivoli Policy Director Management Server.
Action: Enter the SSL listening port.

Press ENTER to continue...
Explanation: The process is waiting for the user to press the ENTER key.
Action: Press the ENTER key.

The file %s could not be read. Verify the path of the file and change the value.
Explanation: The specified file could not be read.
Action: Check the path and file name and re-enter them.

Enter the LDAP Certificate Filename:
Explanation: Prompts the user to enter the name of the LDAP SSL CA certificate file from the LDAP server machine.
Action: Enter the name of the certificate file.

Enter the suffix:
Explanation: Prompts the user to enter the LDAP User Registry suffix.
Action: Enter the LDAP User Registry suffix.

Enter the Name of the Policy Branch:
Explanation: Prompts the user to enter name of the policy branch under which Tivoli Policy Director for Operating Systems is being configured.
Action: Enter the name of the policy branch name.

Enter the Security Master Password (not required here):
Explanation: Prompts the user to enter the Tivoli Policy Director security master password.
Action: Enter the security master password here, if desired. This value is optional.

Enter the name of the Response File (not required):
Explanation: Prompts the user to enter the name of the response file to be used for configuration.
Action: If you wish to use a response file for configuration, enter the name of the response file here. Leave this field blank if you do not wish to use a response file.

All values must be supplied before continuing.
Explanation: A required value is missing.
Action: Supply a value for all required values before continuing.

An error occurred while configuring Policy Director.
Explanation: Information only.
Action: None

An error occurred while configuring Policy Director for Operating Systems.
Explanation: Information only.
Action: None

An error occurred while installing %s.
Explanation: Information only.
Action: None

See %s for more details.
Explanation: An unexpected error occurred during the installation process. See the specified log file for additional information on the errors encountered.
Action: Correct the problem and retry. If the error persists, contact IBM Customer Support.

Could not find the %s file.
Explanation: A necessary file could not be located.
Action: Check the file permissions and directory path.

Not Specified
Explanation: This message tells the user the status of a configuration option.
Action: None

Not Required
Explanation: This message tells the user that the component is not required.
Action: None
0x358cd04e  Not Available
Explanation: This message tells the user that the component is not available.
Action: None

0x358cd04f  Selected
Explanation: This message tells the user that the component is selected for installation.
Action: None

0x358cd050  The response file could not be read.
Explanation: The response file name issued on the command line could not be read.
Action: Check the path, name, and permissions of the response file and try again.

0x358cd051  The response file is missing the required values.
Explanation: One or more of the required values is missing from the response file.
Action: Add the values to the response file and try again, or run the process without the response file.

0x3591c001  Updating policy
Explanation: An updated version of the policy is being sent to the PDOS kernel.
Action: None. Another message is produced when the update to the policy is complete.

0x3591c002  Finished updating policy (version number = %lld)
Explanation: The update of the policy is complete. The updated policy is now in effect.
Action: None

0x3591c003  Invalid date (%s) attached to protected object name (%s)
Explanation: The format of the holiday date attached to the object is not valid.
Action: Verify that the holiday date specified is correct. Re-create the policy to ensure the correct version is being used.

0x3591c004  Attribute (%s) not defined in ACL template attached to %s
Explanation: The attribute specified is not explicitly defined in the ACL template associated with the object.
Action: No action is required if you want to use the default values for the attribute. Otherwise, add the desired values for the attribute to the ACL template.

0x3591c005  Attribute (%s) not defined in %s attached to %s
Explanation: The attribute specified is not explicitly defined in the Object, POP or ACL associated with the object.
Action: No action is required if you want to use the default values for the attribute. Otherwise, add the desired values for the attribute to the appropriate template.

0x3591c006  The following invalid permissions (%s) are ignored in the Access-Restrictions attribute value (%s). Only OSSEAL permissions are allowed.
Explanation: The Access-Restrictions attribute value has incorrect permissions specified. Only OSSEAL access permissions are allowed.
Action: Correct the permissions in the specified Access-Restriction attribute value so that only OSSEAL permissions are specified.

0x3591c007  No Sudo argument present
Explanation: No Sudo arguments were found for the Sudo command.
Action: Add an attribute specifying the Sudo arguments to be used.

0x3591c008  No Sudo Command present
Explanation: No Sudo command attribute was found.
Action: Add an attribute specifying the Sudo command to be issued.

0x3591c009  Attribute %s which is attached to %s needs to be a single valued attribute, random value will be enforced.
Explanation: The attribute specified appears to have multiple values or to have been incorrectly specified multiple times. This attribute only accepts a single value and must be specified only once. The value being used for this attribute is unpredictable.
Action: Correct the attribute so that it only has a single value and delete multiple occurrences of the attribute.
Could not add policy for %s : Reason: %d:%s
Explanation: The policy for the specified object could not be added.
Action: See the associated reason for cause of problem. Correct the problem and retry the operation.

Could not delete policy for %s : Reason: %d:%s
Explanation: The policy for the specified object could not be deleted.
Action: See the associated reason for cause of problem. Correct the problem and retry the operation.

Invalid policy name (%s)
Explanation: The name of the policy specified is not valid.
Action: Verify the syntax for the policy name and correct it. After the updated policy has been replicated on the machine, make sure you do not see this error message. If problem persists, contact IBM Support.

Error (%d): %s
Explanation: An error occurred while processing a request.
Action: Use the error code and error text provided to determine the cause of the error and correct the problem.

Invalid Access-Restrictions attribute value: (%s)
Explanation: An incorrect value was found for an Access-Restrictions attribute.
Action: Verify the syntax of the Access-Restrictions attribute value and correct it. After the updated policy has been replicated on the machine, retry the request that failed.

The Access-Restrictions attribute has an unknown accessor type (%s)
Explanation: An unknown accessor type was specified for an Access-Restrictions attribute value.
Action: Verify the syntax of the accessor type for the Access-Restrictions attribute and correct it. After the updated policy has been replicated on the machine, retry the request that failed.

KPCMGR: Mutex lock failed
Explanation: The PDOS Kernel Policy Cache Manager (KPCMGR) was unable to obtain the mutex lock to serialize updates to the policy database. The old policy will continue to be enforced.
Action: Check system resources, such as virtual memory usage and the number of active threads, to determine why the obtain of the mutex lock failed. Correct the problem. If the problem persists, contact IBM Customer Support.

KPCMGR: Mutex unlock failed
Explanation: The PDOS Kernel Policy Cache Manager (KPCMGR) was unable to release the mutex lock after processing a policy update notification from Policy Director.
Action: Check system resources, such as virtual memory usage and the number of active threads, to determine the cause of the mutex unlock failure. Restart the PDOS daemons. If the problem persists, contact IBM Customer Support.

KPCMGR: Mutex initialization failed
Explanation: The PDOS Kernel Policy Cache Manager (KPCMGR) failed during mutex initialization.
Action: Check system resources, such as virtual memory usage and the number of active threads, to determine the cause of the mutex initialization failure. Restart the PDOS daemons. If the problem persists, contact IBM Customer Support.

Conflicting policy: Policies cannot exist on a Login Terminal entry with the same name as the basename of a wildcarded File entry
Explanation: An error occurred because of conflicting policy definitions. Policies exist on a Login Terminal entry and a wildcard file entry with the same basename as the Login Terminal. This is not permitted.
Action: Correct the conflicting policy for the file by removing it from either the Login Terminal or the wildcard entry.

Error in getting unauthenticated credentials
Explanation: An error occurred when attempting to obtain a credential for an unauthenticated user from Policy Director.
Action: This message is preceded by one or more error messages. Correct the cause of the failure, then retry the request that failed.
### 0x3591c089 Invalid Access-Restrictions attributes attached to %s

**Explanation:** An error occurred processing the Access-Restrictions extended attribute. The extended attribute is associated with the specified protected object name. One or more of the Access-Restrictions attribute values attached to the object may be invalid.

**Action:** Remove the incorrect Access-Restrictions attribute values attached to the object. Retry the request after the updated policy gets replicated.

### 0x3591c08a Error removing old Sudo entry %s (%s)

**Explanation:** An error occurred removing the Sudo entry specified.

**Action:** Use the error text provided in the message to determine why the Sudo entry could not be removed and correct the problem.

### 0x3591c08b Error adding Wildcard entry %s (err = %d)

**Explanation:** An error occurred adding the wildcard entry specified.

**Action:** Use the error status provided in the message to determine the cause of the problem and correct it.

### 0x3591c08c Error in removing File from Wildcard Database %s (err = %s)

**Explanation:** An error occurred when removing a file from the Wildcard Database.

**Action:** Use the error text provided in the message to determine the cause of the problem and correct it. If the problem persists, contact IBM Customer Support.

### 0x3591c08d Error in getting wildcarded data for %s (err = %s)

**Explanation:** An error occurred when obtaining the wildcard data for the entry from the Wildcard Database.

**Action:** Use the error text provided in the message to determine the cause of the problem and correct it. If the problem persists, contact IBM Customer Support.

### 0x3591c08e Error in creating Resource record for: %s (err = %s)

**Explanation:** An error occurred creating the policy record for the resource specified. Policy for the object is not being enforced because of the error.

**Action:** Use the error text provided in the message to determine the cause of the problem and correct it. If the problem persists, contact IBM Customer Support.

### 0x3591c08f Error in adding Holiday %s (err = %s)

**Explanation:** An error occurred in enforcing policy for the Holiday specified.

**Action:** Use the error text provided in the message to determine the cause of the problem and correct it. If the problem persists, contact IBM Customer Support.

### 0x3591c090 Error in deleting cached Holiday entries: %d - %s

**Explanation:** An error occurred while deleting the cached Holiday entry. Policy for the holiday object might still be enforced even though the entry has been deleted.

**Action:** Use the error text provided in the message to determine the cause of the problem and correct it. If the problem persists, contact IBM Customer Support.

### 0x3591c091 Error in getting the version number of the Object Signature Database: %d (%s)

**Explanation:** An error occurred attempting to obtain the version number of the object signature database. The updated policy will be resent to the object signature database even if there are potentially no new policy to be added to the object signature database.

**Action:** Use the error text provided in the message to determine the cause of the problem and correct it. If the problem persists, contact IBM Customer Support.

### 0x3591c092 Error in computing the list of policies which have changed

**Explanation:** An error occurred when determining the list of policies that have changed.

**Action:** Review the errors that occurred preceding this one and correct the problems found.

### 0x3591c094 Send to PDOS kernel failed

**Explanation:** An error occurred sending the updated policy to the PDOS kernel.

**Action:** Review the errors that occurred preceding this one and correct the problems encountered.

### 0x3591c095 Could not extract the Login and Password policy data

**Explanation:** The login and password policy data could not be extracted and written to the local configuration file. As a result, the original login and password policy continues to be enforced.

**Action:** Correct previous errors and restart the PDOS daemons. If the problem persists, contact IBM Customer Support.
Unable to add Sudo entry (%s) to Wildcard Database

Explanation: Unable to add the specified Sudo entry to the wildcard database.

Action: See the previous error messages from the wildcard engine to determine the cause of the error. Correct the problem. If the problem persists after a new replica with the corrected policy is sent down to the machine, contact IBM Customer Support.

Previous value of this Access-Restrictions attribute type (%s) exists. Random value picked.

Explanation: The Access-Restrictions attribute specified appears to have multiple values. The Access-Restrictions attribute only accepts a single value. The value being used for this attribute is unpredictable.

Action: Correct the Access-Restrictions attribute so that it only has a single value.

Unable to add entry (%s)

Explanation: An error occurred applying the policy for the object.

Action: See subsequent error messages to determine the cause of the error. Correct the problem. If the problem persists after a new replica with the corrected policy is sent down to the machine, contact IBM Customer Support.

Unable to remove entry (%s)

Explanation: An error occurred applying the policy for the object.

Action: See subsequent error messages to determine the cause of the error. Correct the problem. If the problem persists after a new replica with the corrected policy is sent down to the machine, contact IBM Customer Support.

Error in getting time since epoch: 0x%0x: %s

Explanation: An error occurred when obtaining the time since epoch from the PDOS kernel.

Action: Use the error status and error text provided in the message to correct the problem. Restart the PDOS daemons. If the problem persists, contact IBM Customer Support.

Error in notifying PDOS kernel about resources: 0x%x: %s

Explanation: An error occurred when notifying the PDOS kernel about the Protected Object Policies.

Action: Use the error status and error text provided in the message to correct the problem. Restart the PDOS daemons. If the problem persists, contact IBM Customer Support.

Error in setting policy version: 0x%x: %s

Explanation: An error occurred when setting the policy version in the PDOS kernel.

Action: Use the error status and error text provided in the message to correct the problem. Restart the PDOS daemons. If the problem persists, contact IBM Customer Support.

Error in committing Policy Epoch: 0x%x: %s

Explanation: An error occurred when committing the Policy Epoch to the PDOS kernel.

Action: Use the error status and error text provided in the message to correct the problem. Restart the PDOS daemons. If the problem persists, contact IBM Customer Support.

Send to Object Signature Database failed

Explanation: An error occurred when sending the policy to the Object Signature Database.

Action: See preceding error messages to determine the cause of the error. Correct the problem. If the problem persists, contact IBM Customer Support.

Error in getting Policy database version number

Explanation: Status code indicating that there was an error in extracting the policy database version number from the Policy Director Database.

Action: See preceding error messages to determine the cause of the error. Correct the problem. If the problem persists, contact IBM Customer Support.

Error in getting time since epoch

Explanation: Internal status code indicating that the PDOS Kernel Policy Cache Manager KPCMGR could not retrieve the error since epoch from the PDOS Kernel.

Action: Restart the daemons and report the error to IBM Customer Support.
0x3591c0a1 Error in setting policy version
Explanation: Internal status code indicating that the PDOS Kernel Policy Cache Manager (KPCMGR) could not set the policy version number in the PDOS Kernel.
Action: Restart the daemons and report the error to IBM Customer Support.

0x3591c0a2 Error in committing Policy Epoch
Explanation: Internal status code indicating that the PDOS Kernel Policy Manager (KPCMGR) could not commit the Policy Epoch to the PDOS Kernel.
Action: Restart the daemons and report the error to IBM Customer Support.

0x3591c0a3 Error in notifying PDOS kernel about resources
Explanation: Internal status code indicating that the PDOS Kernel Policy Manager (KPCMGR) could not notify the PDOS Kernel about some protected object policy.
Action: See preceding error messages to determine the cause of the error. Correct the problem. If the problem persists, contact IBM Customer Support.

0x3591c0a4 Unknown KPCMGR audit event
Explanation: Internal status code indicating an unknown PDOS Kernel Policy Cache Manager (KPCMGR) audit event.
Action: Restart the daemons and report the error to IBM Customer Support.

0x3591c100 PDOS kernel version number %lld
Explanation: Informational message providing the version number of the PDOS kernel.
Action: None

0x3591c101 Object signature database Version number %lld
Explanation: Informational message providing the version number of the Object signature database.
Action: None

0x3591c102 Policy database version number %lld
Explanation: Informational message providing the version number of the Policy database.
Action: None

0x3591c103 Time taken to update policy = (%d seconds)
Explanation: Informational message indicating the elapsed time, in seconds, that it took to update the policy.
Action: None

0x3591c180 Unable to audit a KPCMGR related event. Audit event ID 0x%x is unknown.
Explanation: An attempt was made to audit an event that is not recognized by the PDOS Kernel Policy Cache Manager (KPCMGR).
Action: Restart the daemons and report the error to IBM Customer Support.

0x3591c181 Error allocating audit record for event %s (0x%x). The error status is 0x%x: %s
Explanation: An error was encountered when allocating memory for the audit record.
Action: Check system resources to determine the cause of the problem. After correcting the problem, restart the PDOS daemons. If the problem persists, contact IBM Customer Support.

0x3591c182 Error auditing event %s (0x%x). The error status is 0x%x: %s.
Explanation: An error occurred during the processing of an audit event.
Action: Use the error status code and text to determine the cause of the error. Correct the problem and restart the PDOS daemons. If the problem persists, contact IBM Customer Support.

0x35947001 Tivoli Policy Director OS Security Account Management Utility
Explanation: Informational message
Action: None

0x35947002 Unknown argument %s
Explanation: An unknown command line option was specified.
Action: Review the syntax for the command and its argument. Correct the parameters and re-issue the command.
0x35947003 Usage:
Explanation: Usage string
Action: None

0x35947004 Help: %s -?/-h
Explanation: Usage string.
Action: None

0x35947005 Version information: %s -v
Explanation: Informational message
Action: None

0x35947006 Quiet (no output)
Explanation: Informational message
Action: None

0x35947007 Silent mode (rc only) %s -q
Explanation: Informational message
Action: None

0x35947008 User report: %s -r [-f] [-e|-d] [user] ...
Options: -f Full report of account -e Query only unlocked(enabled) accounts -d Query only locked(disabled) accounts user An account user login name Default is all records.
Explanation: Informational message
Action: None

0x35947009 Configuration settings:
Explanation: Informational message
Action: None

0x3594700a Configuration: %s -c onloff [-n clientserver]
Options: -c Parameter on or off specifies whether should be configured or unconfigured. -n Configure NIS for PDOS, parameter specifies whether a client or server is being configured.
Explanation: Options to configure the PDOS Login Activity Policy. The -n option configures an NIS server or client for PDOS.
Action: Configure PDOS Login Activity Policy.

0x3594700b Administration settings:
Explanation: Informational message
Action: None

0x3594700c Administration: %s -m <user> [<password change date>] | -p [<exception>] | -x <user>
Explanation: Informational message
Action: None

0x3594700d Account state for %s, id %d:
Explanation: Informational message
Action: None

0x3594700e Lock status: %s
Explanation: Informational message.
Action: None

0x3594700f Last successful login: %s
Explanation: Informational message.
Action: None

0x35947010 Login failures since locked: %d
Explanation: Informational message
Action: None

0x35947011 Current grace logins: %d
Explanation: Informational message
Action: None

0x35947012 Login failure data:
Explanation: Informational message
Action: None

0x35947013 Failure record %d:
Explanation: Informational message
Action: None
TTY name: %s
Explanation: Informational message
Action: None

rhost name: %s
Explanation: Informational message
Action: None

ruser name: %s
Explanation: Informational message
Action: None

Failing pid: %d (%s)
Explanation: Informational message
Action: None

Failure time: %s
Explanation: Informational message
Action: None

Options: -e Query only unlocked(enabled) accounts field One of %s, %s, %s, %s, %s, %s, or %s. newvalue For %s newvalue is true or false. For all others new value must be 0 or a positive integer.
Explanation: Informational message
Action: None

Lock user: %s -l <user1> <user2> ... user An account user login name
Explanation: Informational message
Action: None

Unlock user: %s -u [-z] <user1> <user2> ... user An account user login name. -z option zeros out all fields, resetting account (lock time, reason, failed logins, grace logins, etc.).
Explanation: Informational message
Action: None

Options: -m, -p, -x, -r, -c, -l and -u are mutually exclusive.
Explanation: Informational message
Action: None

User (uid)
Explanation: Informational message
Action: None

State
Explanation: Informational message
Action: None

Time Locked
Explanation: Informational message
Action: None

Reason
Explanation: Informational message
Action: None

Locked
Explanation: Informational message
Action: None

Unlocked
Explanation: Informational message
Action: None

Suspended
Explanation: Informational message
Action: None

You are not authorized to perform this action.
Explanation: The current user does not have sufficient permission to modify accounts.
Action: Contact the system administrator to correct the problem.
0x35947025 Your account was locked due to expiration of password.
Explanation: The password for this account has expired and the account has been locked.
Action: Contact the system administrator to correct the problem. In the future, the user password should be changed before the expiration date.

0x35947026 Your account was locked by an administrator.
Explanation: An administrator has locked the account.
Action: Contact the system administrator to have the account unlocked.

0x35947027 Your password has expired.
Explanation: The password for this account has expired. You must change your password.
Action: Change the user password.

0x35947028 PASSWORD EXPIRED - %d grace logins will be permitted before account is locked.
Explanation: The user password for this account has expired. The system administrator has allowed the specific number of grace logins to be permitted before the account is automatically locked.
Action: Change the user password before the number of grace logins is exceeded.

0x35947029 Unable to update passwd for %s. Password was recently changed.
Explanation: A request was made to change the password for this account within the period specified by the MinPasswordDays policy attribute. The password was not changed.
Action: No immediate action is required. Contact the system administrator if the password must be changed at this time.

0x3594702a Your account has been locked due to inactivity.
Explanation: An inactive account has been locked.
Action: Contact the system administrator to reactivate the account.

0x3594702b Your account has been suspended due to excessive login failures.
Explanation: An account has been suspended because of too many consecutive login failures.
Action: Contact the system administrator to reactivate the account.

0x3594702c User account %s has been locked.
Explanation: The account has been successfully disabled.
Action: None

0x3594702d User account %s has been unlocked.
Explanation: The account has been successfully enabled.
Action: None

0x3594702e Please see the system administrator
Explanation: Only the system administrator can perform the requested action.
Action: Contact the system administrator to have the action performed.

0x3594702f User %s does not exist.
Explanation: The specified user cannot be found on the local system.
Action: Ensure that the specified user is defined on the system.

0x35947030 Error opening user account database, code %d.
Explanation: The PDOS user database cannot be opened.
Action: Ensure that the database exists and has the proper permissions.

0x35947031 Error closing user account database, code %d.
Explanation: The PDOS user database cannot be closed.
Action: Ensure that the database exists and has the proper permissions.
Error locking user account database, code %d.

Explanation: The PDOS user database cannot be opened.

Action: Ensure that the database exists and has the proper permissions.

User %s not found in user account database.

Explanation: The user cannot be located in the PDOS user database.

Action: Ensure that the user exists on the local system, that the PDOS user database exists, and that the database has the proper permissions.

Error reading user account database, code %d.

Explanation: A record for a user could not be read from the PDOS user database.

Action: Ensure that the database exists and has the proper permissions.

Error writing user account database, code %d.

Explanation: A record for a user could not be written to the PDOS user database.

Action: Ensure that the database exists and has the proper permissions.

Error deleting record from user account database, code %d.

Explanation: The specified user record could not be deleted from the state database.

Action: Ensure that the correct user was specified. If the problem persists, contact IBM Customer Support.

Error iterating through the PDOS user account database, code %d.

Explanation: Unable to sequentially read user records from the user state database.

Action: Verify that the user state database exists, has the proper permissions, and its data is not corrupt.

Unable to read the login policy.

Explanation: The PDOS login policy cannot be read in.

Action: Ensure that the login policy file exists and has the proper permissions.

Unable to access login policy, using defaults.

Explanation: The PDOS policy database, lpm.conf, cannot be modified.

Action: Ensure that the database exists and has the correct permissions.

No user state database (%s) was found.

Explanation: The user state database specified could not be opened.

Action: Check that the specified file exists and can be read.

The user state database record had a bad version (%d).

Explanation: Version numbers are used to track changes in the record format, the version is unknown.

Action: Check that the database file is not corrupted.

No user state database record for %s was found.

Explanation: There is no record of the user logging in.

Action: Check that the database file is not corrupted.

No corresponding failure record was found.

Explanation: A successful login was attempting to remove a corresponding failure record, but no failure record was found.

Action: Check that the PDOS LPM authentication module is active.

Bad parameter passed to function.

Explanation: An invalid parameter was passed, most likely a NULL pointer.

Action: Contact IBM Customer Support.

Bad configuration value, %d, ignoring (use default).

Explanation: An invalid configuration value was specified. The default value will be used instead.

Action: Correct the Login Policy configuration values that are in error.
**0x35947040** Unable to communicate with daemon, status %d.

**Explanation:** The pdoslpm daemon is not responding to requests.

**Action:** Verify that the pdoslpm daemon is running. If not, restart it. If the problem persists, contact IBM Customer Support.

**0x35947041** Memory allocation error.

**Explanation:** A system error has occurred.

**Action:** Contact IBM Customer Support.

**0x35947042** Unknown system error.

**Explanation:** An unknown system error has occurred.

**Action:** Contact IBM Customer Support.

**0x35947043** The PDOS LPM module is disabled.

**Explanation:** The policy specifies that the LPM module is not active.

**Action:** Contact IBM Customer Support.

**0x35947044** Usage: %s {start|stop|help}

**Explanation:** Usage message

**Action:** None

**0x35947045** Starting PDOS LPM daemon

**Explanation:** The PDOS LPM daemon is starting.

**Action:** None

**0x35947046** Stopping PDOS LPM daemon

**Explanation:** The PDOS LPM daemon is stopping.

**Action:** None

**0x35947047** pdoslpm daemon failed to start, code %d.

**Explanation:** An unexpected error occurred starting the pdoslpm daemon. The daemon was not started.

**Action:** See the returned error code for the cause of the error. Correct the problem and restart the pdoslpm daemon. If the problem persists, contact IBM Customer Support.

**0x35947048** Error on socket() call, errno %d.

**Explanation:** An unexpected error occurred issuing the socket() system call.

**Action:** See the returned error code for the cause of the error. Correct the problem and retry the operation.

**0x35947049** Error on connect() call, errno %d.

**Explanation:** An unexpected error occurred issuing the connect() system call.

**Action:** See the returned error code for the cause of the error. Correct the problem and retry the operation.

**0x3594704a** Error on read() call, rc %d errno %d.

**Explanation:** An unexpected error occurred issuing the read() system call.

**Action:** See the returned error code for the cause of the error. Correct the problem and retry the operation.

**0x3594704b** Error on write() call, rc %d errno %d.

**Explanation:** An unexpected error occurred issuing the write() system call.

**Action:** See the returned error code for the cause of the error. Correct the problem and retry the operation.

**0x3594704c** Error in PDOS LPM daemon, invalid request code %d received.

**Explanation:** Internal coding error.

**Action:** Contact IBM Customer Support.

**0x3594704d** Error in PDOS LPM daemon, bad request format/not understood.

**Explanation:** Internal coding error.

**Action:** Contact IBM Customer Support.

**0x3594704f** Unable to determine the platform or PAM library.

**Explanation:** The pdoslpm process was unable to determine the operating system platform.

**Action:** This process only runs on Solaris or HP-UX systems.
0x35947050  Could not update the /etc/pam.conf file.
Explanation: An error occurred updating the /etc/pam.conf file. The file could be corrupt or inaccessible.
Action: Ensure that the file exists and has the proper permissions.

0x35947051  Could not unconfigure the /usr/lib/security/methods.cfg file.
Explanation: An unexpected error occurred unconfiguring the /usr/lib/security/methods.cfg file. The file could be corrupt or inaccessible.
Action: Ensure that the file exists and has the proper permissions.

0x35947052  Could not unconfigure the /etc/security/user file.
Explanation: An unexpected error occurred unconfiguring the /etc/security/user file. The file could be corrupt or inaccessible.
Action: Ensure that the file exists and has the proper permissions.

0x35947053  Could not configure the /etc/security/user file.
Explanation: An unexpected error occurred during the configuring of the /etc/security/user file. The file could be corrupt or inaccessible.
Action: Ensure that the file exists and has the proper permissions.

0x35947054  Could not configure the /usr/lib/security/methods.cfg file.
Explanation: An unexpected error occurred during the configuring of the /usr/lib/security/methods.cfg file. The file could be corrupt or inaccessible.
Action: Ensure that the file exists and has the proper permissions.

0x35947055  Could not overwrite the /etc/security/user file.
Explanation: An unexpected error occurred attempting to overwrite the existing /etc/security/user file. The file could be corrupt or inaccessible.
Action: Ensure that the file exists and has the proper permissions.

0x35947056  Successfully updated login policy files.
Explanation: Configuration was successful.
Action: None

0x35947058  Unable to truncate the policy db (lpm.conf).
Explanation: The PDOS policy database, lpm.conf, could not be truncated.
Action: Ensure that the database exists and has the proper permissions.

0x35947059  No exception for %s, use default policy.
Explanation: The object has no exception specified to the default PDOS LPM policy.
Action: None

0x3594705a  Policy for %s is:
Explanation: 
Action: None

0x3594705b  -m Set new password change date for specified user. Default is current time. Date is in 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). -p Display policy for a specified exception. Default is default policy. -x Delete specified user record from login activity db.
Explanation: Fields that can be specified with the admin option.
Action: None

0x3594705c  No password change date available for user %s.
Explanation: It was not possible to retrieve a password change date for the specified user.
Action: Check that the user has a password change date defined as part of their account information. On HP-UX systems, also check that the system is trusted.
0x3594705d  Password change date: %s
Explanation: The last time the password was changed.
Action: None

0x3594705e  <N/A>
Explanation: The date field has not been set.
Action: None

0x3594705f  (local)
Explanation: Indicates that the date was retrieved from the local state record.
Action: None

0x35947060  The date format %s is invalid, use: mmdhhmm[ccyy]
Explanation: The format used for the date is not valid.
Action: Specify the desired date in the correct format and retry the operation.

0x35947061  Maximum concurrent logins (%d) has been reached - login not allowed.
Explanation: The login was denied because the user has reached the limit for the maximum number of concurrent logins. No further logins are allowed until one of the current login sessions ends.
Action: Terminate one of the other logins to allow this specific login to succeed. To increase the maximum number of concurrent logins allowed for the user, contact the system administrator.

0x35947062  Concurrent logins(allowed): %d(%d)
Explanation: The user has reached the limit for the maximum number of concurrent logins, as specified by policy. No further logins are allowed until a current login session is ended.
Action: None

0x35947063  Error retrieving data from PAM.
Explanation: Unable to retrieve necessary data from PAM.
Action: Contact IBM Customer Support.

0x35947064  Error setting data in PAM.
Explanation: Unable to set necessary data in PAM.
Action: Contact IBM Customer Support.

0x35947065  The user is an unknown UNIX user.
Explanation: Unable to retrieve the required information about the user name.
Action: Check the user’s entry in the local system. If the problem persists, contact IBM Customer Support.

0x35947066  Error initializing LPM state.
Explanation: The pdoslpmd daemon was unable to open, lock, or read the user state database.
Action: Restart the pdoslpmd daemon. If the problem persists, contact IBM Customer Support.

0x35947067  Error on update of LPM state database.
Explanation: The pdoslpmd daemon was unable to write or delete a record in the user state database.
Action: Contact IBM Customer Support.

0x35947068  Error sending request to LPM daemon.
Explanation: On HP-UX systems, an unexpected error occurred sending a request to the pdoslpmd daemon.
Action: Restart the pdoslpmd daemon and report the problem to IBM Customer Support.

0x35947069  Error receiving response from LPM daemon.
Explanation: On HP-UX systems, an unexpected error occurred when receiving a response from the pdoslpmd daemon.
Action: Restart the pdoslpmd daemon and report the problem to IBM Customer Support.

0x3594706a  Error updating the pdosd.conf file.
Explanation: An unexpected error occurred updating the pdosd.conf file. The file could be corrupt or inaccessible.
Action: Ensure that the file exists and has the proper permissions.
Unable to find $YPDIR/Makefile, cannot configure NIS for PDOS.

**Explanation:** The YP Makefile was not found in the directory specified by the script variable YPDIR. NIS was not configured.

**Action:** Verify that the YP Makefile is located in the directory specified by the script variable YPDIR in lpmniscfg.sh.

Configuration of NIS for PDOS failed, unable to make a backup copy of Makefile in YPDIR.

**Explanation:** The configuration of NIS failed due to an error creating a backup copy of the Makefile.

**Action:** Verify that the directory where the Makefile is located has the proper access permissions.

No password change date information is available.

**Explanation:** A shadow password file with password change date information was not found.

**Action:** Password change date information cannot be made available from the NIS server.

Configuration of NIS for PDOS failed to complete, unknown Makefile format.

**Explanation:** The configuration of NIS did not complete because the YP Makefile was not in a recognizable format.

**Action:** If the YP Makefile has been significantly changed, configure NIS for use manually. Otherwise, determine why NIS configuration did not complete and correct the error.

Configuration of NIS for PDOS failed to complete, make failed.

**Explanation:** An unexpected error occurred when make was issued to build the NIS map.

**Action:** Invoke make manually to build the new NIS map. Determine why make did not complete and correct the error.

Unable to retrieve NIS domain name.

**Explanation:** An attempt to retrieve data from an NIS environment failed because no domain name was set.

**Action:** Check that the NIS client configuration is correct and verify that the proper domain name has been set.

Error attempting to bind to a server in the NIS domain.

**Explanation:** An unexpected error occurred attempting to bind to an NIS server using the yp_bind() system call.

**Action:** Verify that the NIS client configuration is correct and that the machine can bind to an NIS server. ypcat and ypmatch can be used for this validation.

Error retrieving data for user from the NIS server.

**Explanation:** An unexpected error occurred fetching user data from the NIS server using the yp_match() system call.

**Action:** Verify that the NIS client configuration and the NIS server map for PDOS are correct. ypcat and ypmatch can be used for this validation.

Error processing data from the NIS server, invalid format.

**Explanation:** Data for the user was fetched from the map on the NIS server, but the format was not recognized.

**Action:** Verify that the data format of the NIS map is in a valid format.

Error converting NIS password change date for user, unknown conversion factor.

**Explanation:** The data from the NIS map contains a conversion factor, such as secs, days, or weeks, that is not valid.

**Action:** Verify that the data format of the NIS map has valid format.

Error dynamically loading lnlpmext library.

**Explanation:** Dynamic load of shared library lnlpmext failed.

**Action:** Verify that lnlpmext is a valid shared library for the platform.

Required symbol in lnlpmext not found.

**Explanation:** A required symbol in the lnlpmext shared library was not found.

**Action:** Verify that lnlpmext is a valid shared library for the platform.
Password length does not satisfy policy requirements.

Explanation: The password specified does not contain enough characters and is not allowed by policy.

Action: The password being set must contain additional characters. Check the policy for the minimum allowed password length.

Password alpha count does not satisfy policy requirements.

Explanation: The password specified does not have enough alphabetic characters and is not allowed by policy.

Action: The password being set must have more alphabetic characters. Check the policy for the required number of alphabetic characters.

Password alphanumeric count does not satisfy policy requirements.

Explanation: The password specified does not have enough alphanumeric characters and is not allowed by policy.

Action: The password being set must have more alphanumeric characters. Check the policy for the required number of alphanumeric characters.

Password numeric count does not satisfy policy requirements.

Explanation: The password specified does not have enough numeric characters and is not allowed by policy.

Action: The password being set must have more numeric characters. Check the policy for the required number of numeric characters.

Password lowercase char count does not satisfy policy requirements.

Explanation: The password specified does not have enough lowercase alphabetic characters and is not allowed by policy.

Action: The password being set must have more lowercase alphabetic characters. Check the policy for the required number of lowercase alphabetic characters.

Password uppercase char count does not satisfy policy requirements.

Explanation: The password specified does not have enough uppercase alphabetic characters and is not allowed by policy.

Action: The password being set must have more uppercase alphabetic characters. Check the policy for the required number of uppercase alphabetic characters.

Password special character count does not satisfy policy requirements.

Explanation: The password specified does not have enough special characters and is not allowed by policy.

Action: The password being set must have more special characters. Check the policy for the required number of special characters.

Password has too many repeated characters to satisfy policy requirements.

Explanation: The password specified has too many repeated characters and is not allowed by policy.

Action: The password being set must have a fewer number of repeated characters. Check the policy for the maximum number of required characters allowed.

New password is contained in or contains the user name.

Explanation: The new password is not allowed by policy because it either contains or is contained in the user’s name.

Action: The password being set must not be contained in or contain the user name.

New password is contained in or contains the old password.

Explanation: The new password is not allowed by policy because it either contains or is contained in the previous password.

Action: The password being set must not be contained in or contain the previous password.

New password is not allowed because it is a recently used password.

Explanation: The new password is not allowed by policy because it has been used recently.

Action: Specify a new password that has not been used recently. Check the policy to verify the password history.

A database record appears to be corrupted.

Explanation: Data fields in the database record are inconsistent, indicating that the record is corrupt.

Action: The record may need to be deleted. The administrator can also attempt to recover the database.
The total size of the user activity database record is too large.

**Explanation:** Limitations of the underlying database do not allow a record of this size.

**Action:** Review the current policy. The number of maximum failed logins and maximum concurrent logins affect the size of the record.

---

Received invalid action.

**Explanation:** An internal service specified an invalid action to an internal function.

**Action:** Report the error to IBM Customer Support.

---

Invalid action 0x%x specified in %s message.

**Explanation:** An internal service specified an invalid action to an internal function.

**Action:** Report the error to IBM Customer Support.

---

Invalid value in %s message. The %s field value should be 0 but it is %d.

**Explanation:** An internal service specified an invalid value to an internal function.

**Action:** Report the error to IBM Customer Support.

---

A %s message has inconsistent data: nwflags value 0x%x.

**Explanation:** An internal service specified an invalid value to an internal function.

**Action:** Report the error to IBM Customer Support.

---

A %s message has inconsistent data. Terminal group information is missing for local terminal name %s. The local_term_extdata_len is %d.

**Explanation:** An internal service specified an invalid value to an internal function.

**Action:** Report the error to IBM Customer Support.

---

The Authorization Service tried to generate an unexpected audit event.

**Explanation:** An internal service specified an invalid audit event to an internal function.

**Action:** Report the error to IBM Customer Support.

---

Unable to audit an Authorization related event. Audit event identifier 0x%x is unknown.

**Explanation:** An internal service specified an invalid audit event to an internal function.

**Action:** Report the error to IBM Customer Support.

---

Error allocating audit record for event %s (0x%x). The error status is 0x%x: %s

**Explanation:** An error occurred when allocating space for an audit record.

**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

---

Error auditing event %s (0x%x). The error status is 0x%x: %s.

**Explanation:** An error occurred when the PDOS Authorization Service tried to add an audit event to the audit queue.

**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

---

Invalid permitted value returned from AZN API.

**Explanation:** An internal service received an error when it called the Policy Director authorization service.

**Action:** Contact IBM Customer Support.

---

The AZN API did not return a status of AZN_C_COMPLETE.

**Explanation:** An internal service received an error when it called the Policy Director authorization service.

**Action:** Contact IBM Customer Support.

---

Failed to process Permission Info attributes for a protected object.

**Explanation:** An internal service received an error when it called the Policy Director authorization service.

**Action:** Contact IBM Customer Support.
0x35967404 The Credential Service returned NULL credentials.

Explanation: The PDOS Credential Service returned NULL credentials to the PDOS Authorization Service.

Action: Examine the log file /var/pdos/log/pdosd.log to determine if the PDOS Credential Service is experiencing errors and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

0x35967480 Failed to get credentials for user ID %d.

Error status is 0x%x: %s.

Explanation: An error occurred when the PDOSD daemon attempted to get credentials for a user while processing an authorization request.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35967481 Unable to map user ID %lld to a user name: 0x%x: %s

Explanation: While processing a surrogate operation request, the PDOS Authorization Service was unable to map the target user ID to a user name.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35967482 Unable to map group ID %lld to a group name: 0x%x: %s

Explanation: While processing a surrogate operation request, the PDOS Authorization Service was unable to map the target group ID to a group name.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35967483 Operation %s authorized on TCB file %s.

Explanation: An operation was authorized on a Trusted Computing Base (TCB) file which could result in changing the file signature.

Action: No immediate action is required. However, if the file signature does change, the file will be marked untrusted in the Object Signature Database.

0x35967484 Error processing Permission Info attributes for protected object %s. The azn_attrlist_get_names() API failed. Error status is 0x%x: %s.

Explanation: An internal service received an error when it called the Policy Director authorization service.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35967485 AZN attribute %s has %d values, only the first one is valid. The protected object name is %s.

Explanation: The information returned from a call to the Policy Director authorization service for the specified attribute included more values than expected. Only the first attribute is used.

Action: No immediate action is required. However, if PDOS authorization policy is not being enforced correctly, contact IBM Customer Support.

0x35967486 AZN attribute %s has no values. The protected object name is %s.

Explanation: The information returned from a call to the Policy Director authorization service did not contain a value for the specified attribute.

Action: No immediate action is required. However, if PDOS authorization policy is not being enforced correctly, contact IBM Customer Support.

0x35967487 Failed to process AZN attribute %s for protected object %s. Error status is 0x%x: %s.

Explanation: An internal service was unable to process the information returned from a call to the Policy Director authorization service for the specified attribute.

Action: No immediate action is required. However, if PDOS authorization policy is not being enforced correctly, contact IBM Customer Support.

0x35967488 Failed to get group information for user ID %lld when processing %s attribute value for protected object %s. Error status is 0x%x: %s.

Explanation: An internal service was unable to obtain the group list from the user’s credential while processing information returned from a call to the Policy Director authorization server for the attribute associated with the protected object name.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.
Invalid permitted value %d returned from AZN API when evaluating policy. The protected object name is %s. The operation is %s. The user ID is %ld.

Explanation: An internal service received an error when it called the Policy Director authorization service.
Action: Contact IBM Customer Support.

AZN API failure occurred when evaluating policy. The protected object name is %s. The operation is %s. The user ID is %ld.

Explanation: An internal service received an error when it called the Policy Director authorization service.
Action: Examine the log file /var/pdos/log/pdosd.log to determine if the Policy Director authorization service is experiencing errors and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

Audit level %s was specified for protected object %s. It is not a supported PDOS audit level and will have no effect.

Explanation: An unrecognized or unsupported audit level was returned from a call to the Policy Director authorization service for the specified protected object.
Action: Check the authorization policy associated with the specified protected object. Verify that the audit level attribute value of the Policy Object Policy associated with the protected object is supported by PDOS.

Failed to determine state of TCB file %s. Error status is 0x%x: %s

Explanation: The PDOS Authorization Service was unable to determine the trust state of the specified Trusted Computing Base (TCB) file during an authorization request to execute the file.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Error occurred in %s wildcard matching for %d.%d.%d.%d. Error status is 0x%x: %s

Explanation: An internal service failed to determine if the specified IP address matched any wildcard authorization policy for Login location remote terminal resources.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Error occurred in %s wildcard matching for %u.%u.%u.%u:%u. Error status is 0x%x: %s

Explanation: An internal service failed to determine if the specified IP address matched any wildcard authorization policy for Login location remote terminal resources.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Error occurred in %s wildcard matching for %u:%u, %u.%u.%u.%u. Error status is 0x%x: %s

Explanation: An internal service failed to determine if the specified network protocol and port number matched any wildcard authorization policy for NetIncoming resources.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Error occurred in %s wildcard matching for command alias %s. The number of arguments is %d. Error status is 0x%x: %s

Explanation: An internal service failed to determine if the specified pdossudo command alias matched any authorization policy for Sudo resources.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Failed to determine if today is a login holiday while evaluating policy. The protected object name is %s. The user ID is %d. Error status is 0x%x: %s.

Explanation: An internal service failed to determine if today’s date matched any authorization policy for Login Holiday resources.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.
0x35972080  Read of %d bytes on %s failed: %d
Explanation: An internal service failed to write the requested amount of data from a message channel. The last number is the error number returned from the read system call.
Action: Use the returned error code to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35972081  Write of %d bytes on %s failed: %d
Explanation: An internal service failed to write the requested amount of data from a message channel. The last number is the error number returned from the write system call.
Action: Use the returned error code to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35972082  UMSG response name length on channel %s is bad: %d
Explanation: An internal message contains an invalid length for a response message channel name. An authorization or control message could not be processed successfully. The last number is the invalid value.
Action: If the problem persists, contact IBM Customer Support.

0x35972083  UMSG Data length on channel %s is bad: %d
Explanation: An internal message contained an invalid data length value for a response message. An authorization or control message could not be processed successfully. The last number is the invalid value.
Action: If the problem persists, contact IBM Customer Support.

0x35972085  UMSG received message with 0 data length on channel %s
Explanation: An internal service received a response message with no data from an internal message channel. An authorization or control message response could not be processed successfully.
Action: If the problem persists, contact IBM Customer Support.

0x35972086  UMSG unable to create FIFO %s: %d: %s
Explanation: An internal service failed to create the specified FIFO.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35972087  UMSG unable to open FIFO %s: %d: %s
Explanation: An internal service failed to open the specified FIFO.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35972100  Invalid device
Explanation: An internal service was passed an invalid message channel identifier.
Action: If the problem persists, contact IBM Customer Support.

0x35972101  Device creation failed
Explanation: An internal service was unable to create a PDOS message channel.
Action: If the problem persists, contact IBM Customer Support.

0x35972102  Device open failed
Explanation: An internal service was unable to open a PDOS message channel.
Action: If the problem persists, contact IBM Customer Support.

0x35972103  Device does not exist
Explanation: An internal service was passed a message channel identifier for a PDOS message channel that does not exist.
Action: If the problem persists, contact IBM Customer Support.

0x35972104  No listener on device
Explanation: Internal status code.
Action: None
0x35972105 Device read failed
Explanation: An internal service was unable to read data from a PDOS message channel.
Action: If the problem persists, contact IBM Customer Support.

0x35972106 Device write failed
Explanation: An internal service was unable to write data to a PDOS message channel.
Action: If the problem persists, contact IBM Customer Support.

0x35972107 Device already opened
Explanation: An attempt was made to open an internal message channel that was already open.
Action: None

0x35972108 Device is closed
Explanation: An attempt was made to close an internal message channel that was already closed.
Action: None

0x35972109 Device is opening
Explanation: An internal message channel is in the process of being opened.
Action: None

0x3597210a Device is closing
Explanation: An internal message channel is in the process of being closed.
Action: None

0x3597210b Device in invalid state
Explanation: An internal message channel is not in the proper state.
Action: If the problem persists, contact IBM Customer Support.

0x3597210c Device undefined
Explanation: Internal status code.
Action: None

0x3597210d Bad file descriptor
Explanation: Internal status code.
Action: None

0x3597210e Channel is invalid
Explanation: An internal service attempted to use an invalid internal message channel.
Action: If the problem persists, contact IBM Customer Support.

0x3597210f Channel interrupted
Explanation: A system call was interrupted while an internal service was processing data on a PDOS message channel.
Action: If the problem persists, contact IBM Customer Support.

0x35972110 Invalid command
Explanation: Internal status code.
Action: Contact IBM Customer Support.

0x35972111 Received partial message
Explanation: The requested amount of data was not available on a PDOS message channel, only partial message read.
Action: If the problem persists, contact IBM Customer Support.

0x35972112 Bad message length
Explanation: An internal message header contains an invalid value for the message data length field.
Action: If the problem persists, contact IBM Customer Support.

0x35972113 No more data in message
Explanation: Internal status indicating there is no more data to be read from a PDOS message channel.
Action: None

0x35972114 Bad buffer
Explanation: Internal status indicating a bad buffer was passed during the processing of a message.
Action: If the problem persists, contact IBM Customer Support.
0x35972115  Bad length
Explanation: Internal status indicating a request was made to process an invalid amount of message data.
Action: If the problem persists, contact IBM Customer Support.

0x35972116  Bad transaction ID
Explanation: Internal status indicating that the PDOS kernel timed out waiting for a response for an authorization request from the PDOSD daemon.
Action: Additional diagnostic information included with this message includes the type of authorization request being performed and a set of message statistics showing where processing time was spent. If the problem persists, contact IBM Customer Support.

0x35972117  Message too big
Explanation: Internal status indicating the errno E2BIG was received during the processing of a message.
Action: If the problem persists, contact IBM Customer Support.

0x35972118  Not initialized
Explanation: Internal status indicating an uninitialized message was passed to an internal service.
Action: If the problem persists, contact IBM Customer Support.

0x35972119  Message in bad state
Explanation: Internal status indicating a message was not in the correct state when passed to an internal service.
Action: If the problem persists, contact IBM Customer Support.

0x3597211a  Message in init state
Explanation: Internal status indicating a message was not in the correct state when passed to an internal service.
Action: If the problem persists, contact IBM Customer Support.

0x3597211b  Message in processing state
Explanation: Internal status indicating a message was not in the correct state when passed to an internal service.
Action: If the problem persists, contact IBM Customer Support.

0x3597211c  Message in response state
Explanation: Internal status indicating a message was not in the correct state when passed to an internal service.
Action: If the problem persists, contact IBM Customer Support.

0x3597211d  Message in sent state
Explanation: Internal status indicating a message was not in the correct state when passed to an internal service.
Action: If the problem persists, contact IBM Customer Support.

0x3597211e  Message in invalid state
Explanation: Internal status indicating a message was not in the correct state when passed to an internal service.
Action: If the problem persists, contact IBM Customer Support.

0x3597211f  Undefined error
Explanation: Internal status indicating an unexpected error occurred while an internal service was processing a message.
Action: If the problem persists, contact IBM Customer Support.

0x35972120  Bad response pipe name length
Explanation: Internal status indicating a message contains an invalid length for a response message channel name.
Action: If the problem persists, contact IBM Customer Support.

0x35972121  Bad response pipe name
Explanation: Internal status indicating a message does not contain a valid response message channel name.
Action: If the problem persists, contact IBM Customer Support.

0x35972122  Bad data length
Explanation: Internal status indicating a message contains an invalid data length value for a response message.
Action: If the problem persists, contact IBM Customer Support.
0x35972123  Access denied

Explanation: Internal status indicating access was not permitted to an internal message channel.

Action: The PDOS utilities use internal message channels to communicate with the PDOS daemons. This status code indicates that the person running a PDOS utility does not have access to the /var/pdos/umsg directory or an underlying file in this directory. If this person should have access, then check the PDOS policy and the native unix permissions for this directory. If the problem persists, contact IBM Customer Support.

0x35972124  umsg directory not present

Explanation: Internal status indicating that the /var/pdos/umsg directory does not exist.

Action: If the /var/pdos/umsg directory does not exist on the system check if there were problems during the installation of PDOS. If the problem persists, contact IBM Customer Support.

0x35972125  The mktemp() routine was unable to create a temporary file name.

Explanation: An internal service failed to create a temporary file name needed to process a response message.

Action: If the problem persists, contact IBM Customer Support.

0x35972280  msg_chanRecvMsg() failed: %p: 0x%x: %s

Explanation: An internal service was unable to receive a message from a PDOS message channel.

Action: Use the returned error status to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35972300  Invalid message class identifier.

Explanation: Internal status indicating a PDOS message handler routine received a message with an unknown class identifier.

Action: If the problem persists, contact IBM Customer Support.

0x35972301  Incorrect message class version number

Explanation: Internal status indicating a PDOS message processing routine received a message with an incorrect class version number.

Action: If the problem persists, contact IBM Customer Support.

0x35972302  Incorrect message identifier version number

Explanation: Internal status indicating a PDOS message processing routine received a message with an incorrect message identifier version number.

Action: If the problem persists, contact IBM Customer Support.

0x35972303  Invalid message identifier.

Explanation: Internal status indicating a PDOS message processing routine received a message with an invalid message identifier.

Action: If the problem persists, contact IBM Customer Support.

0x35972304  Received message with inconsistent data.

Explanation: Internal status indicating a PDOS message processing routine received a message with inconsistent data.

Action: If the problem persists, contact IBM Customer Support.

0x35972305  Partial read of message occurred.

Explanation: Internal status indicating a PDOS message processing routine was unable to read the complete message.

Action: If the problem persists, contact IBM Customer Support.

0x35972306  Partial write of message occurred.

Explanation: Internal status indicating a PDOS message processing routine was unable to write the complete message.

Action: If the problem persists, contact IBM Customer Support.

0x35972307  Character string is not the expected length.

Explanation: Internal status indicating a character field value read from a message was not the expected length.

Action: If the problem persists, contact IBM Customer Support.

0x35972308  Received invalid %s message. Expected message class %u, received %u.

Explanation: An internal message processing routine received a message with an unknown class identifier. The expected message class is shown along with the received message class.

Action: If the problem persists, contact IBM Customer Support.
0x35972381  Received invalid message. Message identifier %u is not valid for %s message class.

Explanation: An internal message processing routine received a message with an unknown message identifier. The unknown identifier and the message class are shown.

Action: If the problem persists, contact IBM Customer Support.

0x35972382  %s message has wrong class version number %u, expecting version %u.

Explanation: An internal message processing routine received a message with an incorrect class version number. The message class name, the incorrect number and the expected number are shown.

Action: If the problem persists, contact IBM Customer Support.

0x35972383  %s message has wrong version number %u, expecting version %u.

Explanation: An internal message processing routine received a message with an incorrect message version number. The type of message, the incorrect number and the expected number are shown.

Action: If the problem persists, contact IBM Customer Support.

0x35972384  Failed to read %s message header. Read %u instead of %u bytes. Error status is 0x%x: %s.

Explanation: An internal message processing routine failed to read a message header from a message channel.

Action: Use the returned error status to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35972385  Failed to read %s message. Read %u instead of %u bytes. Error status is 0x%x: %s.

Explanation: An internal message processing routine failed to read the expected amount of data from a message channel.

Action: Use the returned error status to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35972386  Failed to write %s message. Wrote %u instead of %u bytes. Error status is 0x%x: %s.

Explanation: An internal message processing routine failed to write the expected amount of data from a message channel.

Action: Use the returned error status to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35972387  Unable to start %s message. Error status is 0x%x: %s.

Explanation: An internal service was unable to start a response message.

Action: Use the returned error status to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35972388  Unable to send %s message. Error status is 0x%x: %s.

Explanation: An internal service was unable to send a response message.

Action: Use the returned error status to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35972389  Unable to send %s message response. Error status is 0x%x: %s. Message statistics: queue len %d, queued time %d secs, credential acquisition time %d secs, processing time %d secs.

Explanation: An internal service was unable to send a response message to an authorization request.

Action: Use the returned error status to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x3597238a  AZN response had bad header.

Explanation: Internal status indicating a PDOS command received an invalid response from an authorization request.

Action: If the problem persists, contact IBM Customer Support.

0x3597238b  AZN response had bad header.

Explanation: Internal status indicating a PDOS command received an invalid response from an authorization request.

Action: If the problem persists, contact IBM Customer Support.

0x3597238c  Received bad AZN result.

Explanation: Internal status indicating a PDOS command received an invalid result from an authorization request.

Action: If the problem persists, contact IBM Customer Support.
0x35972580  Received AZN response header %u.%u.%u.%u expecting %u.%u.%u.%u.

**Explanation:** A PDOS command received an invalid response from the PDOSD daemon for an authorization request.

**Action:** If the problem persists, contact IBM Customer Support.

0x35972581  Received bad AZN result %x

**Explanation:** A PDOS command received an invalid result from the PDOSD daemon for an authorization request.

**Action:** If the problem persists, contact IBM Customer Support.

0x35a50002  Error opening an audit channel to communicate with the audit daemon. Status: 0x%x

**Explanation:** An internal service encountered an error initializing the audit subsystem.

**Action:** Use the returned error code to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a50003  An open is currently in progress on the device.

**Explanation:** An internal service attempted to open a message channel that is already in the process of being opened.

**Action:** None

0x35a50009  Device is already closed.

**Explanation:** An internal service attempted to close a message channel that is already closed.

**Action:** None

0x35a5000a  Device is in an invalid state, failure to open.

**Explanation:** An internal service attempted to close a message channel that was not open.

**Action:** If the problem persists, contact IBM Customer Support.

0x35a5000b  The device specified is not a valid device.

**Explanation:** An internal service attempted to use an invalid internal message channel.

**Action:** If the problem persists, contact IBM Customer Support.

0x35a5000c  The error code returned is not in the known error space

**Explanation:** An internal service encountered an unexpected error when closing a message channel.

**Action:** If the problem persists, contact IBM Customer Support.

0x35a5000d  Error getting the lock to the worker queue.

**Return Code:** 0x%x

**Explanation:** An unexpected error occurred when an internal service was stopping the audit subsystem.

**Action:** If the problem persists, contact IBM Customer Support.

0x35a50010  The message handle passing in is bad.

**Explanation:** An unexpected error occurred when an internal audit service attempted to send an audit record to the PDOSAUDITD daemon.

**Action:** If the problem persists, contact IBM Customer Support.

0x35a50011  A null buffer pointer was passed in.

**Explanation:** An unexpected error occurred when an internal audit service attempted to send an audit record to the PDOSAUDITD daemon.

**Action:** If the problem persists, contact IBM Customer Support.

0x35a50012  A non-positive length was passed in for copy length.

**Explanation:** An unexpected error occurred when an internal audit service attempted to send an audit record to the PDOSAUDITD daemon.

**Action:** If the problem persists, contact IBM Customer Support.

0x35a50013  The message handle is Null.

**Explanation:** An unexpected error occurred when an internal audit service attempted to send an audit record to the PDOSAUDITD daemon.

**Action:** If the problem persists, contact IBM Customer Support.
The message buffer has been filled.

**Explanation:** An unexpected error occurred when an internal audit service attempted to send an audit record to the PDOSAUDITD daemon.

**Action:** If the problem persists, contact IBM Customer Support.

**Message handle is in an unexpected state.**

**Status:** 0x%x

**Explanation:** An unexpected error occurred when an internal audit service attempted to send an audit record to the PDOSAUDITD daemon.

**Action:** If the problem persists, contact IBM Customer Support.

The record was only partially sent.

**Explanation:** An unexpected error occurred when an internal audit service attempted to send an audit record to the PDOSAUDITD daemon.

**Action:** If the problem persists, contact IBM Customer Support.

The value specified as the condition is invalid.

**Return Code:** 0x%x

**Explanation:** An unexpected error occurred when an internal audit service was stopping the audit subsystem.

**Action:** If the problem persists, contact IBM Customer Support.

The parameter value is invalid, unlock of thread failed.

**Return Code:** 0x%x

**Explanation:** An unexpected error occurred when an internal audit service was stopping the audit subsystem.

**Action:** If the problem persists, contact IBM Customer Support.

The specified thread is invalid or a deadlock is detected.

**Return Code:** 0x%x

**Explanation:** An unexpected error occurred when an internal audit service was stopping the audit subsystem.

**Action:** If the problem persists, contact IBM Customer Support.

A kosseal_register call was made to acquire privileged access.

**Explanation:** The audit event generated when a PDOS daemon has made a request for privileged access from the PDOS kernel extension.

**Action:** If the Audit Outcome field indicates success then no action is required. Otherwise, the PDOS daemon was unable to acquire the necessary privileges. Use the error shown in the Audit Fail Status field to diagnose the problem. Check the log in /var/pdos/log/pdosd.log file. If the problem persists, contact IBM Customer Support.
files in the /var/pdos/log director for additional errors. If the problem persists, contact IBM Customer Support.

**0x35a50022  Policy version set in the Kernel Policy Cache.**

**Explanation:** The audit event generated when the PDOSD daemon has processed a policy update and has notified the PDOS kernel extension of the current policy version number.

**Action:** None

**0x35a50023  Kernel Policy Cache epoch updated.**

**Explanation:** The audit event generated when the PDOS kernel extension has generated a new policy epoch value. This is an indication that a policy update is being processed by the PDOSD daemon.

**Action:** None

**0x35a50024  A file has been added to the TCB database**

**Explanation:** The audit event generated when the PDOSD daemon has processed a policy update that contains a new resource in the Trusted Computing Base (TCB). The file has been added to the PDOS object signature database.

**Action:** None

**0x35a50025  A file has been removed from the TCB database**

**Explanation:** The audit event generated when the PDOSD daemon has processed a policy update that has removed a resource from the Trusted Computing Base (TCB). The file has been removed from the PDOS object signature database.

**Action:** None

**0x35a50026  A file has been marked untrusted**

**Explanation:** The audit event generated when the state of a file in the object signature database has changed from trusted to untrusted. This change occurred because either an administrator explicitly changed the state to untrusted or the file’s signature has changed. If this is an executable file, execution is denied until a PDOS administrator changes the state back to trusted.

**Action:** If the Changed Data Attributes Flag field value is signature fail, the state was changed because the file’s current signature does not match the information stored in the object signature database. Use the additional information provided in the audit record to determine the name of the file that changed. Verify that the file has not been compromised. If the change in the file’s signature was the result of an expected event, an administrator can change the state of the file back to trusted by using the pdosobjsig utility.

**0x35a50027  A file has been marked trusted**

**Explanation:** The audit event generated when a PDOS administrator changes a file’s state in the object signature database to trusted.

**Action:** None

**0x35a50028  A PDOS process has started**

**Explanation:** The audit event generated when a PDOS daemon starts.

**Action:** If the Audit Outcome field indicates success then no action is required. Otherwise, an error occurred which prevented the PDOS daemon from starting. Use the error shown in the Audit Fail Status field to diagnose the problem. Check the log file associated with the daemon in the /var/pdos/log directory for additional errors. If the problem persists, contact IBM Customer Support.

**0x35a50029  A PDOS process has stopped**

**Explanation:** The audit event generated when a PDOS daemon stops.

**Action:** If the Audit Outcome field indicates success then no action is required. Otherwise, an error occurred which prevented the PDOS daemon from stopping successfully. Use the error shown in the Audit Fail Status field to diagnose the problem. Check the log file associated with the daemon in the /var/pdos/log directory for additional errors. If the problem persists, contact IBM Customer Support.

**0x35a5002a  A PDOS process has been adopted into the watchdog set**

**Explanation:** The audit event generated when a PDOS daemon becomes part of the set of daemons watched by the PDOS watchdog service.

**Action:** If the Audit Outcome field indicates success then no action is required. Otherwise, an error occurred which prevented the daemon from being added to the watchdog service list. Use the error shown in the Audit Fail Status field to diagnose the problem. Check the log file associated with the daemon in the /var/pdos/log directory for additional errors. If the problem persists, contact IBM Customer Support.

**0x35a5002b  An authorization decision API failure has occurred.**

**Explanation:** The audit event generated when an internal service receives an error from the Policy Director azn_decision_access_allowed_ext() API while making an authorization decision. PDOS policy was not successfully enforced.

**Action:** Use the additional information in the audit record to determine the cause of the error. If the problem continues to exist, contact IBM Customer Support.
0x35a5002c  An authorization decision was made.
Explanation:  The audit event generated when an internal service makes an authorization decision for an access request to a protected resource.
Action:  If the Audit Outcome field indicates success then the decision was made by a successful evaluation of PDOS policy and no action is required. Otherwise, PDOS policy was not successfully evaluated due to an error condition. Use the error shown in the Audit Fail Status field to diagnose the problem. Check the /var/pdos/log/pdosd.log file for additional errors. If the problem persists, contact IBM Customer Support.

0x35a5002d  Access granted to a file that is marked untrusted in the TCB database.
Explanation:  The audit event generated when an internal service makes an authorization decision allowing access to a file whose current state in the object signature database is untrusted.
Action:  Check the file’s state in the object signature database using the pdosobjsig command. Use the information provided to determine if the file has been compromised and take appropriate action.

0x35a5002e  Policy not applied for an invalid protected object name.
Explanation:  The audit event generated when the PDOSD daemon detects invalid policy when processing a policy update.
Action:  Use the information in the audit record shows to determine what policy is invalid. Use the normal method of updating policy to correct the invalid policy.

0x35a5002f  Policy applied for a protected object name.
Explanation:  The audit event generated when the PDOSD daemon successfully applies policy for a protected object name when processing a policy update.
Action:  None

0x35a50030  Credential acquired.
Explanation:  The audit event generated when the PDOSD daemon attempts to acquire a credential from the Policy Director User Registry.
Action:  If the Audit Outcome field indicates success the credential was successfully acquired and no action is required. Otherwise, an error occurred retrieving the credential. Use the error shown in the Audit Fail Status field to diagnose the problem. Check the /var/pdos/log/pdosd.log file for additional errors. Check that the Policy Director user registry server is functioning properly. If the problem persists, contact IBM Customer Support.

0x35a50031  Policy Director user registry is unavailable (isolation mode).
Explanation:  The audit event generated when the PDOS Credential Service is unable to communicate with the Policy Director user registry. PDOS continues to operate but is unable to retrieve any new credentials until connectivity is once again established.
Action:  Verify that network connectivity exists to the Policy Director user registry and correct any communication problems. Check that the user registry server is in a valid state and correct any errors.

0x35a50032  Policy Director user registry is now available.
Explanation:  The audit event generated when communication is re-established between the PDOS Credential Service and the Policy Director user registry.
Action:  None

0x35a50033  A login related authorization decision was made.
Explanation:  The audit event generated when an internal service makes an authorization decision for an access request to a Login related protected resource.
Action:  If the Audit Outcome field indicates success then the decision was made by a successful evaluation of PDOS policy and no action is required. Otherwise, the PDOS policy was not successfully evaluated due to an error condition. Use the error shown in the Audit Fail Status field to diagnose the problem. Check the /var/pdos/log/pdosd.log file for additional errors. If the problem persists, contact IBM Customer Support.

0x35a50034  User account was disabled (locked), preventing future logins.
Explanation:  The audit event generated when a user account is locked due to the enforcement of PDOS Login Activity Policy or administrative action.
Action:  The user associated with the account in the audit record is prevented from future logins until an administrator unlocks the account using the pdoslpadm utility.

0x35a50035  User account was disabled (suspended), preventing future logins.
Explanation:  The audit event generated when a user account is suspended due to the enforcement of PDOS Login Activity Policy. This can occur if the number of failed login attempts reaches the limit set by Login-MaxFailedLogins within the time interval specified by Login-LoginMinutes.
Action:  The account is suspended for the time interval specified by Login-LockMinutes. The account can be enabled at any time by a PDOS administrator using the pdoslpadm utility.
<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Explanation</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x35a50036</td>
<td>User account was enabled for login.</td>
<td>The audit event generated when a user account is re-enabled for login.</td>
<td>None</td>
</tr>
<tr>
<td>0x35a50037</td>
<td>The password change time was modified by an administrator.</td>
<td>The audit event generated when a PDOS administrator executes the pdosladm command and changes the local password change time for a user account.</td>
<td>None</td>
</tr>
<tr>
<td>0x35a50038</td>
<td>Logout occurred.</td>
<td>The audit event generated when a user logs off.</td>
<td>None</td>
</tr>
<tr>
<td>0x35a50039</td>
<td>TRACE Exec program</td>
<td>The audit event generated for audit level trace_exec.</td>
<td>None</td>
</tr>
<tr>
<td>0x35a5003a</td>
<td>TRACE File access</td>
<td>The audit event generated for audit level trace_file.</td>
<td>None</td>
</tr>
<tr>
<td>0x35a5003b</td>
<td>Password change occurred.</td>
<td>The audit event generated when a user’s password is changed.</td>
<td>None</td>
</tr>
<tr>
<td>0x35a53002</td>
<td>PDOSD’s stash file is truncated</td>
<td>An error occurred while reading the stash file indicating that the file is incomplete. Examine additional messages to find the name of the incomplete stash file.</td>
<td>Use the pdosrstr command to restore configuration files that were backed up using the pdosbkup command.</td>
</tr>
<tr>
<td>0x35a53003</td>
<td>PDOSD’s stash file is inaccessible</td>
<td>An error occurred while opening the stash file.</td>
<td>Examine additional messages to determine the cause of the failure. Correct the cause of the failure, then restart the process.</td>
</tr>
</tbody>
</table>
| 0x35a53080  | Usage: pdosd [-fhlvV?] [-t trace-string] -f run daemon in foreground -l list protected objects and terminate -v display verbose messages -V display version information and terminate 

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Explanation</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x35a53081</td>
<td>Authorization API failure: [%08x:%08x]</td>
<td>An internal service received an error when it called the Policy Director authorization service.</td>
<td>Contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35a53082</td>
<td>Authorization API failure: [%08x:%08x] %s</td>
<td>An internal service received an error when it called the Policy Director authorization service.</td>
<td>Use the returned error codes and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35a53083</td>
<td>Unhandled AZN status: [%08x:%08x]</td>
<td>An internal service received an error when it called the Policy Director authorization service.</td>
<td>Contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35a53084</td>
<td>Unhandled Authorization API status: [%08x:%08x] %s</td>
<td>An internal service received an error when it called the Policy Director authorization service.</td>
<td>Use the returned error codes and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
</tbody>
</table>
Unable to initialize Authorization Service: 0x%x: %s

Explanation: An error occurred when the PDOSD daemon attempted to initialize the Policy Director authorization service.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Unable to initialize Audit Service: 0x%x: %s

Explanation: An error occurred when the PDOSD daemon attempted to initialize the audit service.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Unable to shutdown Authorization Service: 0x%x: %s

Explanation: An error occurred when the PDOSD daemon attempted to shut down the Policy Director authorization service.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Unable to shutdown Audit Service: 0x%x: %s

Explanation: An error occurred when the PDOSD daemon attempted to shut down the audit service.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Unable to initialize wildcard service: 0x%x: %s

Explanation: An error occurred when the PDOSD daemon attempted to initialize the wildcard service.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Unable to shutdown wildcard service: 0x%x: %s

Explanation: An error occurred when the PDOSD daemon attempted to shut down the wildcard service.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Authorization Service initialized.

Explanation: The PDOSD daemon has initialized the authorization service.

Action: None

Audit Service initialized.

Explanation: The PDOSD daemon has initialized the audit service.

Action: None

Credential Service initialized.

Explanation: The PDOSD daemon has initialized the credential service.

Action: None
<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Explanation</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x35a53092</td>
<td>Credential Service shutdown</td>
<td>The PDOSD daemon has shut down the credential service.</td>
<td>None</td>
</tr>
<tr>
<td>0x35a53093</td>
<td>Unable to initialize TCB Monitor service</td>
<td>An error occurred when the PDOSD daemon attempted to initialize the Trusted Computing Base (TCB) monitoring service.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35a53094</td>
<td>Unable to shutdown TCB Monitor service</td>
<td>An error occurred when the PDOSD daemon attempted to shut down the Trusted Computing Base (TCB) monitoring service.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35a53095</td>
<td>TCB Monitor service initialized</td>
<td>The PDOSD daemon has initialized the Trusted Computing Base (TCB) monitoring service.</td>
<td>None</td>
</tr>
<tr>
<td>0x35a53096</td>
<td>TCB Monitor service shutdown</td>
<td>The PDOSD daemon has shut down the Trusted Computing Base (TCB) monitoring service.</td>
<td>None</td>
</tr>
<tr>
<td>0x35a53097</td>
<td>Unable to initialize AZN Message Handler Service</td>
<td>An error occurred when the PDOSD daemon attempted to initialize the AZN message handling service.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35a53098</td>
<td>Unable to shutdown AZN Message Handler Service</td>
<td>An error occurred when the PDOSD daemon attempted to shut down the AZN message handling service.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35a53099</td>
<td>AZN Message Handler Service initialized</td>
<td>The PDOSD daemon has initialized the AZN message handler service.</td>
<td>None</td>
</tr>
<tr>
<td>0x35a5309a</td>
<td>AZN Message Handler Service shutdown</td>
<td>The PDOSD daemon has shut down the AZN message handler service.</td>
<td>None</td>
</tr>
<tr>
<td>0x35a5309b</td>
<td>Unable to initialize KPCMGR Service</td>
<td>An error occurred when the PDOSD daemon attempted to initialize the PDOS Kernel Policy Cache Manager (KPCMGR) service.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35a5309c</td>
<td>Unable to shutdown KPCMGR Service</td>
<td>An error occurred when the PDOSD daemon attempted to shut down the PDOS Kernel Policy Cache Manager (KPCMGR) service.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35a5309d</td>
<td>Kernel Policy Cache Manager Service initialized</td>
<td>The PDOSD daemon has initialized the PDOS Kernel Policy Cache Manager (KPCMGR) service.</td>
<td>None</td>
</tr>
</tbody>
</table>
0x35a5309e Kernel Policy Cache Manager Service shutdown

Explanation: The PDOSD daemon has shut down the PDOS Kernel Policy Cache Manager (KPCMGR) service.

Action: None

0x35a5309f PDOSD terminating cleanly

Explanation: The PDOSD daemon is terminating normally.

Action: None

0x35a530a0 PDOSD successfully shutdown

Explanation: The PDOSD daemon has shut down successfully.

Action: None

0x35a530a1 PDOSD was unable to activate kernel interception: 0x%x: %s

Explanation: An error occurred when the PDOSD daemon attempted to activate kernel interception of system calls.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a530a2 PDOSD was unable to deactivate kernel interception: 0x%x: %s

Explanation: An error occurred when the PDOSD daemon attempted to deactivate kernel interception of system calls.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a530a3 Kernel interception activated.

Explanation: The PDOSD daemon has activated kernel interception of system calls.

Action: None

0x35a530a4 Kernel interception deactivated.

Explanation: The PDOSD daemon has deactivated kernel interception of system calls.

Action: None

0x35a530a5 Redirecting output to: %s

Explanation: The PDOSD daemon is redirecting output to the location specified.

Action: None

0x35a530a6 Could not list resources: 0x%x: %s

Explanation: An error occurred while the PDOSD daemon was building a list of the resources in the subscribed policy branch.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a530a7 Could not populate TCB resources: 0x%x: %s

Explanation: An error occurred while the PDOSD daemon was pre-populating the Trusted Computing Base (TCB) with the resources from the subscribed policy branch.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a530a8 PDOSD protected objects for policy %s

Explanation: Message heading for the output from the pdosd -l command.

Action: None

0x35a530a9 %s

Explanation: Data for the output of the pdosd -l command.

Action: None

0x35a530aa Could not perform daemon cleanup: 0x%x: %s

Explanation: During PDOS daemon shut down, an error occurred while cleaning up resources.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a530ab PDOSD is already running.

Explanation: An attempt was made to start the PDOSD daemon again when an instance is already running.

Action: None
Invalid TCB policy object while pre-populating TCB database: %s

Explanation: An invalid policy object was found in the Trusted Computing Base (TCB) portion of the subscribed policy branch while the PDOSD daemon was pre-populating the TCB.

Action: Use the pdadmin command to either correct or remove the invalid policy object.

Added TCB file: %s

Explanation: Status message used during Trusted Computing Base (TCB) pre-population to list each object as it is added to the TCB.

Action: None

Control Message Handler Service initialized

Explanation: The PDOSD daemon has initialized the control message handler service.

Action: None

Unable to initialize Control Message Handler Service: 0x%x: %s

Explanation: An error occurred when the PDOS daemon initialized the control message handling service. The control message handling service manages communications between the PDOS daemon and the PDOS commands.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Could not construct initial credential cache: 0x%x: %s

Explanation: An error occurred when the PDOS daemon attempted to pre-populate the PDOS credential cache with the credentials for members of the osseal-admin group.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

The option, '-%c', is valid only when pdosd is not running.

Explanation: An attempt was made to start the PDOSD daemon using the specified command line option when the PDOSD daemon is already running.

Action: Use the pdosctl -k command to shut down the PDOSD daemon currently running. Then retry the command that failed.

Error auditing unknown event ID 0x%x.

Explanation: An internal service attempted to audit an event that is not recognized by the PDOSD auditing service.

Action: Restart the PDOSD daemon and report the error to IBM Customer Support.

Error allocating audit record for event %s (0x%x). The error status is 0x%x: %s

Explanation: An error occurred when the PDOSD daemon attempted to allocate storage for a data structure to store an audit record.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Control Message Handler Service initialized

Explanation: The PDOSD daemon has initialized the control message handler service.

Action: None

Error auditing event %s (0x%x). The error status is 0x%x: %s.

Explanation: An error occurred when the PDOSD daemon attempted to send an audit event message to the PDOSAUDITD daemon.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

PDOSD’s stash file %s is expected to be %u bytes in size but only %u bytes could be read from it.

Explanation: An error occurred while reading the specified stash file indicating that the file is incomplete.

Action: Use the pdosrstr command to restore configuration files that were backed up using the pdosbkup command.

PDOSD’s stash file %s is inaccessible: %d: %s

Explanation: An error occurred while opening the specified stash file.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Unable to determine PDOSD’s status: 0x%x: %s

Explanation: An error occurred during initialization of the PDOSD daemon when checking to see if the PDOSD daemon is already running.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.
**0x35a61080**  Usage: `%s {start|stop}`

**Explanation:** Usage statement

**Action:** None

---

**0x35a61081**  PDOS kernel failed to start cleanly - aborting PDOS startup

**Explanation:** Unable to load and start the PDOS kernel

**Action:** Check the error logs for previous errors to determine the cause of the problem. Correct the problem. Reboot the machine and restart the PDOS kernel and daemons. If the problem persists, contact IBM Customer Support.

---

**0x35a61082**  PDOS started successfully

**Explanation:** Policy Director for Operating Systems was started successfully.

**Action:** None

---

**0x35a61083**  PDOS failed to start

**Explanation:** The attempt to start Policy Director for Operating Systems was not successful.

**Action:** Check the error logs for other errors which might help determine the cause of the problem. Correct the problem and restart the daemons. If the problem persists, contact IBM Customer Support.

---

**0x35a61084**  PDOS startup failure: PDOS kernel is not started

**Explanation:** An attempt was made to start the PDOS daemons before the PDOS kernel was started.

**Action:** Start the PDOS kernel using the 'rc.kosseal start' command. Then start the daemons.

---

**0x35a61085**  PDOS startup failure: Cannot execute `%s`

**Explanation:** PDOS could not be started because the specified command could not be executed.

**Action:** Verify that the specified command exists and has the correct permissions. Check the error log for previous errors to help determine the cause of the problem. Correct the problem and restart PDOS. If the problem persists, contact IBM Customer Support.

---

**0x35a61086**  PDOS shutdown successfully

**Explanation:** Policy Director for Operating Systems has shut down successfully.

**Action:** None

---

**0x35a61087**  Starting PDOS

**Explanation:** Policy Director for Operating Systems is starting.

**Action:** None. Another message is issued when Policy Director for Operating Systems is running. At that point, you can verify that the daemons are running.

---

**0x35a61088**  Stopping PDOS

**Explanation:** Policy Director for Operating Systems is shutting down.

**Action:** None. Another message is issued when the shut down is complete. At that point, you can verify that Policy Director for Operating Systems has been stopped.

---

**0x35a61089**  PDOS kernel did not load

**Explanation:** The load of the PDOS kernel was not successful.

**Action:** Check the error logs for other errors to help determine why the PDOS kernel could not be loaded. Correct the problem and restart the PDOS daemons. If the problem persists, contact IBM Customer Support.

---

**0x35a6108a**  Usage: `%s {start|stop|help}`

**Explanation:** Usage statement.

**Action:** None

---

**0x35a6108b**  Loading PDOS kernel driver

**Explanation:** The PDOS kernel driver is being loaded.

**Action:** None

---

**0x35a6108c**  Loading PDOS kernel modules

**Explanation:** The PDOS kernel modules are being loaded.

**Action:** None
<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Explanation</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x35a6108d</td>
<td>Unloading PDOS kernel modules</td>
<td>The PDOS kernel modules are being unloaded.</td>
<td>None</td>
</tr>
<tr>
<td>0x35a6108e</td>
<td>PDOS kernel driver load failed: %s</td>
<td>The load of the PDOS kernel driver was not successful.</td>
<td>See the error string to determine the cause of the problem. Correct the problem and reload the PDOS kernel. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35a6108f</td>
<td>File %s/%s not found</td>
<td>The following required specified file could not be found.</td>
<td>Check to see why the file could not be found. Contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35a61090</td>
<td>PDOS kernel driver already loaded</td>
<td>The PDOS kernel driver is already loaded.</td>
<td>None. If you wish to reload the PDOS kernel, you must reboot the machine.</td>
</tr>
<tr>
<td>0x35a61091</td>
<td>PDOS kernel module loaded successfully</td>
<td>The PDOS kernel module was loaded successfully.</td>
<td>None</td>
</tr>
<tr>
<td>0x35a61092</td>
<td>PDOS kernel streams module pushed successfully</td>
<td>The PDOS kernel streams module was pushed successfully.</td>
<td>None</td>
</tr>
<tr>
<td>0x35a61093</td>
<td>Failure pushing the PDOS kernel streams module</td>
<td>The PDOS kernel streams module could not be pushed.</td>
<td>Try rebooting the machine and retrying the PDOS kernel startup. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35a61094</td>
<td>Restarting inetd</td>
<td>The inetd process is restarting.</td>
<td>None</td>
</tr>
<tr>
<td>0x35a61095</td>
<td>An older version of TACF is loaded</td>
<td>An unsupported version of TACF is in use.</td>
<td>Remove the unsupported version of TACF before installing Policy Director for Operating Systems.</td>
</tr>
<tr>
<td>0x35a61096</td>
<td>The PDOS kernel driver failed to load, configuration unsupported</td>
<td>The load of the PDOS kernel driver was unsuccessful because the machine configuration is not supported.</td>
<td>Refer to the Policy Director for Operating Systems documentation for the list of supported machine configurations. If the machine configuration appears to be supported, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35a61097</td>
<td>The PDOS kernel was not configured</td>
<td>The PDOS kernel could not be configured.</td>
<td>Check the previous error messages in the error logs to determine the cause of the problem. Correct the problem and restart the PDOS daemons. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35a61098</td>
<td>System call entry not in /etc/name_to_sysnum</td>
<td>Could not find a required system call entry in /etc/name_to_sysnum.</td>
<td>Check the error logs to determine if there are any error messages relating to other initialization errors. If the cause of the problem can not be determined and corrected, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35a61099</td>
<td>PDOS shutdown failure: PDOS kernel did not shut down</td>
<td>The shut down of Policy Director for Operating Systems was not successful because the PDOS kernel did not shut down.</td>
<td>Reboot the machine and try to start and stop PDOS. If the problem persists, contact IBM Customer Support.</td>
</tr>
</tbody>
</table>
0x35a6109a  PDOS shutdown failure: Cannot execute %s
Explanation: The shut down of Policy Director for Operating
Systems was not successful because the specified command
could not be executed.
Action: Check for other errors in the error log that might have
caused the shut down to not complete. Correct the problem and
attempt the shut down again. If the problem persists, contact
IBM Customer Support.

0x35a6109b  PDOS failed to shutdown
Explanation: The attempt to shut down Policy Director for
Operating Systems was not successful.
Action: Check the previous errors in the error log for the
cause of the problem. Correct the problem and restart PDOS. If
the problem persists, contact IBM Customer Support.

0x35a6109c  The start of the PDOS kernel failed due to a
serious error on a previous start attempt.
Explanation: During startup, PDOS detected that a serious
error had occurred on a previous attempt to start the PDOS
kernel. This situation must be resolved before PDOS can
successfully start.
Action: Collect the screen output from the previous error if it is
available and contact IBM Customer Support. Once the
problem is resolved, the /opt/pdos/etc/kosseal_starting__load
file must be manually deleted prior to starting PDOS.

0x35a62001  Unable to allocate memory
Explanation: An error occurred when the process attempted
to allocate memory from the heap. There is not enough free
memory available to complete the request.
Action: Check the system memory limits using the ulimit
command and increase the hard limits if possible. Restart the
process. If the problem persists, contact IBM Customer
Support.

0x35a62002  Operation not yet implemented
Explanation: An internal service attempted to call a service
that is not yet implemented.
Action: Restart the daemons and report the error to IBM
Customer Support.

0x35a62003  Internal coding error
Explanation: An internal error has occurred.
Action: Restart the daemons and report the error to IBM
Customer Support.

0x35a62005  Access denied
Explanation: The process was denied access to a resource or
system service.
Action: Examine additional messages to determine the cause
of the error and correct the problem. Restart the process. If the
problem persists, contact IBM Customer Support.

0x35a62006  a function call received an invalid parameter
Explanation: An error occurred when an internal function
received a parameter that was not valid.
Action: Restart the process and report the error to IBM
Customer Support.

0x35a62007  Bad command line
Explanation: An error occurred when the command was
invoked with incorrect or missing command line options. The
command usage information also is displayed as a result of this
error.
Action: Verify your command syntax and then invoke the
command again using the proper options.

0x35a62008  System call failed
Explanation: An error occurred when making a system call.
This message is preceded by another error message that
provides additional diagnostic information.
Action: Review the error messages to determine the system
call that failed and the associated error number returned.
Correct the cause of the error and retry the operation.

0x35a62009  Invalid Extended attributes
Explanation: The Access-Restrictions extended attribute of an
ACL is not correct. This message is preceded by another error
message that indicates which ACL is in error.
Action: Review the error messages to determine which ACL
contains the error. Verify the syntax of the Access-Restrictions
extended attribute and correct the error. Wait for the PDOSD
daemon to receive the updated policy.

0x35a6200a  Unable to set UID
Explanation: An error occurred while setting the process
UID.
Action: Examine additional error messages to determine the
cause of the error. Correct the problem, then retry the operation.
<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
<th>Explanation</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x35a6200b</td>
<td>Unable to set GID</td>
<td>An error occurred while setting the process GID.</td>
<td>Examine additional error messages to determine the cause of the error. Correct the problem, then retry the operation.</td>
</tr>
<tr>
<td>0x35a6200c</td>
<td>Unable to set EUID</td>
<td>An error occurred while setting the process EUID.</td>
<td>Examine additional error messages to determine the cause of the error. Correct the problem, then retry the operation.</td>
</tr>
<tr>
<td>0x35a6200d</td>
<td>Unable to set EGID</td>
<td>An error occurred while setting the process EGID.</td>
<td>Examine additional error messages to determine the cause of the error. Correct the problem, then retry the operation.</td>
</tr>
<tr>
<td>0x35a6200e</td>
<td>PDOSD is not running</td>
<td>The pdosdestroy, pdosrefresh, pdossudo, pdoswhoami, and pdoswhois commands require that the PDOSD daemon be running. An attempt was made to use one of these commands while the PDOSD daemon was not running.</td>
<td>Start the PDOSD daemon, then issue the command again.</td>
</tr>
<tr>
<td>0x35a6200f</td>
<td>Authorization API failure</td>
<td>An internal service called a Policy Director API and received an error.</td>
<td>This message is preceded by one or more additional error messages. Examine these additional error messages to determine the cause of the error. Correct the problem, then restart the daemons.</td>
</tr>
<tr>
<td>0x35a62010</td>
<td>Could not open the lock file</td>
<td>An error occurred when opening a temporary lock file.</td>
<td>Examine additional error messages to determine the cause of the error. Correct the problem, then restart the daemons.</td>
</tr>
<tr>
<td>0x35a62011</td>
<td>Could not lock the lock file</td>
<td>An error occurred when locking a temporary lock file.</td>
<td>Examine additional error messages to determine the cause of the error. Correct the problem, then restart the daemons.</td>
</tr>
<tr>
<td>0x35a62080</td>
<td>The operation completed successfully.</td>
<td>The requested operation completed without error.</td>
<td>None</td>
</tr>
<tr>
<td>0x35a62081</td>
<td>Unknown command line option: -%c</td>
<td>The command line option specified is not valid.</td>
<td>Verify the proper syntax for the command. Correct the command and retry the operation.</td>
</tr>
<tr>
<td>0x35a62082</td>
<td>Unknown command line argument: %s</td>
<td>The argument specified is not valid.</td>
<td>Verify the proper syntax for the command. Correct the command and retry the operation.</td>
</tr>
<tr>
<td>0x35a62083</td>
<td>The %s command line option requires an argument</td>
<td>The command line option specified requires an argument. No argument was provided on the command line.</td>
<td>Verify the proper syntax for the command. Correct the command and retry the operation.</td>
</tr>
<tr>
<td>0x35a62084</td>
<td>The %s and %s command line arguments are incompatible</td>
<td>The command line arguments specified are incompatible and cannot be used together.</td>
<td>Verify the proper syntax for the command. Correct the command and retry the operation.</td>
</tr>
<tr>
<td>0x35a62085</td>
<td>Could not set routing for %s messages: %d: %s</td>
<td>An error occurred when establishing the message routing for the specified type of messages.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
</tbody>
</table>
0x35a62086 Trace specification is invalid: %s
Explanation: The trace-string specified on the command line is not valid.
Action: Verify the proper syntax for the command. Correct the command and retry the operation.

0x35a62087 Unable to read configuration file %s: %d:
Explanation: An error occurred when reading the specified configuration file.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62088 Configuration value of [%s:%s]: %s
Explanation: Displays a configuration file entry.
Action: None

0x35a62089 Configuration value of [%s:%s]: %d
Explanation: Displays a configuration file entry.
Action: None

0x35a6208a Configuration value of [%s:%s]: %lld
Explanation: Displays a configuration file entry.
Action: None

0x35a6208b Unable to allocate %d bytes of memory
Explanation: An error occurred when the process attempted to allocate memory from the heap. There is not enough free memory available to complete the request.
Action: Check the system memory limits using the ulimit command and increase the hard limits if possible. Restart the process. If the problem persists, contact IBM Customer Support.

0x35a6208c The argument, "%s", to -%c is invalid.
Explanation: The argument provided is not valid with the command line option specified.
Action: Verify the proper syntax for the command. Correct the command and retry the operation.

0x35a6208d Could not determine full path of executable %s: 0x%x: %s
Explanation: An error occurred when resolving the complete path name of the executing program.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a6208e An error occurred while getting the information about the file: File: %s : %s : %d
Explanation: An error occurred when retrieving information about the specified file from the operating system.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a6208f One or more required options are missing.
Explanation: The user did not specify all of the required command line options.
Action: Verify the proper syntax for the command. Correct the command and retry the operation.

0x35a62090 Unable to set UID to %d: %d: %s
Explanation: An error occurred when setting the process UID to the specified value.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62091 Unable to set GID to %d: %d: %s
Explanation: An error occurred when setting the process GID to the specified value.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62092 Unable to set EUID to %d: %d: %s
Explanation: An error occurred when setting the process EUID to the specified value.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.
0x35a62093  Unable to set EGID to \%d: \%d: \%s
Explanation:  An error occurred when setting the process EGID to the specified value.
Action:  Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62094  Unable to determine maximum number of bytes in a file name in the directory \%s: \%d: \%s
Explanation:  An error occurred when retrieving the maximum byte size of a file name in the specified directory.
Action:  Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62100  Unable to change working directory to \%s
Explanation:  An error occurred when attempting to set the current working directory of the running program.
Action:  Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

0x35a62101  Unable to dissociate from controlling terminal
Explanation:  An error occurred when the process attempted to detach from its controlling terminal.
Action:  Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

0x35a62102  Unable to redirect output
Explanation:  An error occurred when the process attempted to redirect std out and stderr to the error log in the /var/pdos/log directory.
Action:  Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

0x35a62103  Unable to change process priority
Explanation:  An error occurred when the process attempted to change its priority.
Action:  Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

0x35a62104  Unable to change process user identity
Explanation:  An error occurred when setting the UID, EUID, GID, or EGID of the current process.
Action:  Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

0x35a62105  Unable to release Operating System resources
Explanation:  An error occurred when the process attempted to close its open file descriptors.
Action:  Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

0x35a62106  Unable to set resource limits
Explanation:  An error occurred when the process attempted to modify its system resource limits.
Action:  Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

0x35a62107  Unable to establish correct signal handling
Explanation:  An error occurred when the process attempted to initialize its signal handling semantics.
Action:  Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

0x35a62108  oss_become_daemon has returned to the parent process
Explanation:  A child process has been successfully started.
Action:  None

0x35a6210a  Child process is shutting down
Explanation:  A process has detected that one of its child processes is terminating prematurely.
Action:  Examine additional messages to determine the cause of the problem with the child process. Correct the problem and restart the process. If the problem persists, contact IBM Customer Support.
0x35a6210b  Child process did not enter running state before timeout
Explanation:  A child process failed to complete initialization in the specified time.
Action:  Examine the log files in the /var/pdos/log directory to determine if the child process is still initializing. In some cases it might take longer than usual for the process to initialize and that is not a problem. If the process does not complete initialization, examine additional messages to determine the cause and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

0x35a62180  %s failed to start within %d seconds. See log file %s for details.
Explanation:  The daemon failed to complete initialization in the specified time.
Action:  Examine the specified log file to determine if the daemon is still initializing. In some cases it might take longer than usual for the process to initialize and that is not a problem. If the process does not complete initialization, examine additional messages to determine the cause and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

0x35a62181  Unable to change directory to %s: %d: %s
Explanation:  An error occurred when attempting to set the current working directory of the program to the specified value.
Action:  Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62182  Unable to open %s for redirecting output: %d: %s
Explanation:  An error occurred when opening the specified daemon log file.
Action:  Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62183  Unable to redirect stdout: %d: %s
Explanation:  An error was received preventing stdout from being redirected to the appropriate log file.
Action:  Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62184  Unable to redirect stderr: %d: %s
Explanation:  An error was received preventing stderr from being redirected to the appropriate log file.
Action:  Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62185  Unable to change process priority to %d: %d: %s
Explanation:  An error occurred when the process attempted to change its priority as specified.
Action:  Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62186  Unable to fork child process: %d: %s
Explanation:  An error occurred while creating a new child process.
Action:  Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62187  Unable to detach from controlling terminal: %d: %s
Explanation:  An error occurred when the process attempted to detach from its controlling terminal.
Action:  Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62188  Could not determine maximum per-process open file descriptors: %d: %s
Explanation:  An error occurred when retrieving the maximum number of open file descriptors allowed on the system.
Action:  Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62189  Unable to determine current %s resource limit: %d: %s
Explanation:  An error occurred when the process attempted to retrieve the specified system resource limit.
Action:  Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.
0x35a6218a  Unable to set %s resource limit: %d: %s
Explanation: An error occurred when the process attempted to set the specified system resource limit.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a6218b  System call failed: %s: %d: %s
Explanation: The specified system call failed with an unexpected error code.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a6218d  Unable to become daemon: 0x%x: %s
Explanation: An error occurred when the process attempted to turn itself into a daemon process.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a6218e  %s shutdown signal %s received
Explanation: Indicates that the specified process was shut down by the given signal.
Action: None

0x35a62190  Unrecognized %s shutdown signal %d received
Explanation: The specified process was shut down by an unrecognized shut down signal.
Action: Contact IBM Customer Support.

0x35a62191  Could not send status request message to running %s: 0x%x: %s
Explanation: An error occurred when sending a status request message to the specified daemon process.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62192  Could not put data in to status request message: 0x%x: %s
Explanation: An error occurred when building a status request message.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62193  Could not get body of status response message: 0x%x: %s
Explanation: An error occurred when receiving the response data from a status request.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62194  Received an invalid response to a status message: class: %d fmt: %d msg: %d fmt %d
Explanation: The response to a status request contains data that is not valid.
Action: Contact IBM Customer Support.

0x35a62195  Could not get header of status response message: 0x%x: %s
Explanation: An error occurred when receiving the response header of a status request message.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62196  %s is initializing
Explanation: The specified daemon is initializing.
Action: None

0x35a62197  %s is running normally
Explanation: The specified daemon is running under normal conditions.
Action: None

0x35a62198  %s is running under abnormal conditions:
Explanation: The specified daemon is running under one or more abnormal conditions. The daemon continues to run. This message is followed by one or more messages indicating the abnormal conditions that exist.
Action: Examine the messages that follow to determine the abnormal conditions that currently exist and correct them.

0x35a62199  isolated from the master policy server
Explanation: The process is unable to communicate with the Policy Director server.
Action: Verify that network connectivity exists to the Policy Director server and correct any communication problems. Check that the Policy Director server itself is in a valid state and correct any errors.
0x35a6219a  isolated from the user registry
Explanation:  The process is unable to communicate with the Policy Director user registry.
Action: Verify that network connectivity exists to the Policy Director user registry and correct any communication problems. Check that the Policy Director user registry itself is in a valid state and correct any errors.

0x35a6219b  %s is shutting down
Explanation:  The specified daemon is in the process of shutting down.
Action: None

0x35a6219c  %s is in an unexpected state: 0x%x
Explanation:  The specified daemon is in an unknown state.
Action: Contact IBM Customer Support.

0x35a6219d  Could not join the set of watchdog processes: 0x%x: %s
Explanation:  The PDOSD, PDOSAUDITD, and PDOSWDD daemons form a set of processes that watch, or monitor, each other. If one of the processes being watched terminates unexpectedly, another process attempts to restart it. An error occurred when the current process attempted to join the watchdog set so that it could be monitored by the others.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a6219e  Unable to register as a privileged process: 0x%x: %s
Explanation:  An error occurred when the current process attempted to register itself with the kernel as a privileged process.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a6219f  %s registered as a PDOS kernel privileged process.
Explanation:  The specified process has successfully registered itself with the kernel and has set its privilege and immunity.
Action: None

0x35a621a0  %s was unable to become a privileged PDOS kernel process: 0x%x: %s
Explanation:  An error when the current process attempted to register its privilege and immunity with the kernel.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62200  An error occurred during thread initialization
Explanation:  An unexpected error occurred when the thread was initializing.
Action: Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

0x35a62201  An error occurred while locking a mutex
Explanation:  An unexpected error occur when obtaining a mutex lock for serialization.
Action: Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

0x35a62202  An error occurred while unlocking a mutex
Explanation:  An unexpected error occur when releasing a mutex lock.
Action: Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

0x35a62203  An error occurred during thread cancellation
Explanation:  An unexpected error occurred when cancelling a thread.
Action: Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

0x35a62204  An error occurred while joining a thread
Explanation:  An unexpected error occurred when joining a thread.
Action: Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.
0x35a62205  An error occurred while creating a thread  
**Explanation:** An unexpected error occurred when creating a thread.  
**Action:** Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

0x35a62206  An error occurred while signaling a thread  
**Explanation:** An unexpected error occurred when attempting to signal a thread.  
**Action:** Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

0x35a62207  An error occurred while waiting on a condition variable  
**Explanation:** An unexpected error occurred when waiting on a condition variable.  
**Action:** Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

0x35a62208  An error occurred during thread destruction  
**Explanation:** An unexpected error occurred when destroying a thread.  
**Action:** Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

0x35a62209  An error occurred while setting thread cancellation state  
**Explanation:** An unexpected error occurred when setting the cancellation state of a thread.  
**Action:** Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

0x35a6220a  An error occurred while detaching a thread  
**Explanation:** An unexpected error occurred when detaching a thread.  
**Action:** Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

0x35a6220b  An error occurred while initializing a condition variable  
**Explanation:** An unexpected error occurred when initializing a condition variable.  
**Action:** Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

0x35a62218  An error occurred while locking a mutex: %d: %s  
**Explanation:** An unexpected error occurred when obtaining a mutex lock for serialization.  
**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62221  An error occurred while unlocking a mutex: %d: %s  
**Explanation:** An unexpected error occurred when releasing a mutex lock.  
**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62222  An error occurred during thread cancellation: %d: %s  
**Explanation:** An unexpected error occurred when cancelling a thread.  
**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62223  An error occurred while joining a thread: %d: %s  
**Explanation:** An unexpected error occurred when joining a thread.  
**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.
<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
<th>Explanation</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x35a62285</td>
<td>An error occurred while creating a thread: %d: %s</td>
<td>An unexpected error occurred when creating a thread.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35a62286</td>
<td>An error occurred while destroying the mutex: %d: %s</td>
<td>An unexpected error occurred when destroying the mutex lock.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35a62287</td>
<td>An error occurred while signaling a condition variable: %d: %s</td>
<td>An unexpected error occurred when sending a signal to a condition variable.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35a62288</td>
<td>An error occurred while waiting on a condition variable: %d: %s</td>
<td>An unexpected error occurred while waiting on a condition variable.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35a62289</td>
<td>An error occurred while setting thread cancellation state: %d: %s</td>
<td>An unexpected error occurred when setting the cancellation state of a thread.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35a6228a</td>
<td>An error occurred while detaching a thread: %d: %s</td>
<td>An unexpected error occurred when detaching a thread.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35a62300</td>
<td>Invalid argument to routine</td>
<td>An internal service passed an invalid argument to the function that reads the configuration files.</td>
<td>Contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35a62301</td>
<td>Access denied to stanza file</td>
<td>The user ID in which the process is running under does not have sufficient permission to open the configuration file.</td>
<td>Examine additional messages to determine the name of the configuration file. Verify that both UNIX permissions and PDOS policy permit the process to read and write (configuration commands) the configuration file. Correct the problem and restart the process.</td>
</tr>
<tr>
<td>0x35a62302</td>
<td>Stanza file does not exist</td>
<td>A needed configuration file was not found.</td>
<td>Examine additional messages to determine the name of the configuration file. Examine the /var/pdos/log/pdoscfg.log file to determine if PDOS is configured. If PDOS is configured, use the pdocsrstr command to restore the backed up configuration files. Restart the process.</td>
</tr>
<tr>
<td>0x35a62303</td>
<td>Could not open stanza file</td>
<td>An error occurred when attempting to open a configuration file.</td>
<td>Examine additional messages to determine the name of the configuration file and the cause of the failure. Correct the problem and restart the process.</td>
</tr>
<tr>
<td>0x35a62304</td>
<td>Could not lock stanza file</td>
<td>An error occurred when attempting to lock a configuration file.</td>
<td>Examine additional messages to determine the name of the configuration file and the cause of the failure. Correct the problem and restart the process.</td>
</tr>
<tr>
<td>0x35a62305</td>
<td>Stanza file is closed</td>
<td>An internal service attempted to read or write a configuration file that is closed.</td>
<td>Contact IBM Customer Support.</td>
</tr>
</tbody>
</table>
0x35a62306  No terminating bracket on stanza name
Explanation:  The configuration file contains incorrect syntax. Stanzas must be delimited by [ ].
Action:  Examine additional messages to determine the name of the configuration file. Correct the problem and restart the process. The pddrsrstr command can be used to restore a backed up configuration.

0x35a62307  No separator between stanza entry and value
Explanation:  The configuration file contains incorrect syntax. Each entry must contain an = separator character between the entry ID and its value.
Action:  Examine additional messages to determine the name of the configuration file. Correct the problem and restart the process. The pddrsrstr command can be used to restore a backed up configuration.

0x35a62309  Unexpected NULL argument in routine
Explanation:  An internal service passed a NULL stanza name to an internal function.
Action:  Contact IBM Customer Support.

0x35a6230a  Some expected configuration data is not present in the configuration file
Explanation:  A required entry is missing from the configuration file.
Action:  Examine additional messages to determine the name of the configuration file, the stanza name, and the missing entry. Correct the problem and restart the process. The pddrsrstr command can be used to restore a backed up configuration.

0x35a6230b  Stanza file was opened in read-only mode.
Explanation:  An internal service attempted to modify a configuration while it was open for read access only.
Action:  Contact IBM Customer Support.

0x35a6230c  Stanza file could not be read.
Explanation:  An error occurred when reading a configuration file.
Action:  Contact IBM Customer Support.

0x35a6230d  The text in the stanza file could not be replaced.
Explanation:  An error occurred when modifying a configuration file.
Action:  Verify that there is free space in the filesystem containing the /opt/pdos/etc directory. If there is free space, contact IBM Customer Support.

0x35a6230e  The entry does not exist in the stanza file.
Explanation:  An internal service attempted to delete a non-existent entry from a configuration file.
Action:  Contact IBM Customer Support.

0x35a6230f  An invalid audit level was specified.
Explanation:  The configuration file contains an invalid audit level.
Action:  Examine additional messages to determine the name of the configuration file and the invalid audit level. Correct the problem and restart the process. The pddrsrstr command can be used to restore a backed up configuration.

0x35a62310  The audit level string is badly formatted.
Explanation:  The configuration file contains an invalid list of audit levels. Audit levels must be separated by commas.
Action:  Examine additional messages to determine the name of the configuration file. Correct the problem and restart the process. The pddrsrstr command can be used to restore a backed up configuration.

0x35a62380  Could not lock stanza file %s: %d: %s
Explanation:  An error occurred when locking the specified configuration file.
Action:  Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62381  Could not open stanza file %s: %d: %s
Explanation:  An error occurred when opening the specified configuration file.
Action:  Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.
### 0x35a62382 Unexpected NULL argument in %s routine
**Explanation:** An internal service passed a NULL stanza name to an internal function.
**Action:** Contact IBM Customer Support.

### 0x35a62383 Required configuration item [%s:%s] is missing
**Explanation:** The configuration file is missing the specified entry.
**Action:** Examine additional messages to determine the name of the configuration file. Correct the problem and restart the process. The pdosrstr command can be used to restore a backed up configuration.

### 0x35a62384 The '%.s' audit level specified in the %s configuration file is invalid
**Explanation:** The audit level specified in the configuration file is not valid.
**Action:** Consult the product documentation for the valid audit levels. Correct the problem and restart the process. The pdosrstr command can be used to restore a backed up configuration.

### 0x35a62385 The audit level string specified in the %s configuration file is badly formatted
**Explanation:** The specified configuration file contains an invalid list of audit levels. Audit levels must be separated by commas.
**Action:** Correct the problem and restart the process. The pdosrstr command can be used to restore a backed up configuration.

### 0x35a62400 User name has no corresponding UID
**Explanation:** The user name that was specified does not exist in the system’s native user registry.
**Action:** Retry the command using a user name that is in the system’s native user registry.

### 0x35a62402 UID not recognized by system
**Explanation:** The UID that was specified does not exist in the system’s native user registry.
**Action:** Retry the command using a UID that is in the system’s native user registry.

### 0x35a62403 GID not recognized by system
**Explanation:** The GID that was specified does not exist in the system’s native user registry.
**Action:** Retry the command using a GID that is in the system’s native user registry.

### 0x35a62404 Unable to map name to UID
**Explanation:** An error occurred when mapping the user name to a UID.
**Action:** Examine additional messages to determine the cause of the failure and correct the problem. Retry the command. If the problem persists, contact IBM Customer Support.

### 0x35a62405 Unable to map UID to name
**Explanation:** An error occurred when mapping the UID to a user name.
**Action:** Examine additional messages to determine the cause of the failure and correct the problem. Retry the command. If the problem persists, contact IBM Customer Support.

### 0x35a62406 Unable to map name to GID
**Explanation:** An error occurred when mapping the group name to a GID.
**Action:** Examine additional messages to determine the cause of the failure and correct the problem. Retry the command. If the problem persists, contact IBM Customer Support.

### 0x35a62407 Unable to map GID to name
**Explanation:** An error occurred when mapping the GID to a GROUP name.
**Action:** Examine additional messages to determine the cause of the failure and correct the problem. Retry the command. If the problem persists, contact IBM Customer Support.

### 0x35a62408 Unable to get the password
**Explanation:** An error occurred when retrieving the user’s password from the system’s native user registry.
**Action:** Examine additional messages to determine the cause of the failure and correct the problem. Retry the command. If the problem persists, contact IBM Customer Support.
0x35a62480  Unable to map UID %u to name: %d: %s
Explanation:  An error occurred when mapping the specified UID to a user name.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62481  Unable to map GID %u to name: %d: %s
Explanation:  An error occurred when mapping the specified GID to a user name.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62482  Unable to map name %s to UID: %d: %s
Explanation:  An error occurred when mapping the specified user name to a UID.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62483  Unable to map name %s to GID: %d: %s
Explanation:  An error occurred when mapping the specified group name to a GID.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62484  Unable to convert user name %s to a UID: 0x%x: %s
Explanation:  An error occurred when mapping the specified user name to a UID.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62485  Unable to convert group name %s to a GID: 0x%x: %s
Explanation:  An error occurred when mapping the specified group name to a GID.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62486  Unable to get the password for the user %s: %d: %s
Explanation:  An error occurred when retrieving the specified user’s password from the system’s native user registry.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35a62500  Unable to lookup host address information
Explanation:  An error occurred when retrieving the network host information from the system.
Action: Examine additional messages to determine the cause of the failure and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

0x35a62501  Host address information not found
Explanation:  Unable to retrieve the network host information because the host name cannot be found in the system files.
Action: None

0x35a62502  Host address information from cache used but it is stale
Explanation:  The system was unable to convert an network IP address to a host name. However, a stale entry for the address was found in the PDOS hla cache which may be used.
Action: Verify that the network is not experiencing problems. Correct any communication problems and retry the command.

0x35a62503  Service information not found
Explanation:  The specified network service was not found on the system.
Action: Correct the invalid policy and retry.

0x35a62505  Network address family is not supported
Explanation:  An internal service attempted to use an unsupported type of network IP address.
Action: Contact IBM Customer Support.

0x35a62506  Network protocol is not supported
Explanation:  An unsupported type of network protocol was specified.
Action: Contact IBM Customer Support.
The IP address specified is invalid.
Explanation: The IP address specified is not valid.
Action: Retry the command using a valid network IP address.

The Hostname specified is invalid.
Explanation: The host name specified is not valid.
Action: Retry the command using a valid network hostname.

Unable to lookup address information: %s: %d
Explanation: An error occurred while retrieving the network host information for the specified host name from the system.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Unable to lookup address info: %d.%d.%d.%d: %d
Explanation: An error occurred while retrieving the network host information for the specified network IP address from the system.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Network address family is not supported: %d
Explanation: An internal service attempted to use the specified unsupported type of network IP address.
Action: Contact IBM Customer Support.

Network protocol is not supported: %s
Explanation: The specified network protocol is not supported.
Action: Contact IBM Customer Support.

# Internet Address Hostname
Explanation: Header for the output of the pdoshla command.
Action: None

The IP address, %s, is invalid.
Explanation: The specified IP address is not a valid network IP address.
Action: Retry the command using a valid network IP address.

The Hostname, %s, is invalid.
Explanation: The specified host name is not a valid network host name.
Action: Retry the command using a valid network host name.

The database is already initialized.
Explanation: An internal service attempted to initialize a database that had previously been initialized.
Action: Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

The database is not yet initialized
Explanation: An internal service attempted to access a database before the database was initialized.
Action: Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

Failed to open the database.
Explanation: An unexpected error occurred when opening the database.
Action: Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

The database file does not exist.
Explanation: Unable to locate the database file specified.
Action: Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

Failed to create the database.
Explanation: An unexpected error occurred when creating the database.
Action: Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

Failed to close the database.
Explanation: An unexpected error occurred when closing the database.
Action: Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.
An unexpected database error occurred.

Explanation: An unexpected error occurred while accessing the database.

Action: Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

The specified entry was not found in the database.

Explanation: Unable to locate the specified entry in the database.

Action: Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

The specified entry already exists in the database.

Explanation: The database already contains the specified entry.

Action: None

MMAP failed on HP-UX with ENOMEM

Explanation: This error is specific to HP-UX systems. In some circumstances, HP-UX erroneously reports out of memory conditions when memory mapping a file.

Action: No action is required. This condition is handled internally.

Unable to open the database file or directory

Explanation: An error occurred when attempting to open the specified database file or directory.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Unable to create the database file

Explanation: An error occurred when creating the specified database file.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Unable to close the database file

Explanation: An error occurred when closing the specified database file.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

The specified entry, %s, was not found in the database.

Explanation: Unable to locate the specified entry in the database.

Action: Try the command again using the correct object name.

An error occurred while iterating through the database.

Explanation: An unexpected error occurred when iterating through database entries.

Action: Contact IBM Customer Support.

An error occurred while fetching the entry from the database

Explanation: An unexpected error occurred when attempting to retrieve the specified entry from the database.

Action: Contact IBM Customer Support.

An error occurred while deleting the entry from the database

Explanation: An error occurred when attempting to delete the specified entry from the database.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

An error occurred while storing the entry in the database

Explanation: An error occurred when attempting to store the specified entry into the database.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.
An error occurred while getting the host name for the IP address, %s: status = %s: %d

Explanation: An error occurred when the system attempted to convert the given network IP address to a host name.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

An error occurred while trying to get the total number of entries in the database: %s: %d

Explanation: An internal service received an error while querying the database for its number of entries.

Action: Contact IBM Customer Support.

An error occurred in listing the entries in the database: %s: %d

Explanation: An error occurred while dumping the contents of the database.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Could not open the lock file %s: %s: %d

Explanation: An error occurred when opening the specified lock file.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Could not get the lock on the lock file %s: %s: %d

Explanation: An error occurred when locking the specified lock file.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Either there are no entries in the database or there are no entries that satisfy the given criteria.

Explanation: Command response for a database query command.

Action: None

Attempt to lock file with flags 0x%x failed: %d: %s

Explanation: An error occurred when locking the lock file with the specified flags.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Attempt to unlock file failed: %d: %s

Explanation: An error occurred when unlocking the lock file.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

An unexpected database error occurred. %s: %d

Explanation: An unexpected error occurred when accessing the database.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

IO error occurred while accessing kernel policy cache

Explanation: An error was returned from the PDOS kernel policy cache service indicating that it failed with an I/O error.

Action: Contact IBM Customer Support.

Kernel unable to obtain memory

Explanation: An error was returned from the PDOS kernel policy cache service indicating that it failed with an out of memory error.

Action: Contact IBM Customer Support.

Unable to modify kernel policy cache

Explanation: An error was returned from the PDOS kernel policy cache service indicating that it failed while trying to update the policy.

Action: Contact IBM Customer Support.

No kernel policy cache statistics currently available

Explanation: An error was returned from the PDOS kernel policy indicating that the attempt to retrieve statistics failed because none are available.

Action: Contact IBM Customer Support.
0x35a62704  call or parameter value not supported
Explanation:  An error was returned from the PDOS kernel policy cache indicating that it failed because of an invalid parameter.
Action:  Contact IBM Customer Support.

0x35a62705  no entry found for specified operation
Explanation:  An error was returned from the PDOS kernel policy cache indicating a query for a non-existent entry.
Action:  Contact IBM Customer Support.

0x35a62706  a parameter value was too large
Explanation:  An error was returned from the PDOS kernel policy cache indicating that a return value is too big to fit into the allocated space.
Action:  Contact IBM Customer Support.

0x35a62780  invalid parameter value
Explanation:  An error was returned from the PDOS kernel extension indicating that it received an invalid parameter.
Action:  Contact IBM Customer Support.

0x35a62781  insufficient permission
Explanation:  An error was returned from the PDOS kernel extension indicating that the caller is not authorized for the operation.
Action:  Contact IBM Customer Support.

0x35a62782  kosseal currently not available
Explanation:  An error was returned from the PDOS kernel extension indicating that it is not available.
Action:  Contact IBM Customer Support.

0x35a62783  information not found
Explanation:  An error was returned from the PDOS kernel extension indicating that the requested information was not found.
Action:  Contact IBM Customer Support.

0x35a62880  AZN Protected Object Name
Explanation:  Describes an internal object allocation type.
Action:  None

0x35a62881  MSG Q Element
Explanation:  Describes an internal object allocation type.
Action:  None

0x35a62900  An allocator with outstanding allocations may not be deleted.
Explanation:  An internal memory allocation service returned an error because an attempt was made to remove the service while it was still in use.
Action:  Contact IBM Customer Support.

0x35a62901  An allocator with %d outstanding allocations may not be deleted.
Explanation:  An internal memory allocation service returned an error because an attempt was made to remove the service while it was still in use.
Action:  Contact IBM Customer Support.

0x35a7c080  PDOSTECD started successfully.
Explanation:  The PDOSTECD daemon was started successfully.
Action:  None

0x35a7c081  PDOSTECD is already running.
Explanation:  PDOSTECD is already running and it cannot be started again when there is an existing PDOSTECD running.
Action:  Do not try to start PDOSTECD when it is already running.

0x35a7c082  PDOSTECD successfully shut down.
Explanation:  The PDOSTECD daemon has shut down successfully.
Action:  None

0x35a7c083  PDOSTECD was unable to allocate memory.
Explanation:  The PDOSTECD daemon was unable to allocate memory.
Action:  Check the state of system resources such as virtual memory usage. Correct the problem and restart the PDOSTECD daemon. If the problem persists, contact IBM Customer Support.
0x35a7c084  PDOSTECD internal error occurred. Error: %d.
Explanation: An unexpected error occurred in the PDOSTECD daemon.
Action: Use the error code in the message to determine the cause of the problem. Correct the problem and restart the PDOSTECD daemon. If the problem persists, contact IBM Customer Support.

0x35a7c085  Unable to create socket object.
Explanation: The PDOSTECD daemon was unable to create a socket.
Action: Check system resources to determine the cause of the problem. Correct the problem and restart the PDOSTECD daemon. If the problem persists, contact IBM Customer Support.

0x35a7c086  Unable to create string object.
Explanation: The PDOSTECD daemon was unable to create a string object.
Action: Check the state of system resources such as virtual memory usage. Correct the problem and restart the PDOSTECD daemon. If the problem persists, contact IBM Customer Support.

0x35a7c087  Unable to create FIFO.
Explanation: The PDOSTECD daemon was unable to create FIFO.
Action: Check the state of system resources such as virtual memory usage. Verify that the proper UNIX file permissions are set to allow file creation. Correct the problem and restart the PDOSTECD daemon. If the problem persists, contact IBM Customer Support.

0x35a7c088  Unable to open FIFO.
Explanation: The PDOSTECD daemon was unable to open FIFO.
Action: Check the state of system resources such as virtual memory usage. Verify that the proper UNIX file permissions are set to allow it to be opened. Correct the problem and restart the PDOSTECD daemon. If the problem persists, contact IBM Customer Support.

0x35a7c089  Unable to open file.
Explanation: The PDOSTECD daemon was unable to open the event file.
Action: Check the state of system resources such as virtual memory usage. Verify that the proper UNIX file permissions are set to allow the event file to be opened. Correct the problem and restart the PDOSTECD daemon. If the problem persists, contact IBM Customer Support.

0x35a7c08a  Unable to write event.
Explanation: The PDOSTECD daemon was unable to write an event to the event file.
Action: Verify that the proper UNIX file permissions are set to allow the event file to be opened. Correct the problem and restart the PDOSTECD daemon. If the problem persists, contact IBM Customer Support.

0x35a7c08b  Unable to initialize OSS serviceability.
Explanation: The PDOSTECD daemon was unable to initialize the OSS serviceability module.
Action: Check for previous errors in the TEC log files for the cause of the problem. Correct the problem and restart the PDOSTECD daemon. If the problem persists, contact IBM Customer Support.

0x35a7c08c  Unable to initialize audview serviceability.
Explanation: The PDOSTECD daemon was unable to initialize the audit view serviceability module.
Action: Check for previous errors in the TEC log files for the cause of the problem. Correct the problem and restart the PDOSTECD daemon. If the problem persists, contact IBM Customer Support.

0x35a7c08d  Unable to open audit log.
Explanation: The PDOSTECD daemon was unable to open the audit log file.
Action: Verify that the proper UNIX file permissions are set to allow the event file to be opened. Correct the problem and retry the operation. If the problem persists, contact IBM Customer Support.

0x35a7c08e  Unable to determine file size of audit log.
Explanation: The PDOSTECD daemon was unable to determine the size of the audit log file.
Action: The audit log file is located in the /var/pdos/audit directory. Verify that the proper UNIX file permissions are set to allow the audit log file to be opened and read. Correct the problem and retry the operation. If the problem persists, contact IBM Customer Support.
0x35a7c08f Unable to determine file information for audit log.

Explanation: The PDOSTECD daemon encountered an unexpected error retrieving information about the audit log file.

Action: The audit log file is located in the /var/pdos/audit directory. Verify that the proper UNIX file permissions are set to allow the audit log file to be opened and read. Correct the problem and retry the operation. If the problem persists, contact IBM Customer Support.

0x35a7c090 Unable to read audit log.

Explanation: The PDOSTECD daemon was unable to read the audit log file.

Action: The audit log file is located in the /var/pdos/audit directory. Verify that the proper UNIX file permissions are set to allow the audit log file to be opened and read. Correct the problem and retry the operation. If the problem persists, contact IBM Customer Support.

0x35a7c091 Unable to switch to active audit log.

Explanation: The audit daemon was unable to switch over to use the newly activated audit log file.

Action: Check the error logs to determine cause of the problem. Correct the problem and restart the PDOS daemons. If the problem persists, contact IBM Customer Support.

0x35a7c092 Unable to open /var/pdos/audit directory.

Explanation: The process was unable to open the /var/pdos/audit directory which contains the audit log.

Action: Check the UNIX directory permissions to determine the cause of the problem. Correct the problem and retry the operation. If the problem persists, contact IBM Customer Support.

0x35a7c093 An archived audit.log file was not processed.

Explanation: The audit daemon was unable to process events in an archived audit log.

Action: This error generally occurs when there is a high volume of audit events occurring in the system, resulting in the audit log files being filled quickly and rolled over. Try increasing the size of the audit log file using the pdoscfg command to alleviate the problem.

0x35ab3001 Usage: pdosctl -k [daemon [-k daemon ...]]
idosctl -s [daemon [-s daemon ...]] [-q]
idosctl -w [on|off] pdosctl -a [audit-level[:{on|off}] [-a audit-level[:{on|off}] ...
idosctl -A [audit-level[:{on|off}] [-A audit-level[:{on|off}] ...
idosctl -t [daemon[trace-string] [-t
daoen[trace-string] ...
idosctl [-Vvh?] [-t trace-string]

Explanation: pdosctl command usage statement.

Action: None

0x35ab3002 Argument to -%c must be a daemon name. "%s" is invalid.

Explanation: The argument to the given pdosctl command line option must be a valid PDOS daemon name.

Action: Verify the proper syntax of the pdosctl command. Correct the problem and retry the pdosctl command.

0x35ab3003 Argument to -%c must be a valid audit level. "%s" is invalid.

Explanation: The argument to the given pdosctl command line option must be a valid PDOS audit level.

Action: Verify the proper syntax of the pdosctl command. Correct the problem and retry the pdosctl command.

0x35ab3004 Argument to -%c must be 'on' or 'off'. "%s" is invalid.

Explanation: The argument to the given pdosctl command line option must be either 'on' or 'off'.

Action: Verify the proper syntax of the pdosctl command. Correct the problem and retry the pdosctl command.

0x35ab3005 Qualifier to %s argument of -%c option must be 'on' or 'off'. "%s" is invalid.

Explanation: The qualifier for the argument of the given pdosctl command line option must be either 'on' or 'off'.

Action: Verify the proper syntax of the pdosctl command. Correct the problem and retry the pdosctl command.

0x35ab3006 Could not send trace request message to %s: 0x%ex: %s

Explanation: An error occurred when the pdosctl command attempted to send a trace control message to the specified PDOS daemon.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.
0x35ab3007  Could not put data to trace request message for \%s: 0x%\x: \%s
Explanation:  An error occurred when the pdosctl command was creating the data structure that is used to send a trace control message to the specified PDOS daemon.
Action:  Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab3008  Could not get body of trace response message from \%s: 0x%\x: \%s
Explanation:  An error occurred when the pdosctl command was receiving the response to a trace control message from the specified PDOS daemon.
Action:  Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab3009  Received an invalid response to a trace message from \%s: class: \%d fmt: \%d msg: \%d fmt \%d
Explanation:  The pdosctl command received an invalid response to a trace control message from the specified PDOS daemon.
Action:  Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab300a  Could not get header of trace response message from \%s: 0x%\x: \%s
Explanation:  An error occurred when the pdosctl command was receiving the response to a trace control message from the specified PDOS daemon.
Action:  Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab300b  Could not send shutdown request message to \%s: 0x%\x: \%s
Explanation:  An error occurred when the pdosctl command attempted to send a shut down control message to the specified PDOS daemon.
Action:  Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab300c  Could not put data to shutdown request message for \%s: 0x%\x: \%s
Explanation:  An error occurred when the pdosctl command was creating the data structure that is used to send a shut down control message to the specified PDOS daemon.
Action:  Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab300d  Could not get body of shutdown response message from \%s: 0x%\x: \%s
Explanation:  An error occurred when the pdosctl command was receiving the response to a shut down control message from the specified PDOS daemon.
Action:  Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab300e  Received an invalid response to a shutdown message from \%s: class: \%d fmt: \%d msg: \%d fmt \%d
Explanation:  The pdosctl command received an invalid response to a shut down control message from the specified PDOS daemon.
Action:  Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab300f  Could not get header of shutdown response message from \%s: 0x%\x: \%s
Explanation:  An error occurred when the pdosctl command was receiving the response to a shut down control message from the specified PDOS daemon.
Action:  Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab3010  %s shutdown
Explanation:  The pdosctl command has successfully shut down the specified PDOS daemon.
Action:  None

0x35ab3011  %s would not shutdown: 0x%\x: \%s
Explanation:  The pdosctl command was not able to shut down the specified PDOS daemon.
Action:  Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.
<table>
<thead>
<tr>
<th>Code</th>
<th>Message</th>
<th>Explanation</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x35ab3012</td>
<td>%s is not running</td>
<td>Response from the pdosctl command indicating that the specified PDOS daemon is not currently running.</td>
<td>None</td>
</tr>
<tr>
<td>0x35ab3013</td>
<td>%s is not running</td>
<td>Response from the pdosctl command indicating that the specified PDOS daemon is not currently running.</td>
<td>None</td>
</tr>
<tr>
<td>0x35ab3015</td>
<td>%s failed to process request: 0x%x: %s</td>
<td>An error occurred when the specified PDOS daemon attempted to process the request from the pdosctl command.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35ab3016</td>
<td>Unable to shutdown %s: 0x%x: %s</td>
<td>An error occurred when the pdosctl command was shutting down the specified PDOS daemon.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35ab3017</td>
<td>Unable to determine status of %s: 0x%x: %s</td>
<td>An error occurred when the pdosctl command queried the status of the specified PDOS daemon.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35ab3018</td>
<td>Unable to set audit level for %s: 0x%x: %s</td>
<td>An error occurred when the pdosctl command was setting the audit level of the specified PDOS daemon.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35ab3019</td>
<td>Unable to determine global audit setting: 0x%x: %s</td>
<td>An error occurred when the pdosctl command queried the audit level of the PDOSD daemon.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35ab301a</td>
<td>Unable to change global warning mode: 0x%x: %s</td>
<td>An error occurred when the pdosctl command was setting the global warning mode of the PDOSD daemon.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35ab301b</td>
<td>Unable to determine global warning mode: 0x%x: %s</td>
<td>An error occurred when the pdosctl command queried the global warning mode of the PDOSD daemon.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35ab301c</td>
<td>Could not set trace level for %s: 0x%x: %s</td>
<td>An error occurred when the pdosctl command was setting the trace level of the specified PDOS daemon.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35ab301d</td>
<td>Unable to determine trace levels for requested daemons: 0x%x: %s</td>
<td>An error occurred when the pdosctl command queried the trace level of the requested PDOS daemons.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35ab301e</td>
<td>Could not send status request message to %s: 0x%x: %s</td>
<td>An error occurred when the pdosctl command attempted to send a status control message to the specified PDOS daemon.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35ab301f</td>
<td>Could not put data to status request message for %s: 0x%x: %s</td>
<td>An error occurred when the pdosctl command was creating the data structure that is used to send a status control message to the specified PDOS daemon.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
</tbody>
</table>
0x35ab3020  Could not get body of status response message from %s: 0x%x: %s
Explanation: An error occurred when the pdosctl command was receiving the response to a status control message from the specified PDOS daemon.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab3021  Received an invalid response to a status message from %s: class: %d fmt: %d msg: %d
Explanation: The pdosctl command received an invalid response to a status control message from the specified PDOS daemon.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab3022  Could not get header of status response message from %s: 0x%x: %s
Explanation: An error occurred when the pdosctl command was receiving the response to a status control message from the specified PDOS daemon.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab3023  %s is initializing
Explanation: Response from the pdosctl command indicating that the specified PDOS daemon is initializing.
Action: None

0x35ab3024  %s trace level set to %s
Explanation: Response from the pdosctl command displaying the current trace level of the specified PDOS daemon after setting it.
Action: None

0x35ab3025  %s is running normally
Explanation: Response from the pdosctl command indicating that the specified PDOS daemon is running under normal conditions.
Action: None

0x35ab3026  %s is running under abnormal conditions:
Explanation: Response from the pdosctl command indicating that the specified PDOS daemon is running under abnormal conditions.
Action: Examine the messages that follow to determine the abnormal conditions that exist. Correct the problems and restart the daemon if necessary.

0x35ab3027  isolated from the master policy server
Explanation: Response from the pdosctl command indicating that the specified PDOS daemon is running but it cannot communicate with the Policy Director authorization server.
Action: Verify that network connectivity exists to the Policy Director authorization server and correct any communication problems. Check that the authorization server is in a valid state and correct any errors.

0x35ab3028  isolated from the user registry
Explanation: Response from the pdosctl command indicating that the specified PDOS daemon is running but it cannot communicate with the Policy Director user registry.
Action: Verify that network connectivity exists to the Policy Director user registry and correct any communication problems. Check that the user registry is in a valid state and correct any errors.

0x35ab3029  %s is shutting down
Explanation: Response from the pdosctl command indicating that the specified PDOS daemon is currently shutting down.
Action: None

0x35ab302a  %s is in an unexpected state: 0x%x
Explanation: Response from the pdosctl command indicating that the specified PDOS daemon is currently in an unknown state.
Action: Examine the log associated with the specified daemon to identify the problems that exist. Take the appropriate action to correct the problems.

0x35ab302b  %s has no trace levels set
Explanation: Response from the pdosctl command indicating that there are no trace levels set for the specified PDOS daemon.
Action: None
0x35ab302c %s trace level set to %s
Explanation: Response from the pdosctl command displaying the current trace level of the specified PDOS daemon.
Action: None

0x35ab3032 %s has the following audit levels on: %s
Explanation: Response from the pdosctl displaying the current audit level of the specified PDOS daemon.
Action: None

0x35ab302d Could not send audit request message to %s: 0x%x: %s
Explanation: An error occurred when the pdosctl command attempted to send an audit control message to the specified PDOS daemon.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab3033 Could not send warning mode change request message to %s: 0x%x: %s
Explanation: An error occurred when the pdosctl command attempted to send a warning mode change control message to the specified PDOS daemon.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab302e Could not put data to audit request message for %s: 0x%x: %s
Explanation: An error occurred when the pdosctl command was creating the data structure that is used to send an audit control message to the specified PDOS daemon.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab3034 Could not put data to warning request message for %s: 0x%x: %s
Explanation: An error occurred when the pdosctl command was creating the data structure that is used to send a warning mode change control message to the specified PDOS daemon.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab302f Could not get body of audit response message from %s: 0x%x: %s
Explanation: An error occurred when the pdosctl command was receiving the response to an audit control message from the specified PDOS daemon.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab3035 Could not get body of warning response message from %s: 0x%x: %s
Explanation: An error occurred when the pdosctl command was receiving the response to a warning mode change control message from the specified PDOS daemon.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab3030 Received an invalid response to a audit message from %s: class: %d fmt: %d msg: %d fmt %d
Explanation: The pdosctl command received an invalid response to an audit control message from the specified PDOS daemon.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab3036 Received an invalid response to a warning mode message from %s: class: %d fmt: %d msg: %d fmt %d
Explanation: The pdosctl command received an invalid response to a warning mode change control message from the specified PDOS daemon.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab3031 Could not get header of audit response message from %s: 0x%x: %s
Explanation: An error occurred when the pdosctl command was receiving the response to an audit control message from the specified PDOS daemon.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab3037 Could not get header of warning mode response message from %s: 0x%x: %s
Explanation: An error occurred when the pdosctl command was receiving the response to a warning mode change control message from the specified PDOS daemon.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.
**0x35ab3038**  The global warning mode setting is %s

**Explanation:** Response from the pdosctl command displaying the global warning mode setting.

**Action:** None

**0x35ab3039**  Daemon did not terminate within timeout period

**Explanation:** The PDOS daemon did not complete its shut down processing within the expected time period.

**Action:** Examine additional messages to determine if there is a problem or if the PDOS daemon is just slow in shutting down. If the problem persists, contact IBM Customer Support.

**0x35ab303a**  %s did not terminate within %d seconds

**Explanation:** The PDOS daemon did not complete its shut down processing within the time period specified.

**Action:** Examine additional messages in the PDOS daemon log file to determine if there is a problem or if the PDOS daemon is just slow in shutting down. If the problem persists, contact IBM Customer Support.

**0x35ab303b**  Unable to determine global audit setting of %s: 0x%x: %s

**Explanation:** An error occurred when the pdosctl command queried the audit level of the specified PDOS daemon.

**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

**0x35ab303c**  Unable to change global warning mode of %s: 0x%x: %s

**Explanation:** An error occurred when the pdosctl command was setting the global warning mode of the specified PDOS daemon.

**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

**0x35ab303d**  Unable to determine global warning mode of %s: 0x%x: %s

**Explanation:** An error occurred when the pdosctl command queried the global warning mode of the specified PDOS daemon.

**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

**0x35ab303e**  Unable to determine trace level of %s: 0x%x: %s

**Explanation:** An error occurred when the pdosctl command queried the trace level of the specified PDOS daemon.

**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

**0x35ab3064**  Usage: pdosunauth [-Vvh?] [-t trace-string] [command]

**Explanation:** pdosunauth command usage statement.

**Action:** None

**0x35ab3066**  Executing: %s

**Explanation:** Message from the pdosunauth command showing that the command that it is executing with unauthenticated credentials.

**Action:** None

**0x35ab3067**  Could not execute command %s: %d: %s

**Explanation:** An error occurred when the pdosunauth command attempted to execute the specified command.

**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

**0x35ab3068**  Cannot unauthenticate when no command specified and the SHELL environment variable is not set.

**Explanation:** The SHELL environment variable must be set in order to spawn a new shell from the pdosunauth command.

**Action:** Set the SHELL environment variable appropriately and retry the command.

**0x35ab3069**  Unable to adopt the unauthenticated identity: 0x%x: %s

**Explanation:** An error occurred when the pdosunauth command attempted to modify its environment to execute as an unauthenticated user.

**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.
<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x35ab30c8</td>
<td>Usage: pdosrefresh [-Vvh?] [-t trace-string] [-u uid] [-u uid ...] [-n name] [-n name ...]</td>
</tr>
<tr>
<td>Explanation:</td>
<td>pdosrefresh command usage statement.</td>
</tr>
<tr>
<td>Action:</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x35ab30c9</td>
<td>There is no need to refresh unauthenticated credentials.</td>
</tr>
<tr>
<td>Explanation:</td>
<td>The pdosrefresh command was executed from an unauthenticated environment that was created using the pdosunauth command. Unauthenticated credentials are not cached so there is nothing to refresh.</td>
</tr>
<tr>
<td>Action:</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x35ab30ca</td>
<td>Unable to refresh the credentials of the invoker: 0x%x : %s</td>
</tr>
<tr>
<td>Explanation:</td>
<td>An error occurred when the pdosrefresh command was refreshing the credentials of the invoking user.</td>
</tr>
<tr>
<td>Action:</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x35ab30cb</td>
<td>The credential of the invoker has been refreshed.</td>
</tr>
<tr>
<td>Explanation:</td>
<td>The pdosrefresh command has refreshed the credentials of the invoking user.</td>
</tr>
<tr>
<td>Action:</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x35ab30cc</td>
<td>Unable to refresh the credential of the user, %s: 0x%x : %s</td>
</tr>
<tr>
<td>Explanation:</td>
<td>An error occurred when the pdosrefresh command was refreshing the credentials of the specified user.</td>
</tr>
<tr>
<td>Action:</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x35ab30cd</td>
<td>The credential of the user, %s, has been refreshed.</td>
</tr>
<tr>
<td>Explanation:</td>
<td>The pdosrefresh command has refreshed the credentials of the specified user.</td>
</tr>
<tr>
<td>Action:</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x35ab30ce</td>
<td>Unable to refresh the credential for the uid, %lld: 0x%x : %s</td>
</tr>
<tr>
<td>Explanation:</td>
<td>An error occurred when the pdosrefresh command was refreshing the credentials of the specified UID.</td>
</tr>
<tr>
<td>Action:</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x35ab30cf</td>
<td>The credential for UID %lld has been refreshed.</td>
</tr>
<tr>
<td>Explanation:</td>
<td>The pdosrefresh command has refreshed the credentials of the specified UID.</td>
</tr>
<tr>
<td>Action:</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x35ab30d0</td>
<td>Unable to refresh the credential: 0x%x: %s</td>
</tr>
<tr>
<td>Explanation:</td>
<td>An error occurred when the pdosrefresh command was refreshing credentials.</td>
</tr>
<tr>
<td>Action:</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x35ab312c</td>
<td>Usage: pdosdestroy [-Vvh?] [-t trace-string] [-u uid] [-u uid ...] [-n name] [-n name ...]</td>
</tr>
<tr>
<td>Explanation:</td>
<td>pdosdestroy command usage statement.</td>
</tr>
<tr>
<td>Action:</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x35ab312e</td>
<td>There is no need to destroy unauthenticated credentials.</td>
</tr>
<tr>
<td>Explanation:</td>
<td>The pdosdestroy command was executed from an unauthenticated environment that was created using the pdosunauth command. Unauthenticated credentials are not cached so there is nothing to destroy.</td>
</tr>
<tr>
<td>Action:</td>
<td>None</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x35ab312f</td>
<td>Unable to destroy the credential: 0x%x: %s</td>
</tr>
<tr>
<td>Explanation:</td>
<td>An error occurred that prevented the pdosdestroy command from removing a credential from the PDOS Credential Cache.</td>
</tr>
<tr>
<td>Action:</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
</tbody>
</table>
0x35ab3130 Unable to destroy the credential of the invoker: 0x%x : %s

Explanation: An error occurred when the pdosdestory command was removing the credentials of the invoking user from the PDOS Credential Cache.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab3131 The credential of the invoker has been destroyed.

Explanation: The pdosdestory command has removed the credentials of the invoking user from the PDOS Credential Cache.

Action: None

0x35ab3132 Unable to destroy the credential of the user, %s: 0x%x : %s

Explanation: An error occurred when the pdosdestory command was removing the credentials of the specified user from the PDOS Credential Cache.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab3133 The credential of the user, %s, has been destroyed.

Explanation: The pdosdestory command has removed the credentials of the specified user from the PDOS Credential Cache.

Action: None

0x35ab3134 Unable to destroy the credential for the uid, %lld: 0x%x : %s

Explanation: An error occurred when the pdosdestory command was removing the credentials of the specified UID from the PDOS Credential Cache.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab3135 The credential for UID %lld has been destroyed.

Explanation: The pdosdestory command has removed the credentials of the specified UID from the PDOS Credential Cache.

Action: None

0x35ab3137 Unable to determine the ID of the invoker: 0x%x : %s

Explanation: An error occurred when retrieving the invoking accessor's ID.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab3139 Usage: pdoswhoami [-Vvh?] [-t trace-string] [-{n|a|l}]

Explanation: pdoswhoami command usage statement.

Action: None

0x35ab313a Unauthenticated.

Explanation: Response from the pdoswhoami command when the invoking user is running with unauthenticated credentials.

Action: None

0x35ab313b Unable to map UID %lld to a user name: 0x%x : %s

Explanation: An error occurred when the pdoswhoami command was mapping the specified UID to a user name.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab313c %lld %s

Explanation: Response from the pdoswhoami command.

Action: None

0x35ab313d %s

Explanation: Response from the pdoswhoami command.

Action: None

0x35ab313e %lld

Explanation: Response from the pdoswhoami command.

Action: None

0x35ab313f Could not get the credential of the invoker: 0x%x : %s

Explanation: An error occurred when the pdoswhoami command attempted to retrieve the credential for the invoking user.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.
Could not send a credential control message to pdosd: 0x%x: %s

Explanation: An error occurred when the command attempted to send a credential control message to the PDOSD daemon.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Error in sending the control credential message to pdosd 0x%x: %s

Explanation: An error occurred when the command was creating the data structure that is used to send a credential control message to the PDOSD daemon.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Could not get the body of credential control response message from pdosd: 0x%x: %s

Explanation: An error occurred when the command was receiving the response to a credential control message from the PDOSD daemon.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Could not get header of credential control response message from pdosd: 0x%x: %s

Explanation: An error occurred when the command was receiving the response to a credential control message from the PDOSD daemon.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Unable to determine the ID of the invoker: 0x%x: %s

Explanation: An error occurred when the pdoswhoami command was retrieving the invoking user’s accessor ID.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Usage: pdoswhois [-Vvh?] [-t trace-string] [-l] pid [pid [pid ...]] Process ID(s) must be specified last.

Explanation: pdoswhois command usage statement.

Action: None

The process with pid, %d, is running as unauthenticated.

Explanation: Response message from the pdoswhois command when the queried process is running with unauthenticated credentials.

Action: None

Process ID is missing.

Explanation: The Process ID is missing from the pdoswhois command line.

Action: Verify the proper syntax of the pdoswhois command line. Correct the problem and retry the pdoswhois command.

Pid, %d, is running under the UID = %ld, user name = %s.

Explanation: Response message from the pdoswhois command when the queried process is running with authenticated credentials.

Action: None

The credential is associated with the following groups:

Explanation: Response message from the pdoswhois and pdoswhoami commands.

Action: None

%ls

Explanation: Response message from the pdoswhois and pdoswhoami commands.

Action: None
0x35ab31fc The credential was last refreshed at %s
Explanation: Response message from the pdoswhois and pdoswhoami commands.
Action: None

0x35ab31fd The credential refresh time expires at %s
Explanation: Response message from the pdoswhois and pdoswhoami commands.
Action: None

0x35ab31fe The credential was last accessed at %s
Explanation: Response message from the pdoswhois and pdoswhoami commands.
Action: None

0x35ab31ff The credential hold time expires at %s
Explanation: Response message from the pdoswhois and pdoswhoami commands.
Action: None

0x35ab3200 The credential refresh time never expires.
Explanation: Response message from the pdoswhois and pdoswhoami commands.
Action: None

0x35ab3201 The credential hold time never expires.
Explanation: Response message from the pdoswhois and pdoswhoami commands.
Action: None

0x35ab3202 Could not get the credential for the process, %d : 0x%x: %s
Explanation: An error occurred when the pdoswhois command was retrieving the credentials for the specified process.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab3203 Could not get the credential: 0x%x: %s
Explanation: An error occurred when the pdoswhois command was retrieving the credentials for the process.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab3204 The credential does not have any group membership associated with it.
Explanation: Response message from the pdoswhois and pdoswhoami commands.
Action: None

0x35ab3205 Unable to determine the UID of the process %d: 0x%x: %s
Explanation: An error occurred when the pdoswhois command was retrieving the accessor ID for the specified process.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab3208 Usage: pdosexempt [-Vvh?] [-t trace-string] [-i] [pid [pid ...]] If process IDs are specified, they have to be specified last.
Explanation: pdosexempt command usage statement.
Action: None

0x35ab3209 Arguments must be valid process IDs: "%s" is invalid.
Explanation: The argument to the pdosexempt command must be a valid numerical process ID.
Action: Verify the proper syntax of the pdosexempt command. Correct the problem and retry the pdosexempt command.

0x35ab320a -i option is valid only when particular process IDs are specified.
Explanation: The -i option to the pdosexempt command can only be specified in conjunction with one or more process IDs.
Action: Verify the proper syntax of the pdosexempt command. Correct the problem and retry the pdosexempt command.
Could not make privileged ID exempt: 0x%x: %s

Explanation: An error occurred when the pdosexempt command attempted to disable PDOS authorization decisions for the OSSEAL privileged user, osseal.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

User %s (uid %lld) is now exempt from PDOS policy.

Explanation: The pdosexempt command has disabled PDOS authorization decisions for all processes running under the specified user ID.

Action: None

The PDOS privileged ID is now exempt from PDOS policy.

Explanation: The pdosexempt command has disabled PDOS authorization decisions for all processes running under the OSSEAL privileged user, osseal.

Action: None

UID %lld is now exempt from PDOS policy.

Explanation: The pdosexempt command has disabled PDOS authorization decisions for all processes running under the specified UID.

Action: None

Unable to map UID %lld to a user name: 0x%x: %s

Explanation: An error occurred when the pdosexempt command was mapping the specified UID to a user name.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Process %d is now exempt from PDOS policy.

Explanation: The pdosexempt command has disabled PDOS authorization decisions for the specified process ID.

Action: None

Process %d and any future children are now exempt from PDOS policy.

Explanation: The pdosexempt command has disabled PDOS authorization decisions for the specified process ID and all of its future child processes.

Action: None

Process %d was not found.

Explanation: The pdosexempt command was unable to disable PDOS authorization decisions for the specified process ID because it was not found.

Action: Retry the pdosexempt command using the correct process ID.

Could not make process %d exempt: 0x%x: %s

Explanation: An error occurred when the command attempted to disable PDOS authorization decisions for the specified process.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Unable to determine privileged ID: 0x%x: %s

Explanation: An error occurred when the pdosexempt command was retrieving the newly exempt accessor ID.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Usage: pdosrevoke [-Vvh?] [-t trace-string] [pid [pid ...]] If process IDs are specified, they have to be specified last.

Explanation: pdosrevoke command usage statement.

Arguments must be valid process IDs: "%s" is invalid.

Explanation: The argument to the pdosrevoke command must be a valid numerical process ID.

Action: Verify the proper syntax of the pdosrevoke command. Correct the problem and retry the pdosrevoke command.
Could not revoke exemption for privileged ID: 0x%x: %s

Explanation: An error occurred when the pdosrevoke command attempted to revoke the exemption from PDOS authorization decisions for the OSSEAL privileged user, osseal, that was previously granted with the pdosexempt command.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Process %d is no longer exempt from PDOS policy.

Explanation: The pdosrevoke command revoked the exemption from PDOS authorization decisions for the specified process ID.

Action: None

Could not revoke exemption for privileged process %d: 0x%x: %s

Explanation: An error occurred when the pdosrevoke command attempted to revoke the exemption from PDOS authorization decisions for the specified process ID.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Process %d was not found.

Explanation: The pdosrevoke command was unable to revoke the exemption from PDOS authorization decisions for the specified process ID because it was not found.

Action: Retry the pdosrevoke command using the correct process ID.

User %s (uid %lld) is no longer exempt from PDOS policy.

Explanation: The pdosrevoke command revoked the exemption from PDOS authorization decisions for all processes running under the specified user ID.

Action: None

The PDOS privileged ID is no longer exempt from PDOS policy.

Explanation: The pdosrevoke command revoked the exemption from PDOS authorization decisions for all processes running under the OSSEAL privileged user, osseal.

Action: None

UID %lld is no longer exempt from PDOS policy.

Explanation: The pdosrevoke command revoked the exemption from PDOS authorization decisions for all processes running under the specified user ID.

Action: None

Unable to map UID %lld to a user name: 0x%x: %s

Explanation: An error occurred when the pdosrevoke command was mapping the specified UID to a user name.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Unable to determine privileged ID: 0x%x: %s

Explanation: An error occurred when the pdosrevoke command was retrieving the accessor ID of the OSSEAL privileged user, osseal.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Usage: pdosuidprog -l [-H] [-s] [-x directory [-x directory ...]] [directories [directories ...]]
pdosuidprog -g [-c { Login-Programs | Secure-files | Secure-Programs | Impersonator-Programs | Immune-Programs } [-H] [-s] [-p policy-branch] [-x directory [-x directory ...]] [directories [directories ...]]
pdosuidprog [-Vvh?] [-t trace-string]

Explanation: pdosuidprog command usage statement.

Action: None

An error occurred in opening the directory, %s: %d: %s.

Explanation: An error occurred when the pdosuidprog command attempted to open the specified directory to read its contents.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.
0x35ab3322 %s : %d : %d
Explanation: Output from the pdosuidprog command for a program that is both a setuid and setgid program.
Action: None

0x35ab3323 %s : %d
Explanation: Response from the pdosuidprog command for a program that is a setuid program.
Action: None

0x35ab3324 %s : : %d
Explanation: Response from the pdosuidprog command for a program that is a setgid program.
Action: None

0x35ab3325 The directory, %s, is in the exclude list of directories.
Explanation: Response from the pdosuidprog command listing a directory that is excluded from the search.
Action: None

0x35ab3385 Usage: pdossudo [-Vvh?] [-t trace-string] command-alias [arg [arg ...]]
Explanation: pdossudo command usage statement.
Action: None

0x35ab3386 The command alias is missing.
Explanation: The command alias is missing from the pdossudo command line.
Action: Verify the proper syntax of the pdossudo command. Correct the problem and retry the pdossudo command.

0x35ab3387 The user is not authorized to execute the Sudo command alias.
Explanation: The pdossudo command failed because the invoking user does not have the required authorization to execute the Sudo command alias.
Action: Verify that the PDOS Sudo policy is correct and retry the pdossudo command as a user who is authorized to execute the Sudo command.

0x35ab3388 Executing: %s
Explanation: Response from the pdossudo command showing the Sudo command alias that it is executing.
Action: None

0x35ab3389 Could not execute command %s: %d: %s
Explanation: An error occurred when the pdossudo command attempted to execute the real command represented by the Sudo command alias.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab338a pdossudo command failed: 0x%x: %s
Explanation: An error occurred when processing the pdossudo command.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab338b Could not set the environment variable: %d: %s
Explanation: An error occurred when the pdossudo command was setting an environment variable.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab338c Unable to determine UID of the process: 0x%x: %s
Explanation: An error occurred when the pdossudo command was retrieving the invoking user’s accessor ID.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab338d Unable to get the Protected Object Name of the process: 0x%x: %s
Explanation: An error occurred when the pdossudo command queried the PDOS kernel policy cache for the Protected Object Name of the running process.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.
0x35ab338e The password entered is invalid.
Explanation: The user entered an incorrect password.
Action: Retry the pdossudo command using the correct password.

0x35ab338f Could not get the password from the user: 
%d : %s
Explanation: An error occurred when the pdossudo command attempted to read the user’s password.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab3390 Enter your password:
Explanation: Prompt from the pdossudo command for the user to enter their own password.
Action: Enter the correct password.

0x35ab3391 Enter the password for the user, %s:
Explanation: Prompt from the pdossudo command for the user to enter the password for the Sudo target user.
Action: Enter the correct password for the target user.

0x35ab3392 Could not get body of the sudo response message from pdosd daemon: 0x%x: %s
Explanation: An error occurred when the pdossudo command was receiving the response to a Sudo control message from the PDOSD daemon.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab3393 Could not get header of sudo response message from pdosd daemon 0x%x: %s
Explanation: An error occurred when the pdossudo command was receiving the response to a Sudo control message from the PDOSD daemon.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab3394 Could not get all requested data from sudo response. Requested data = %u, Got = %u.
Explanation: An error occurred when the pdossudo command was receiving the response to a Sudo control message from the PDOSD daemon.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab3395 Could not get %u bytes from sudo response: 0x%x: %s
Explanation: An error occurred when the pdossudo command was receiving the response to a Sudo control message from the PDOSD daemon.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab3396 Could not set the target UID for the sudo: %lld: %d: %s
Explanation: An error occurred when the pdossudo command attempted to switch to the specified UID.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35ab3397 Received an invalid sudo response from the pdosd daemon: cla ss: %d fmt: %d msg: %d fmt %d
Explanation: The response from the PDOSD daemon to a Sudo request contains invalid data.
Action: Contact IBM Customer Support.

0x35ab3398 Command alias is not a recognized Sudo command.
Explanation: The command alias that was specified on the pdossudo command line is not registered in the PDOS policy as a Sudo command.
Action: Retry the pdossudo command using the correct Sudo command.

0x35ab3399 The command alias %s is not a recognized Sudo command.
Explanation: The command alias that was specified on the pdossudo command line is not registered in the PDOS policy as a Sudo command.
Action: Retry the pdossudo command using the correct Sudo command.
Unable to get the password information from the system authentication database for the user, %s: %x: %s

Explanation: An error occurred when the pdossudo command attempted to retrieve the user's password from the system user registry for comparison with the password entered by the user.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Unable to map UID %u to name: %x: %s

Explanation: An error occurred while mapping the UID to a user name.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Unable to map name %s to UID: %x: %s

Explanation: An error occurred while mapping the user name to a UID.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Unable to become a privileged process: %x: %s

Explanation: The command failed when it attempted to temporarily become an OSSEAL privileged process.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Unable to revoke privilege: %x: %s

Explanation: The command failed when it attempted to revoke the temporary privilege that it was granted when it became an OSSEAL privileged process.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Unable to create the Policy Director context

Explanation: An error occurred when the pdosrgyimp command attempted to initiate contact with the Policy Director Management Server.

Action: Verify that the Policy Director Run Time Environment is properly configured. Examine additional messages to determine the cause of the failure and correct the problem.

failed to create the Policy Director context

Explanation: An error occurred when the pdosrgyimp command attempted to terminate contact with the Policy Director Management Server.

Action: Examine additional messages to determine the cause of the failure and correct the problem.

The group already exists in PD

Explanation: The pdosrgyimp command attempted to create a new group in the Policy Director user registry but a group by the same name already exists.

Action: Determine if this conflict needs to be resolved and take action accordingly.

The group already exists in LDAP

Explanation: The pdosrgyimp command attempted to create a new group in the Policy Director user registry but a group by the same name already exists in the LDAP registry but not in the Policy Director user registry.

Action: Determine if this conflict needs to be resolved and take action accordingly.

Unable to create the new group

Explanation: An error occurred when the pdosrgyimp command tried to create a new group in the Policy Director user registry.

Action: Examine additional messages to determine the cause of the failure and correct the problem.

group DN exists in LDAP, unable to import

Explanation: An error occurred when the pdosrgyimp command tried to import a group from the LDAP registry into the Policy Director user registry.

Action: Examine additional messages to determine the cause of the failure and correct the problem.

group DN exists in LDAP, unable to import because the cn's do not match

Explanation: An error occurred when the pdosrgyimp command tried to import a group from the LDAP registry into the Policy Director user registry. The common name of the group in the LDAP registry does not match the common name of the group that the pdosrgyimp command expects.

Action: Resolve this conflict and take action accordingly.
**0x35ab33f0**  group DN exists in LDAP, import failed

**Explanation:**  An error occurred when the pdosrgyimp command tried to import a group from the LDAP registry into the Policy Director user registry.

**Action:**  Examine additional messages to determine the cause of the failure and correct the problem.

---

**0x35ab33f1**  The user already exists in PD

**Explanation:**  The pdosrgyimp command attempted to create a new user in the Policy Director user registry but a user by the same name already exists.

**Action:**  Determine if this conflict needs to be resolved and take action accordingly.

---

**0x35ab33f2**  The user already exists in LDAP

**Explanation:**  The pdosrgyimp command attempted to create a new user in the Policy Director user registry but a user by the same name already exists in the LDAP registry but not in the Policy Director user registry.

**Action:**  Determine if this conflict needs to be resolved and take action accordingly.

---

**0x35ab33f3**  Unable to create the new user

**Explanation:**  An error occurred when the pdosrgyimp command tried to create a new user in the Policy Director user registry.

**Action:**  Examine additional messages to determine the cause of the failure and correct the problem.

---

**0x35ab33f4**  user DN exists in LDAP, unable to import

**Explanation:**  An error occurred when the pdosrgyimp command tried to import a user from the LDAP registry into the Policy Director user registry.

**Action:**  Examine additional messages to determine the cause of the failure and correct the problem.

---

**0x35ab33f5**  user DN exists in LDAP, unable to import because the sn’s do not match

**Explanation:**  An error occurred when the pdosrgyimp command tried to import a user from the LDAP registry into the Policy Director user registry. The surname of the user in the LDAP registry does not match the surname of the user that the pdosrgyimp command expects.

**Action:**  Resolve this conflict and take action accordingly.

---

**0x35ab33f6**  user DN exists in LDAP, unable to import

**Explanation:**  An error occurred when the pdosrgyimp command tried to import a user from the LDAP registry into the Policy Director user registry. The surname of the user in the LDAP registry does not match the surname of the user that the pdosrgyimp command expects.

**Action:**  Resolve this conflict and take action accordingly.

---

**0x35ab33f7**  user DN exists in LDAP, import failed

**Explanation:**  An error occurred when the pdosrgyimp command tried to import a user from the LDAP registry into the Policy Director user registry.

**Action:**  Examine additional messages to determine the cause of the failure and correct the problem.

---

**0x35ab33f8**  The call to set the Policy Director description failed

**Explanation:**  An error occurred when the pdosrgyimp command tried to set the description of the user in the Policy Director user registry.

**Action:**  Examine additional messages to determine the cause of the failure and correct the problem. The pdadmin command can be used to modify the user’s description.

---

**0x35ab33f9**  The call to set the Policy Director password invalid failed

**Explanation:**  An error occurred when the pdosrgyimp command tried to set the user’s password to invalid in the Policy Director user registry.

**Action:**  Examine additional messages to determine the cause of the failure and correct the problem. The pdadmin command can be used to set the user’s password to invalid.

---

**0x35ab33fa**  The call to set the Policy Director account valid failed

**Explanation:**  An error occurred when the pdosrgyimp command tried to mark the user’s account valid in the Policy Director user registry.

**Action:**  Examine additional messages to determine the cause of the failure and correct the problem. The pdadmin command can be used to set the user’s account to valid.
0x35ab33fb  The call to set the Policy Director account
invalid failed

Explanation: An error occurred when the pdosrgyimp
command tried to mark the user’s account invalid in the Policy
Director user registry.

Action: Examine additional messages to determine the cause
of the failure and correct the problem. The padmin command
can be used to set the user’s account to invalid.

0x35ab33fc  The group was not found in the UNIX
registry

Explanation: The group does not exist in the UNIX registry.

Action: Create the group in the UNIX registry if it does not
exist. If the group already exists in the UNIX registry, contact
IBM Customer Support.

0x35ab33fd  create group

Explanation: Comment in a pdosrgyimp log file delimiting a
successful group create command.

Action: None.

0x35ab33fe  create group failed

Explanation: Comment in a pdosrgyimp log file delimiting a
failed group create command.

Action: Examine error messages from the pdosrgyimp
command along with the UNIX and Policy Director user
registries to determine the appropriate action.

0x35ab33ff  create group failed - group already exists in
LDAP

Explanation: Comment in a pdosrgyimp log file delimiting a
failed group create command for a group that already exists in
the LDAP registry but not in the Policy Director user registry.

Action: Examine error messages from the pdosrgyimp
command along with the UNIX and Policy Director user
registries to determine the appropriate action.

0x35ab3401  create group failed - group already exists -
refreshing members

Explanation: Comment in a pdosrgyimp log file delimiting a
failed group create command for a group that already exists in
the Policy Director user registry. This also indicates that the
existing group membership will be refreshed to include
members from the current pdosrgyimp command invocation.

Action: Examine error messages from the pdosrgyimp
command along with the UNIX and Policy Director user
registries to determine the appropriate action.

0x35ab3402  create default group failed - group already
exists - populating new members

Explanation: Comment in a pdosrgyimp log file delimiting a
failed group create command for a group that already exists in
the Policy Director user registry. This also indicates that the
existing group membership will be refreshed to include
members from the current pdosrgyimp command invocation.

Action: Examine error messages from the pdosrgyimp
command along with the UNIX and Policy Director user
registries to determine the appropriate action.

0x35ab3403  import LDAP group

Explanation: Comment in a pdosrgyimp log file delimiting a
successful group import from LDAP command.

Action: None

0x35ab3404  import LDAP group failed

Explanation: Comment in a pdosrgyimp log file delimiting a
failed group import from LDAP command.

Action: Examine error messages from the pdosrgyimp
command along with the UNIX and Policy Director user
registries to determine the appropriate action.

0x35ab3405  group modify add member failed

Explanation: Comment in a pdosrgyimp log file delimiting a
failed group add member command.

Action: Examine error messages from the pdosrgyimp
command along with the UNIX and Policy Director user
registries to determine the appropriate action.

0x35ab3406  create user

Explanation: Comment in a pdosrgyimp log file delimiting a
successful user create command.

Action: None
create user failed
Explanation: Comment in a pdosrgyimp log file delimiting a failed user create command.
Action: Examine error messages from the pdosrgyimp command along with the UNIX and Policy Director user registries to determine the appropriate action.

create user failed - user already exists in LDAP
Explanation: Comment in a pdosrgyimp log file delimiting a failed user create command for a user that already exists in the LDAP registry but not in the Policy Director user registry.
Action: Examine error messages from the pdosrgyimp command along with the UNIX and Policy Director user registries to determine the appropriate action.

create user failed - user already exists
Explanation: Comment in a pdosrgyimp log file delimiting a failed user create command for a user that already exists in the Policy Director user registry.
Action: Examine error messages from the pdosrgyimp command along with the UNIX and Policy Director user registries to determine the appropriate action.

import LDAP user
Explanation: Comment in a pdosrgyimp log file delimiting a successful user import from LDAP command.
Action: None

import LDAP user failed
Explanation: Comment in a pdosrgyimp log file delimiting a failed user import from LDAP command.
Action: Examine error messages from the pdosrgyimp command along with the UNIX and Policy Director user registries to determine the appropriate action.

modify user description failed
Explanation: Comment in a pdosrgyimp log file delimiting a failed user modify description command.
Action: Examine error messages from the pdosrgyimp command along with the UNIX and Policy Director user registries to determine the appropriate action.

set password invalid failed
Explanation: Comment in a pdosrgyimp log file delimiting a failed user modify password-valid command.
Action: Examine error messages from the pdosrgyimp command along with the UNIX and Policy Director user registries to determine the appropriate action.

set account valid failed
Explanation: Comment in a pdosrgyimp log file delimiting a failed user modify account-valid command.
Action: Examine error messages from the pdosrgyimp command along with the UNIX and Policy Director user registries to determine the appropriate action.

set account invalid failed
Explanation: Comment in a pdosrgyimp log file delimiting a failed user modify account-valid command.
Action: Examine error messages from the pdosrgyimp command along with the UNIX and Policy Director user registries to determine the appropriate action.

Explanation: pdosrgyimp command usage statement.
Action: None

Enter Administrator Password:
Explanation: Prompt from the pdosrgyimp command asking for the Policy Director administrator’s password.
Action: Enter the password for the Policy Director administrator.

Cannot open file %s: 0x%x: %s
Explanation: An error occurred when opening the specified file.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.
The -S option is required
Explanation: The -S option is required by the pdosrgyimp command.
Action: Verify the proper syntax for the pdosrgyimp command. Correct the command and retry the operation.

The -l option is required
Explanation: The -l option is required by the pdosrgyimp command.
Action: Verify the proper syntax for the pdosrgyimp command. Correct the command and retry the operation.

The -p option is required
Explanation: The -p option is required by the pdosrgyimp command.
Action: Verify the proper syntax for the pdosrgyimp command. Correct the command and retry the operation.

Invalid import/export entry: %s
Explanation: An invalid entry was found in either the include file or the exclude file. The invalid entry is ignored by the pdosrgyimp command.
Action: Examine the invalid entry and take corrective action, if necessary.

User %s was not found in the registry - omitting
Explanation: An entry in either the include file or the exclude file specified a user that does not exist in the UNIX registry. This entry is ignored by the pdosrgyimp command.
Action: Examine the invalid user entry and take corrective action, if necessary.

Group %s was not found in the registry - omitting
Explanation: An entry in either the include file or the exclude file specified a group that does not exist in the UNIX registry. This entry is ignored by the pdosrgyimp command.
Action: Examine the invalid group entry and take corrective action, if necessary.

An error occurred while parsing the include file: 0x%x: %s
Explanation: An error occurred when the pdosrgyimp command was parsing the include file.
Action: Use the returned error code and error text to diagnose and correct the problem. Retry the pdosrgyimp command. If the problem persists, contact IBM Customer Support.

An error occurred while parsing the exclude file: 0x%x: %s
Explanation: An error occurred when the pdosrgyimp command was parsing the exclude file.
Action: Use the returned error code and error text to diagnose and correct the problem. Retry the pdosrgyimp command. If the problem persists, contact IBM Customer Support.

An error occurred while adding the default group to the include list: 0x%x: %s
Explanation: An error occurred when the pdosrgyimp command added the default group to an internal list.
Action: Use the returned error code and error text to diagnose and correct the problem. Retry the pdosrgyimp command. If the problem persists, contact IBM Customer Support.

An error occurred while initializing the PD context: 0x%x: %s
Explanation: An error occurred when the pdosrgyimp command attempted to initiate contact with the Policy Director Management Server.
Action: Use the returned error code and error text to diagnose and correct the problem. Retry the pdosrgyimp command. If the problem persists, contact IBM Customer Support.

An error occurred while initializing the password limits: 0x%x: %s
Explanation: An error occurred when the pdosrgyimp command calculated the limits for user passwords in the Policy Director user registry.
Action: Use the returned error code and error text to diagnose and correct the problem. Retry the pdosrgyimp command. If the problem persists, contact IBM Customer Support.

The default password (%s) is not a valid PD password: 0x%x: %s
Explanation: The default password does not meet the password requirements for passwords in the Policy Director user registry.
Action: Use the returned error code and error text to diagnose and correct the problem. Retry the pdosrgyimp command. If the problem persists, contact IBM Customer Support.
0x35ab3421  An error occurred while deleting the PD context: 0x%x: %s  
Explanation: An error occurred when the pdosrgyimp command attempted to terminate contact with the Policy Director Management Server.
Action: Use the returned error code and error text to diagnose and correct the problem. Retry the pdosrgyimp command. If the problem persists, contact IBM Customer Support.

0x35ab3423  An error occurred while scanning the user registry: 0x%x: %s  
Explanation: An error occurred when the pdosrgyimp command attempted to build an internal list of users based on the UNIX user registry.
Action: Use the returned error code and error text to diagnose and correct the problem. Retry the pdosrgyimp command. If the problem persists, contact IBM Customer Support.

0x35ab3424  An error occurred while scanning the group registry: 0x%x: %s  
Explanation: An error occurred when the pdosrgyimp command attempted to build an internal list of groups based on the UNIX user registry.
Action: Use the returned error code and error text to diagnose and correct the problem. Retry the pdosrgyimp command. If the problem persists, contact IBM Customer Support.

0x35ab3425  An error occurred while processing the users: 0x%x: %s  
Explanation: An error occurred while the pdosrgyimp command was importing user entries into the Policy Director user registry.
Action: Use the returned error code and error text to diagnose and correct the problem. Retry the pdosrgyimp command. If the problem persists, contact IBM Customer Support.

0x35ab3426  An error occurred while processing the groups: 0x%x: %s  
Explanation: An error occurred while the pdosrgyimp command was importing group entries into the Policy Director user registry.
Action: Use the returned error code and error text to diagnose and correct the problem. Retry the pdosrgyimp command. If the problem persists, contact IBM Customer Support.

0x35ab3427  An error occurred while importing group (%s): 0x%x: %s  
Explanation: An error occurred when the pdosrgyimp command attempted to create a group in the Policy Director user registry.
Action: Use the returned error code and error text to diagnose and correct the problem. Retry the pdosrgyimp command. If the problem persists, contact IBM Customer Support.

0x35ab3428  An error occurred while populating group (%s): 0x%x: %s  
Explanation: An error occurred when the pdosrgyimp command was populating the group membership of the specified group in the the Policy Director user registry.
Action: Use the returned error code and error text to diagnose and correct the problem. Retry the pdosrgyimp command. If the problem persists, contact IBM Customer Support.

0x35ab3429  An error occurred while adding user (%s) to group (%s)  
Explanation: An error occurred when the pdosrgyimp command attempted to add the specified user to the group in the Policy Director user registry.
Action: Use the returned error code and error text to diagnose and correct the problem. Retry the pdosrgyimp command. If the problem persists, contact IBM Customer Support.

0x35ab342a  Successfully created group %s  
Explanation: The specified group was created in the Policy Director user registry.
Action: None

0x35ab342b  Successfully imported group %s from LDAP  
Explanation: The specified group was imported from the LDAP registry into the Policy Director user registry.
Action: None

0x35ab342c  An error occurred while importing user (%s): 0x%x: %s  
Explanation: An error occurred when the pdosrgyimp command attempted to create a user in the Policy Director user registry.
Action: Use the returned error code and error text to diagnose and correct the problem. Retry the pdosrgyimp command. If the problem persists, contact IBM Customer Support.
Successfully created user `%s`  
**Explanation:** The specified user was created in the Policy Director user registry.  
**Action:** None

Successfully imported user `%s` from LDAP  
**Explanation:** The specified user was imported from the LDAP registry into the Policy Director user registry.  
**Action:** None

**Explanation:** Usage statement  
**Action:** None

Cannot open log file for reading  
**Explanation:** Cannot open the audit log file for reading.  
**Action:** The audit log files are in the /var/pdos/audit directory. Check the file’s UNIX permissions. Also check the PDOS error logs for previous errors. Correct the problem and retry the operation. If the problem persists, contact IBM Customer Support.

%`s` opened for processing.  
**Explanation:** The audit log file is open for processing.  
**Action:** None

Error reading variable data: `%d`  
**Explanation:** An unexpected error occurred reading the variable data in the audit log.  
**Action:** See specified error number for cause of the read problem. Correct the problem and retry the operation. If the problem persists, contact IBM Customer Support.

Error closing input file  
**Explanation:** An unexpected error occurred closing input audit log file.  
**Action:** None

strptime failed - cannot check this record for date: `%s`  
**Explanation:** The date provided could not be converted to a time stamp.  
**Action:** Specify the date and time in the YYYY-MM-DD-hh:mm:ss format.

Timestamp  
**Explanation:** Descriptive label used in the verbose format output from the pdosaudview utility. The value is the time that the audit record was generated.  
**Action:** None

Audit Event  
**Explanation:** Descriptive label used in the verbose format output from the pdosaudview utility. The value is a text string describing the audit event associated with this audit record.  
**Action:** None

Originating Process  
**Explanation:** Descriptive label used in the verbose format output from the pdosaudview utility. The value is the name of the process that generated the audit record.  
**Action:** None

Audit View  
**Explanation:** Descriptive label used in the verbose format output from the pdosaudview utility. The value is the audit view associated with the audit record.  
**Action:** None

Audit Action  
**Explanation:** Descriptive label used in the verbose format output from the pdosaudview utility. The value is the action associated with the audit record. The possible values are Check Access, Add Delete, Change, Retrieve, Apply, Trust, Untrust, Start, Stop, Register, Trace, Isolated, Not Isolated, Login, Logout, Enable, or Disable.  
**Action:** None
0x35adb15f  Audit Reason

Explanation: Descriptive label used in the verbose format output from the pdosaudview utility. The value is the reason why the audit record was generated. Possible values are Global Audit, Resource Audit, Global Warning, or Resource Warning.

Action: None

0x35adb160  Audit Outcome

Explanation: Descriptive label used in the verbose format output from the pdosaudview utility. If the audit record was generated as a result of a action taken due to an error condition, the value is Failure. Otherwise, the value is Success.

Action: None

0x35adb161  Audit Fail Status

Explanation: Descriptive label used in the verbose format output from the pdosaudview utility. If the Audit Outcome field of the audit record is Failure, this field contains an error message or code indicating the error that occurred.

Action: None

0x35adb162  Audit Resource Type

Explanation: Descriptive label used in the verbose format output from the pdosaudview utility. The value is the resource type associated with the audit record. Possible values are Process, TCB, Cred, Policy, Login, File, NetIncoming, NetOutgoing, Surrogate, or Sudo.

Action: None

0x35adb163  Accessor Name

Explanation: Descriptive label used in the verbose format output from the pdosaudview utility. The value is the user name associated with the accessing user’s UID.

Action: None

0x35adb164  Accessor Effective Name

Explanation: Descriptive label used in the verbose format output from the pdosaudview utility. The value is the user name associated with the accessing user’s effective UID.

Action: None

0x35adb165  Running Program Protected Name

Explanation: Descriptive label used in the verbose format output from the pdosaudview utility. The value is the name of the running program as registered in the Trusted Computing Base (TCB). This field only appears in the audit record if the running program is registered in the PDOS TCB.

Action: None

0x35adb166  Running Program System Resource Name

Explanation: Descriptive label used in the verbose format output from the pdosaudview utility. The value is the name of the running program as executed.

Action: None

0x35adb167  Protected Object Name

Explanation: Descriptive label used in the verbose format output from the pdosaudview utility. The value is the protected object name associated with the audit record.

Action: None

0x35adb168  System Resource Name

Explanation: Descriptive label used in the verbose format output from the pdosaudview utility. The value is the system name of the resource associated with the audit record. If the audit resource type is File, this is the name of the file being accessed. If the audit resource type is TCB and the audit action is Trust or Untrust, this is the name of the TCB resource that was marked trusted or untrusted in the Object Signature Database. If the audit resource type is Login and the audit view is Admin and the audit action is Disable or Enable, this is the name of the user account that was enabled or disabled for login.

Action: None

0x35adb169  Accessor Process ID

Explanation: Descriptive label used in the verbose format output from the pdosaudview utility. The value is the process identifier of the running process associated with the audit record.

Action: None

0x35adb170  Originating Location Name

Explanation: The value is the host name of the machine where the audit record was generated.

Action: None
**Sudo Flags**

**Explanation:** Descriptive label used in the verbose format output from the pdosaudview utility. This field is only shown when the audit resource type is Sudo. The value provides information about the Sudo policy such as whether or not the invoker password, the target user password, or both were required before a target command could be executed.

**Action:** None

**Changed Data Attributes Flags**

**Explanation:** Descriptive label used in the verbose format output from the pdosaudview utility. This field is only shown if the audit resource type is TCB. The value provides additional information associated with the Trusted Computing Base (TCB) resource.

**Action:** None

**Policy Epoch**

**Explanation:** Descriptive label used in the verbose format output from the pdosaudview utility. This field is only shown if the audit resource type is Policy. The value provides additional information associated with the Policy audit record.

**Action:** None

**Policy Version Number**

**Explanation:** Descriptive label used in the verbose format output from the pdosaudview utility. This field is only shown if the audit resource type is Policy. The value provides additional information associated with the Policy audit record.

**Action:** None

**START OF NEW RECORD**

**Explanation:** Marks the beginning of a new record in the verbose output of the pdosaudview utility.

**Action:** None

**Cannot determine the size of the audit.log.**

**Explanation:** The pdosaudview utility could not process an audit log file because it could not determine the size of the file.

**Action:** If the problem persists, contact IBM Customer Support.
0x35adb1a4  Surrogate Name

Explanation: Descriptive label used in the verbose format output from the pdosaudview utility. This field is only shown if the Audit Resource Type is Surrogate. The value is the user name or user ID of the target user or the group name or group ID of the target group.

Action: None

0x35adb1a6  Login Location Identifier

Explanation: Descriptive label used in the verbose format output from the pdosaudview utility. This field is only shown if the Audit Resource Type is Login. If the login occurred from a local terminal the value is the terminal name. If the login occurred from a remote system, the value is either the host name or the IP address of the remote system.

Action: None

0x35adb1a7  Protected Resource Specification

Explanation: Descriptive label used in the verbose format output from the pdosaudview utility. This field is only shown if the Audit Resource Type is TraceExec or TraceFile. The value is the protected object name of the program being executed.

Action: None

0x35adb1a8  Accessed Resource Specification

Explanation: Descriptive label used in the verbose format output from the pdosaudview utility. This field is only shown if the Audit Resource Type is TraceExec or TraceFile. For TraceFile records, the value is the name of the file used in the access. For TraceExec records, the value is the name of the file resource as it was specified in the execute operation.

Action: None

0x35adb1a9  Additional Parameters

Explanation: Descriptive label used in the verbose format output from the pdosaudview utility. The value is additional information related to the audit record.

Action: None

0x35adb1aa  Network Remote Host Identifier

Explanation: Descriptive label used in the verbose format output from the pdosaudview utility. This field is only shown if the Audit Resource Type is NetIncoming or NetOutgoing. The value is the name of the remote host where access originated. For NetOutgoing records, the value is the name of the remote host being accessed.

Action: None

0x35adb1ab  Network Protocol

Explanation: Descriptive label used in the verbose format output from the pdosaudview utility. This field is only shown if the Audit Resource Type is NetIncoming or NetOutgoing. The value is the name of the protocol being used in the access.

Action: None

0x35adb1ac  Network Service

Explanation: Descriptive label used in the verbose format output from the pdosaudview utility. This field is only shown if the Audit Resource Type is NetIncoming or NetOutgoing. The value is the service name or port number of the remote network service being accessed.

Action: None

0x35adb1ad  Sudo Command and Arguments

Explanation: Descriptive label used in the verbose format output from the pdosaudview utility. This field is only shown if the Audit Resource Type is Sudo. The value is the target command name and arguments.

Action: None

0x35adb1ae  Sudo User Name

Explanation: Descriptive label used in the verbose format output from the pdosaudview utility. This field is only shown if the Audit Resource Type is Sudo. The value is the target user name that the Sudo target command will be executed as.

Action: None

0x35adb1af  Audit Uniqifier

Explanation: Descriptive label used in the verbose format output from the pdosaudview utility. The value is an integer number that uniquely identifies audit records that occur within the same second.

Action: None

0x35adb1b0  Audit log file cannot be processed because it was created by a previous version of PDOS, with an incompatible audit record format. Record version = %d.

Explanation: The pdosaudview utility encountered an audit.log file in a format that is no longer supported.

Action: The pdosaudview utility cannot process the file because the file format is no longer supported. If you must extract information from this audit.log file, contact IBM Customer Support.
User account is locked

Explanation: Login was prevented because the account is locked.

Action: Request that a PDOS administrator unlock the account using the pdoslpadm utility.

The user password has expired and no further grace logins remain.

Explanation: Login was prevented because the user password has expired and the number of grace logins permitted has been exceeded.

Action: Request that a PDOS administrator unlock the account using the pdoslpadm utility.

Maximum number of concurrent logins reached.

Explanation: Login was prevented because the user is already logged in from the maximum number of terminals allowed by Login Activity Policy.

Action: Log off from one of the currently logged on terminals and retry the login. You also can request that a PDOS administrator increase the maximum number of concurrent logins allowed for the account using the pdoslpadm utility.

Lock time interval has not elapsed.

Explanation: Login was prevented because the user account is locked and the time interval defined by the Login Activity Policy to suspend the account has not yet elapsed.

Action: Request that a PDOS administrator unlock the account using the pdoslpadm utility.

Minimum time interval required between password changes has not elapsed.

Explanation: The password cannot be changed at this time because the minimum time required between password changes has not elapsed.

Action: Wait the required minimum time interval as defined by Login Activity Policy before attempting to change the password. Contact a PDOS administrator if immediate action is required.

User account was unlocked because lock time interval has elapsed.

Explanation: The user account was unlocked because the period of time specified in the Login Activity Policy to suspend an account has elapsed.

Action: None

Maximum number of failed logins reached.

Explanation: Login was prevented because the maximum number of failed logins allowed by the Login Activity Policy has been reached.

Action: Request that a PDOS administrator unlock the account using the pdoslpadm utility.

Maximum inactive days has elapsed.

Explanation: Login was prevented because the maximum number of days allowed by the Login Activity Policy before an inactive account is locked has elapsed.

Action: Request that a PDOS administrator unlock the account using the pdoslpadm utility.

Maximum time interval since last password change has elapsed.

Explanation: Login was prevented because the account password has expired.

Action: Change the password.

Checking login location access control policy.

Explanation: The login location access control policy is being checked.

Action: None

Checking Access-Restrictions associated with login location access control policy.

Explanation: The login location Access-Restrictions attributes associated with login location access control policy are being checked.

Action: None

Checking login holiday access control policy.

Explanation: The login holiday access control policy is being checked.

Action: None

Checking Access-Restrictions associated with login holiday access control policy.

Explanation: The login holiday Access-Restrictions attributes associated with login holiday access control policy are being checked.

Action: None
0x35adb28e Checking time of day login access control policy.

Explanation: The time of day login access control policy is being checked.
Action: None

0x35adb290 Login denied by native authentication method.

Explanation: Login was denied by the native operating system authentication method.
Action: Check the login policy set for the user in the native authentication. Make the required changes to let the native authentication permit the login and retry the operation. If the problem persists, contact IBM Customer Support.

0x35adb291 User account modified by administrative action.

Explanation: User account status was modified by an administrative action.
Action: None

0x35adb292 All login policy checks permitted access.

Explanation: All login policy checks permitted login access.
Action: None

0x35adb293 Checking resource access control policy.

Explanation: The resource access control policy is being checked.
Action: None

0x35adb294 Checking Access-Restrictions associated with resource access control policy.

Explanation: The Access-Restrictions attributes associated with resource access control policy are being checked.
Action: None

0x35adb295 Checking trust state for TCB resource.

Explanation: The trust state for a Trusted Computing Base (TCB) resource is being checked.
Action: None

0x35adb296 Error occurred reading the request message data.

Explanation: An internal service encountered an error while attempting to read the data associated with an authorization request. PDOS policy was not successfully evaluated.
Action: Check the /var/pdos/log/pdosd.log file for additional error messages to help diagnose the problem. If the problem persists, contact IBM Customer Support.

0x35adb297 All resource policy checks permitted access.

Explanation: All resource policy checks permitted access to the resource.
Action: None

0x35adb298 Converting surrogate target ID to name.

Explanation: Surrogate target ID is being converted to a name in order to evaluate Surrogate policy.
Action: None

0x35adb308 Keyword Mapping

Explanation: for mapping of keywords.
Action: None

0x35adb30a Audit Event Mapping

Explanation: Title for mapping of audit events.
Action: None

0x35adb30c View Mapping

Explanation: Title for mapping of views.
Action: None

0x35adb30e Reason Mapping

Explanation: Title for mapping of reasons.
Action: None

0x35adb310 Permission Mapping

Explanation: Title for mapping of permissions.
Action: None
**Qualifier Mapping**

**Explanation:** Title for mapping of qualifiers.

**Action:** None

**Outcome Mapping**

**Explanation:** Title for mapping of outcomes

**Action:** None

**Wildcarded file path component is too high in the path name.**

**Explanation:** The first element of a file specification cannot contain wildcard elements.

**Action:** Remove the incorrectly specified wildcard file entry and allow the updated policy to be replicated. If the problem persists, contact IBM Customer Support.

**Wildcarded file path component is not an absolute path.**

**Explanation:** The wildcarded file path component needs to be an absolute path.

**Action:** Check previous errors in the error log to identify the cause of the error. Correct the problem. If the problem persists, contact IBM Customer Support.

**Service specified is unrecognized**

**Explanation:** Unknown service specified in the network policy.

**Action:** Check the service specification in the network policy and verify that it corresponds to a valid service. Correct the policy and then let the updated policy get replicated. If the problem persists, contact IBM Customer Support.

**Port number is not in the range 1 to 65535**

**Explanation:** The port number specified is outside of the range of 1 to 65535.

**Action:** Correct the port number in the policy to be between 1 and 65535. Let the policy be replicated. If the problem persists, contact IBM Customer Support.

**Hostspec is not an IP address**

**Explanation:** The host specification in the network policy must be a valid IP address.

**Action:** Check the syntax of the network policy. Correct the host specification part of the policy and then let the updated policy be replicated. If the problem persists, contact IBM Customer Support.

**Network policy is ambiguous**

**Explanation:** The network policy is ambiguous. Policies exist for the same host spec and service under different policy object names.

**Action:** Check the syntax of the resources with network policy to determine the cause of the ambiguous policy. Correct the policy and let the updated policy be replicated. If the problem persists, contact IBM Customer Support.

**Sudo command specified multiple times with conflicting attribute**

**Explanation:** The Sudo command attribute is specified multiple times with conflicting attributes.

**Action:** Remove the conflicting entries for the Sudo command and let the updated policy be replicated. If the problem persists, contact IBM Customer Support.

**No executable command specified in Sudo attributes**

**Explanation:** The Sudo attributes specified do not include an executable command to be run.

**Action:** Correct the Sudo command attribute in the policy. Let the policy be replicated. If the problem persists, contact IBM Customer Support.

**Protected Object Name has wildcarding syntax error**

**Explanation:** A syntax error was encountered while processing the wildcarding of the Protected Object Name.

**Action:** Check the syntax of the protected object name. Correct the problem. Let the policy be replicated. If the problem persists, contact IBM Customer Support.

**No matching wildcard information was found**

**Explanation:** No matching wildcard information found.

**Action:** Check previous errors to see if there was an error adding a wildcard entry which could have matched with the current object for cause of problem. Also check the syntax of the wildcarded entry which you expect to match with the current object for cause of problem. Correct the problem. Let the policy be replicated. If the problem persists, contact IBM Customer Support.
<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Explanation</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x35af2702</td>
<td>The wildcard pattern is already present in the database</td>
<td>The wildcard pattern specified is already present in the database.</td>
<td>None</td>
</tr>
<tr>
<td>0x35af2703</td>
<td>The pattern contains no wildcards</td>
<td>The pattern specified does not contain any wildcards.</td>
<td>None, if the protected object name is not supposed to have any wildcards. Otherwise, correct the pattern to include the necessary wildcarding.</td>
</tr>
<tr>
<td>0x35af2704</td>
<td>The engine contains no patterns</td>
<td>Internal status code indicating that the engine contains no patterns.</td>
<td>None</td>
</tr>
<tr>
<td>0x35af2780</td>
<td>Invalid feature set for creating a wildcard engine: 0x%x</td>
<td>The feature set specified for creating a wildcard engine is not valid.</td>
<td>None</td>
</tr>
<tr>
<td>0x35af2781</td>
<td>The internal representation of the wildcard pattern %s invalid: %d</td>
<td>The internal representation of the wildcard pattern is not valid.</td>
<td>None</td>
</tr>
<tr>
<td>0x35af2800</td>
<td>The representation of the date is invalid.</td>
<td>The date representation specified is not valid.</td>
<td>None</td>
</tr>
<tr>
<td>0x35af2880</td>
<td>%s is an invalid date.</td>
<td>The date representation specified is not valid.</td>
<td>Check the date syntax in the holiday object. Correct the holiday object name and let the updated policy be replicated. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35af2881</td>
<td>An error occurred in mktime for time: %u-%u-%u:%u:%u: % % %u</td>
<td>Internal coding error.</td>
<td>Contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35af3001</td>
<td>An invalid watch identifier provided</td>
<td>An unexpected error occurred because an invalid daemon identifier was passed to the watchdog service.</td>
<td>Restart the PDOS daemons and report the error to IBM Customer Support.</td>
</tr>
<tr>
<td>0x35af3002</td>
<td>The requested operation would block but a non-blocking operation was requested</td>
<td>A non-blocking operation was requested but it cannot be completed without blocking.</td>
<td>Restart the daemon and report the error to IBM Customer Support.</td>
</tr>
<tr>
<td>0x35af3003</td>
<td>The requested operation could not complete because we are at EOF</td>
<td>An error occurred reading the watchdog state file. The file might have been truncated or corrupted.</td>
<td>Contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35af3004</td>
<td>Daemon start request forwarded to a running daemon</td>
<td>A request has been sent to another daemon requesting a restart.</td>
<td>None</td>
</tr>
<tr>
<td>0x35af3005</td>
<td>Could not access a watchdog file</td>
<td>An error occurred when opening a watchdog file.</td>
<td>Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.</td>
</tr>
</tbody>
</table>
**0x35af3006  Watch directory cannot be accessed**

**Explanation:** An error occurred which prevents the daemon from accessing the watchdog directory.

**Action:** Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

---

**0x35af3007  Could not lock a watchdog file**

**Explanation:** An error occurred when locking a watchdog file.

**Action:** Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

---

**0x35af3008  Could not unlock a watchdog file**

**Explanation:** An error occurred when unlocking a watchdog file.

**Action:** Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

---

**0x35af3009  Could not seek in a watchdog file**

**Explanation:** An error occurred when seeking to the correct position in the watchdog state file.

**Action:** Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

---

**0x35af300a  Could not read from a watchdog file**

**Explanation:** An error occurred when reading from the watchdog state file.

**Action:** Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

---

**0x35af300b  Could not write to a watchdog file**

**Explanation:** An error occurred when writing to the watchdog state file.

**Action:** Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

---

**0x35af300d  Unable to find suitable program to watch on initial start**

**Explanation:** The daemon was unable to locate any other daemons to monitor.

**Action:** Contact IBM Customer Support.

---

**0x35af300e  Unable to set file to blocking mode**

**Explanation:** An error occurred when setting the file status flags of the open file descriptor for the watchdog FIFO to blocking mode.

**Action:** Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

---

**0x35af300f  Unable to get file blocking mode**

**Explanation:** An error occurred when fetching the file status flags of the open file descriptor for the watchdog FIFO.

**Action:** Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

---

**0x35af3010  Blocking read unexpectedly succeeded**

**Explanation:** An error occurred when the blocking read operation on the file descriptor for the watchdog FIFO of the watched process successfully read data. The FIFO should contain no data which means that the read should never complete. The read operation should block until the watched process closes its file descriptor for the same FIFO.

**Action:** Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

---

**0x35af3011  Blocking read failed**

**Explanation:** An error occurred when the blocking read operation on the file descriptor for the watchdog FIFO of the watched process failed.

**Action:** Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.

---

**0x35af3012  Watchee is invalid**

**Explanation:** An error occurred when the current daemon attempted to act as the watchdog for itself.

**Action:** Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.
0x35af3100 Could not open watchdog file %s: %d: %s
Explanation: An error occurred when opening the specified watchdog file.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35af3101 Could not lock watchdog file %s: %d: %s
Explanation: An error occurred when locking the specified watchdog file.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35af3102 Could not unlock watchdog file %s: %d: %s
Explanation: An error occurred when unlocking the specified watchdog file.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35af3103 Could not seek to %d in watchdog file %s: %d: %s
Explanation: An error occurred when seeking to the given position in the specified watchdog state file.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35af3104 Could not read byte %d in watchdog file %s: %d: %s
Explanation: An error occurred when reading at the given position in the specified watchdog state file.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35af3105 Could not write byte %d in watchdog file %s: %d: %s
Explanation: An error occurred when writing at the given position in the specified watchdog state file.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35af3107 Failed to start %s: exec failed: %d: %s
Explanation: An error occurred which prevented the specified daemon from being started by the current daemon.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35af3108 Successfully started %s
Explanation: A watchdog process has been successfully started.
Action: None

0x35af3109 Failed to start %s: Program exited with status: %d
Explanation: An error occurred when starting the specified daemon.
Action: Examine additional messages along with the exit status to determine the cause of the error and correct the problem. Restart the daemons. If the problem persists, contact IBM Customer Support.

0x35af310a Failed to start %s: Program was notified with signal: %d
Explanation: An error occurred when starting the specified daemon.
Action: Examine additional messages along with the signal number to determine the cause of the error and correct the problem. Restart the daemons. If the problem persists, contact IBM Customer Support.

0x35af310b Failed to start %s: Unexpected wait status: 0x%x
Explanation: An error occurred when starting the specified daemon.
Action: Examine additional messages along with the wait status code to determine the cause of the error and correct the problem. Restart the daemons. If the problem persists, contact IBM Customer Support.

0x35af310c %s died and returned an unexpected wait status: 0x%x
Explanation: The specified daemon terminated abnormally and the watchdog service was unable to determine the cause.
Action: The watchdog service should have restarted the daemon. Check additional messages to be sure the restart succeeded. If not, contact IBM Customer Support.
<table>
<thead>
<tr>
<th>Code</th>
<th>Message</th>
<th>Explanation</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x35af310d</td>
<td>Failed to start <code>%s</code> but no children have terminated</td>
<td>An error occurred when starting the specified daemon.</td>
<td>Restart the daemons and contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35af310e</td>
<td>Child <code>%s</code> died but no children have terminated</td>
<td>The watchdog service detected that the specified daemon terminated abnormally but the operating system reports that no child processes have terminated.</td>
<td>The watchdog service should have restarted the daemon. Check additional messages to be sure the restart succeeded. If not, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35af310f</td>
<td>Failed to start <code>%s</code> and could not call wait to find out why: <code>%d</code>: <code>%s</code></td>
<td>An error occurred when starting the specified daemon.</td>
<td>Examine additional messages along with the wait error code and status code to determine the cause of the error and correct the problem. Restart the daemons. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35af3110</td>
<td><code>%s</code> died and could not call wait to find out why: <code>%d</code>: <code>%s</code></td>
<td>The specified daemon terminated abnormally and the watchdog service was unable to determine the cause.</td>
<td>The watchdog service should have restarted the daemon. Check additional messages to be sure the restart succeeded. If not, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35af3111</td>
<td>Failed to start <code>%s</code>: fork failed: <code>%d</code>: <code>%s</code></td>
<td>An error occurred when starting the specified daemon.</td>
<td>Examine additional messages along with the error code and error text to determine the cause of the error and correct the problem. Restart the daemons. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35af3112</td>
<td>Failed to start <code>%s</code>: respawning too rapidly</td>
<td>An error occurred when starting the specified daemon.</td>
<td>Examine additional messages to determine the cause of the error and correct the problem. Stop all of the daemons and try to restart them. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35af3113</td>
<td>Cannot safely watch any program - watch thread terminating</td>
<td>The watchdog service is unable to watch any other daemons.</td>
<td>Examine additional messages to determine the cause of the error and correct the problem. Stop all of the daemons and try to restart them. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35af3114</td>
<td>Aborting watch thread - tried to watch <code>%s</code> but could not lock watch file: %0x%x: <code>%s</code></td>
<td>The watchdog service is unable to watch the specified daemon because another daemon is already watching it.</td>
<td>Examine additional messages to determine the cause of the error and correct the problem. Stop all of the daemons and try to restart them. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35af3115</td>
<td>Aborting watch thread - could not unlock watch file for <code>%s</code>: %0x%x: <code>%s</code></td>
<td>An error occurred when unlocking the watchdog lock file for the specified daemon.</td>
<td>Examine additional messages along with the error code and error text to determine the cause of the error and correct the problem. Restart the daemons. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35af3116</td>
<td>Aborting watch thread - could not lock watch file for <code>%s</code>: %0x%x: <code>%s</code></td>
<td>An error occurred when locking the watchdog lock file for the specified daemon.</td>
<td>Examine additional messages along with the error code and error text to determine the cause of the error and correct the problem. Restart the daemons. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35af3117</td>
<td>Aborting watch thread - could not open <code>%s</code> FIFO for write: %0x%x: <code>%s</code></td>
<td>An error occurred when opening the specified watchdog FIFO.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. Restart the daemons. If the problem persists, contact IBM Customer Support.</td>
</tr>
</tbody>
</table>
Aborting watch thread - could not open %s FIFO for read: 0x%x: %s

Explanation: An error occurred when opening the specified watchdog FIFO.

Action: Use the returned error code and error text to diagnose and correct the problem. Restart the daemons. If the problem persists, contact IBM Customer Support.

Aborting watch thread - could not block on watchee %s: 0x%x: %s

Explanation: The daemon is unable to watch the specified watchee daemon.

Action: Use the returned error code and error text to diagnose and correct the problem. Restart the daemons. If the problem persists, contact IBM Customer Support.

Aborting watch thread - could not read state of %s: 0x%x: %s

Explanation: The daemon is unable to watch the specified watchee daemon due to problems reading the watchdog state file.

Action: Use the returned error code and error text to diagnose and correct the problem. Restart the daemons. If the problem persists, contact IBM Customer Support.

Aborting watch thread - could not set state of %s: 0x%x: %s

Explanation: The daemon is unable to watch the specified watchee daemon due to problems writing the watchdog state file.

Action: Use the returned error code and error text to diagnose and correct the problem. Restart the daemons. If the problem persists, contact IBM Customer Support.

Aborting watch thread - could not set state of %s: 0x%x: %s

Explanation: The daemon is unable to watch the specified watchee daemon due to problems writing the watchdog state file.

Action: Use the returned error code and error text to diagnose and correct the problem. Restart the daemons. If the problem persists, contact IBM Customer Support.

Aborting watch thread - new watchee is invalid: %d

Explanation: An error occurred when taking over the watchdog duties of the previously watched daemon.

Action: Restart the daemons. If the problem persists, contact IBM Customer Support.

Aborting watch thread - unable to adopt required watchee: %s: 0x%x: %s

Explanation: An error occurred when taking over the watchdog duties of the previously watched daemon.

Action: Use the returned error code and error text to diagnose and correct the problem. Restart the daemons. If the problem persists, contact IBM Customer Support.

Watch directory %s is not a directory as expected

Explanation: An error occurred indicating that the specified watchdog directory path name is not a directory.

Action: The directory should have been created at install time. Try to re-create the directory. If the problem persists, contact IBM Customer Support.

Watch directory %s cannot be accessed: %d: %s

Explanation: An error occurred which prevents the daemon from accessing the specified watchdog directory.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Unable to set %s to blocking mode: %d: %s

Explanation: An error occurred when setting the file status flags of the open file descriptor for the specified watchdog file to blocking mode.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

Unable to get %s current blocking mode: %d: %s

Explanation: An error occurred when fetching the file status flags of the open file descriptor for the specified watchdog file.

Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.
<table>
<thead>
<tr>
<th>Code</th>
<th>Message</th>
<th>Explanation</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x35af3123</td>
<td>Blocking read on %s unexpectedly successfully read data: 0x%x</td>
<td>An error occurred when the blocking read operation on the file descriptor for the watchdog FIFO of the watched process successfully read data. The FIFO should contain no data which means that the read should never complete. The read operation should block until the watched process closes its file descriptor for the same FIFO.</td>
<td>Stop the daemons and remove the specified file. Restart the daemons. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35af3124</td>
<td>Blocking read on %s failed: %d: %s</td>
<td>An error occurred when the blocking read operation on the file descriptor for the watchdog FIFO of the watched process failed.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35af3125</td>
<td>Watchee %u for program %u is invalid</td>
<td>An error occurred when the current daemon attempted to act as the watchdog for itself.</td>
<td>Stop the daemons and remove the files under the /var/pdos/watch directory. Restart the daemons. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35af3126</td>
<td>Detected abnormal termination of %s</td>
<td>The watchdog service detected the abnormal termination of the daemon it is monitoring. The watchdog service will attempt to restart the daemon.</td>
<td>None</td>
</tr>
<tr>
<td>0x35af3127</td>
<td>Detected normal termination of %s</td>
<td>The watchdog service detected the normal termination of the daemon it is monitoring. The watchdog service will not attempt to restart the daemon.</td>
<td>None</td>
</tr>
<tr>
<td>0x35af3128</td>
<td>Failed to start %s: kosseal_setPidPriv failed: 0x%x: %s</td>
<td>An error occurred which prevented the current daemon from gaining the privilege needed to start the specified daemon.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35af3300</td>
<td>Join request rejected by %u which is already watching %u</td>
<td>An error occurred when a daemon that is already being watched by the watchdog service of the current daemon sent a new request to be watched.</td>
<td>Examine additional messages to determine the cause of the error and correct the problem. The watchdog service should handle this condition on its own. If not, restart the daemons. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35af3400</td>
<td>Read from a FIFO failed</td>
<td>An error occurred when reading from the watchdog FIFO.</td>
<td>Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35af3401</td>
<td>Write to a FIFO failed</td>
<td>An error occurred when writing to the watchdog FIFO.</td>
<td>Examine additional messages to determine the cause of the error and correct the problem. Restart the process. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35af3500</td>
<td>Could not read from FIFO %s: %d: %s</td>
<td>An error occurred when reading from the specified watchdog FIFO.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35af3501</td>
<td>Could not write to FIFO %s: %d: %s</td>
<td>An error occurred when writing to the specified watchdog FIFO.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
<tr>
<td>0x35af3502</td>
<td>Join thread could not open FIFO: 0x%x: %s</td>
<td>An error occurred when opening the watchdog join FIFO.</td>
<td>Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.</td>
</tr>
</tbody>
</table>
0x35af3503 Join thread could not unlock FIFO: 0x%x: %s
Explanation: An error occurred when unlocking the watchdog join FIFO.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35af3504 Join thread could not read FIFO: 0x%x: %s
Explanation: An error occurred when reading from the watchdog join FIFO.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35af3505 Join thread received a request for an invalid program: %d
Explanation: An error occurred when an invalid join request was read from the watchdog join FIFO.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35af3602 PDOSWDD tried to generate an unexpected audit event.
Explanation: An attempt was made to audit an event that is not recognized by the watchdog service.
Action: Restart the daemons and report the error to IBM Customer Support.

0x35af3700 Usage: pdoswdd [-fhlv?] [-t trace-string] -f run daemon in foreground -v display verbose messages -V display version information and terminate -[h?] display this usage message -t specify initial trace level
Explanation: pdoswdd usage statement.
Action: None

0x35af3708 Could not perform daemon cleanup: 0x%x: %s
Explanation: An error occurred during the shut down of the daemon when cleaning up the watchdog state.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35af370f Unable to initialize Message Handler service: 0x%x: %s
Explanation: An error occurred when the PDOSWDD daemon attempted to initialize the AZN message handling service.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35af3710 Unable to shutdown Message Handler service: 0x%x: %s
Explanation: An error occurred when the PDOSWDD daemon attempted to shut down the AZN message handling service.
Action: Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

0x35af3711 PDOSWDD terminating cleanly
Explanation: The PDOSWDD daemon is terminating normally.
Action: None

0x35af3712 PDOSWDD successfully shutdown
Explanation: The PDOSWDD daemon has shut down successfully.
Action: None

0x35af3713 Message Handler service initialized
Explanation: The PDOSWDD daemon has initialized the message handler service.
Action: None

0x35af3714 Message Handler service shutdown
Explanation: The PDOSWDD daemon has shut down the message handler service.
Action: None

0x35af3715 PDOSWDD is already running.
Explanation: An attempt was made to start the PDOSWDD daemon again when an instance is already running.
Action: None
**0x35af3b00** Program terminated for an indeterminate reason

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

---

**0x35af3b01** Program respawning too rapidly

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

---

**0x35af3b02** Could not fork

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

---

**0x35af3c00** Error auditing unknown event ID 0x%x on watched program %s.

**Explanation:** An attempt was made to audit an event that is not recognized by the PDOSWDD auditing service.

**Action:** Restart the PDOSWDD daemon and report the error to IBM Customer Support.

---

**0x35af3c01** Could not allocate audit record for 0x%x:0x%x audit event on watched program %s:0x%x: %s

**Explanation:** An error occurred when the PDOSWDD daemon attempted to allocate storage for a data structure to store an audit record.

**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

---

**0x35af3c02** Could not audit 0x%x:0x%x audit event on watched program %s: 0x%x: %s

**Explanation:** An error occurred while the PDOSWDD daemon attempted to audit an event pertaining to its watched daemon.

**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

---

**0x35af3c03** Error auditing unknown event ID 0x%x.

**Explanation:** An attempt was made to audit an event that is not recognized by the PDOSWDD auditing service.

**Action:** Restart the PDOSWDD daemon and report the error to IBM Customer Support.

---

**0x35af3c04** Error allocating audit record for event %s (0x%x). The error status is 0x%x: %s

**Explanation:** An error occurred when the PDOSWDD daemon attempted to allocate storage for a data structure to store an audit record.

**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

---

**0x35af3c05** Error auditing event %s (0x%x). The error status is 0x%x: %s.

**Explanation:** An error occurred when the PDOSWDD daemon attempted to send an audit event message to the PDOSAUDITD daemon.

**Action:** Use the returned error code and error text to diagnose and correct the problem. If the problem persists, contact IBM Customer Support.

---

**0x35af3d00** Program terminated with exit status 0

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

---

**0x35af3d01** Program terminated with exit status 1

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

---

**0x35af3d02** Program terminated with exit status 2

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.
<table>
<thead>
<tr>
<th>Code</th>
<th>Explanation</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x35af3d03</td>
<td>Program terminated with exit status 3</td>
<td>Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td></td>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3d04</td>
<td>Program terminated with exit status 4</td>
<td>Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td></td>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3d05</td>
<td>Program terminated with exit status 5</td>
<td>Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td></td>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3d06</td>
<td>Program terminated with exit status 6</td>
<td>Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td></td>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3d07</td>
<td>Program terminated with exit status 7</td>
<td>Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td></td>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3d08</td>
<td>Program terminated with exit status 8</td>
<td>Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td></td>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3d09</td>
<td>Program terminated with exit status 9</td>
<td>Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td></td>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3d0a</td>
<td>Program terminated with exit status 10</td>
<td>Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td></td>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3d0b</td>
<td>Program terminated with exit status 11</td>
<td>Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td></td>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3d0c</td>
<td>Program terminated with exit status 12</td>
<td>Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td></td>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3d0d</td>
<td>Program terminated with exit status 13</td>
<td>Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td></td>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3d0e</td>
<td>Program terminated with exit status 14</td>
<td>Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td></td>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3d0f</td>
<td>Program terminated with exit status 15</td>
<td>Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td></td>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3d10</td>
<td>Program terminated with exit status 16</td>
<td>Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td></td>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>Program terminated with exit status 17</td>
<td>Program terminated with exit status 24</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>---------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td></td>
</tr>
<tr>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Program terminated with exit status 18</th>
<th>Program terminated with exit status 25</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Program terminated with exit status 19</th>
<th>Program terminated with exit status 26</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Program terminated with exit status 20</th>
<th>Program terminated with exit status 27</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Program terminated with exit status 21</th>
<th>Program terminated with exit status 28</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Program terminated with exit status 22</th>
<th>Program terminated with exit status 29</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Program terminated with exit status 23</th>
<th>Program terminated with exit status 30</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
</tbody>
</table>
**Program terminated with exit status 31**  
**Explanation:** Audit Fail Status field of an audit record.  
**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

**Program terminated with exit status 32**  
**Explanation:** Audit Fail Status field of an audit record.  
**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

**Program terminated with exit status 33**  
**Explanation:** Audit Fail Status field of an audit record.  
**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

**Program terminated with exit status 34**  
**Explanation:** Audit Fail Status field of an audit record.  
**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

**Program terminated with exit status 35**  
**Explanation:** Audit Fail Status field of an audit record.  
**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

**Program terminated with exit status 36**  
**Explanation:** Audit Fail Status field of an audit record.  
**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

**Program terminated with exit status 37**  
**Explanation:** Audit Fail Status field of an audit record.  
**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

**Program terminated with exit status 38**  
**Explanation:** Audit Fail Status field of an audit record.  
**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

**Program terminated with exit status 39**  
**Explanation:** Audit Fail Status field of an audit record.  
**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

**Program terminated with exit status 40**  
**Explanation:** Audit Fail Status field of an audit record.  
**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

**Program terminated with exit status 41**  
**Explanation:** Audit Fail Status field of an audit record.  
**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

**Program terminated with exit status 42**  
**Explanation:** Audit Fail Status field of an audit record.  
**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

**Program terminated with exit status 43**  
**Explanation:** Audit Fail Status field of an audit record.  
**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

**Program terminated with exit status 44**  
**Explanation:** Audit Fail Status field of an audit record.  
**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.
Program terminated with exit status 45
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 46
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 47
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 48
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 49
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 50
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 51
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 52
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 53
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 54
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 55
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 56
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 57
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 58
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.
<table>
<thead>
<tr>
<th>Code</th>
<th>Program terminated with exit status</th>
<th>Explanation</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x35af3d3b</td>
<td>59</td>
<td>Audit Fail Status field of an audit record</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3d3c</td>
<td>60</td>
<td>Audit Fail Status field of an audit record</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3d3d</td>
<td>61</td>
<td>Audit Fail Status field of an audit record</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3d3e</td>
<td>62</td>
<td>Audit Fail Status field of an audit record</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3d3f</td>
<td>63</td>
<td>Audit Fail Status field of an audit record</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3d40</td>
<td>64</td>
<td>Audit Fail Status field of an audit record</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3d41</td>
<td>65</td>
<td>Audit Fail Status field of an audit record</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3d42</td>
<td>66</td>
<td>Audit Fail Status field of an audit record</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3d43</td>
<td>67</td>
<td>Audit Fail Status field of an audit record</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3d44</td>
<td>68</td>
<td>Audit Fail Status field of an audit record</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3d45</td>
<td>69</td>
<td>Audit Fail Status field of an audit record</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3d46</td>
<td>70</td>
<td>Audit Fail Status field of an audit record</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3d47</td>
<td>71</td>
<td>Audit Fail Status field of an audit record</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3d48</td>
<td>72</td>
<td>Audit Fail Status field of an audit record</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>Line</td>
<td>Program Terminated with Exit Status</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>73</td>
<td><strong>Program terminated with exit status 73</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Explanation:</strong></td>
<td>Audit Fail Status field of an audit record.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>74</td>
<td><strong>Program terminated with exit status 74</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Explanation:</strong></td>
<td>Audit Fail Status field of an audit record.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>75</td>
<td><strong>Program terminated with exit status 75</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Explanation:</strong></td>
<td>Audit Fail Status field of an audit record.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>76</td>
<td><strong>Program terminated with exit status 76</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Explanation:</strong></td>
<td>Audit Fail Status field of an audit record.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>77</td>
<td><strong>Program terminated with exit status 77</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Explanation:</strong></td>
<td>Audit Fail Status field of an audit record.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>78</td>
<td><strong>Program terminated with exit status 78</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Explanation:</strong></td>
<td>Audit Fail Status field of an audit record.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>79</td>
<td><strong>Program terminated with exit status 79</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Explanation:</strong></td>
<td>Audit Fail Status field of an audit record.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>80</td>
<td><strong>Program terminated with exit status 80</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Explanation:</strong></td>
<td>Audit Fail Status field of an audit record.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>81</td>
<td><strong>Program terminated with exit status 81</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Explanation:</strong></td>
<td>Audit Fail Status field of an audit record.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>82</td>
<td><strong>Program terminated with exit status 82</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Explanation:</strong></td>
<td>Audit Fail Status field of an audit record.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>83</td>
<td><strong>Program terminated with exit status 83</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Explanation:</strong></td>
<td>Audit Fail Status field of an audit record.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>84</td>
<td><strong>Program terminated with exit status 84</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Explanation:</strong></td>
<td>Audit Fail Status field of an audit record.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>85</td>
<td><strong>Program terminated with exit status 85</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Explanation:</strong></td>
<td>Audit Fail Status field of an audit record.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>86</td>
<td><strong>Program terminated with exit status 86</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Explanation:</strong></td>
<td>Audit Fail Status field of an audit record.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Program terminated with exit status 87

Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 88

Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 89

Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 90

Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 91

Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 92

Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 93

Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 94

Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 95

Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 96

Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 97

Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 98

Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 99

Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 100

Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.
Program terminated with exit status 101
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 102
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 103
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 104
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 105
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 106
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 107
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 108
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 109
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 110
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 111
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 112
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 113
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 114
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.
Program terminated with exit status 115
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 116
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 117
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 118
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 119
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 120
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 121
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.
0x35af3d81  Program terminated with exit status 129
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3d82  Program terminated with exit status 130
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3d83  Program terminated with exit status 131
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3d84  Program terminated with exit status 132
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3d85  Program terminated with exit status 133
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3d86  Program terminated with exit status 134
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3d87  Program terminated with exit status 135
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3d88  Program terminated with exit status 136
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3d89  Program terminated with exit status 137
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3d8a  Program terminated with exit status 138
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3d8b  Program terminated with exit status 139
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3d8c  Program terminated with exit status 140
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3d8d  Program terminated with exit status 141
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3d8e  Program terminated with exit status 142
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.
0x35af3d8f  Program terminated with exit status 143
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3d90  Program terminated with exit status 144
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3d91  Program terminated with exit status 145
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3d92  Program terminated with exit status 146
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3d93  Program terminated with exit status 147
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3d94  Program terminated with exit status 148
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3d95  Program terminated with exit status 149
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3d96  Program terminated with exit status 150
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3d97  Program terminated with exit status 151
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3d98  Program terminated with exit status 152
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3d99  Program terminated with exit status 153
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3d9a  Program terminated with exit status 154
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3d9b  Program terminated with exit status 155
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3d9c  Program terminated with exit status 156
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.
<table>
<thead>
<tr>
<th>Program terminated with exit status 157</th>
<th>Program terminated with exit status 164</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td><strong>Program terminated with exit status 158</strong></td>
<td><strong>Program terminated with exit status 165</strong></td>
</tr>
<tr>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td><strong>Program terminated with exit status 159</strong></td>
<td><strong>Program terminated with exit status 166</strong></td>
</tr>
<tr>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td><strong>Program terminated with exit status 160</strong></td>
<td><strong>Program terminated with exit status 167</strong></td>
</tr>
<tr>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td><strong>Program terminated with exit status 161</strong></td>
<td><strong>Program terminated with exit status 168</strong></td>
</tr>
<tr>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td><strong>Program terminated with exit status 162</strong></td>
<td><strong>Program terminated with exit status 169</strong></td>
</tr>
<tr>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td><strong>Program terminated with exit status 163</strong></td>
<td><strong>Program terminated with exit status 170</strong></td>
</tr>
<tr>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
<td><strong>Explanation:</strong> Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
<td><strong>Action:</strong> Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>Message ID</td>
<td>Status Code</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>0x35af3dab</td>
<td>171</td>
</tr>
<tr>
<td>0x35af3dac</td>
<td>172</td>
</tr>
<tr>
<td>0x35af3dad</td>
<td>173</td>
</tr>
<tr>
<td>0x35af3dae</td>
<td>174</td>
</tr>
<tr>
<td>0x35af3daf</td>
<td>175</td>
</tr>
<tr>
<td>0x35af3db0</td>
<td>176</td>
</tr>
<tr>
<td>0x35af3db1</td>
<td>177</td>
</tr>
<tr>
<td>0x35af3db2</td>
<td>178</td>
</tr>
<tr>
<td>0x35af3db3</td>
<td>179</td>
</tr>
<tr>
<td>0x35af3db4</td>
<td>180</td>
</tr>
<tr>
<td>0x35af3db5</td>
<td>181</td>
</tr>
<tr>
<td>0x35af3db6</td>
<td>182</td>
</tr>
<tr>
<td>0x35af3db7</td>
<td>183</td>
</tr>
<tr>
<td>0x35af3db8</td>
<td>184</td>
</tr>
</tbody>
</table>
Program terminated with exit status 185
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 186
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 187
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 188
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 189
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 190
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 191
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 192
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 193
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 194
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 195
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 196
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 197
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 198
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.
Program terminated with exit status 199
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 200
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 201
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 202
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 203
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 204
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 205
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 206
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 207
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 208
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 209
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 210
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 211
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 212
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.
Program terminated with exit status 213

Explanation: Audit Fail Status field of an audit record.

Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 214

Explanation: Audit Fail Status field of an audit record.

Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 215

Explanation: Audit Fail Status field of an audit record.

Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 216

Explanation: Audit Fail Status field of an audit record.

Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 217

Explanation: Audit Fail Status field of an audit record.

Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 218

Explanation: Audit Fail Status field of an audit record.

Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 219

Explanation: Audit Fail Status field of an audit record.

Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 220

Explanation: Audit Fail Status field of an audit record.

Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 221

Explanation: Audit Fail Status field of an audit record.

Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 222

Explanation: Audit Fail Status field of an audit record.

Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 223

Explanation: Audit Fail Status field of an audit record.

Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 224

Explanation: Audit Fail Status field of an audit record.

Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 225

Explanation: Audit Fail Status field of an audit record.

Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 226

Explanation: Audit Fail Status field of an audit record.

Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.
0x35af3de3  Program terminated with exit status 227
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3de4  Program terminated with exit status 228
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3de5  Program terminated with exit status 229
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3de6  Program terminated with exit status 230
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3de7  Program terminated with exit status 231
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3de8  Program terminated with exit status 232
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3de9  Program terminated with exit status 233
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3dea  Program terminated with exit status 234
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3deb  Program terminated with exit status 235
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3dec  Program terminated with exit status 236
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3ded  Program terminated with exit status 237
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3dee  Program terminated with exit status 238
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3def  Program terminated with exit status 239
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3df0  Program terminated with exit status 240
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.
Program terminated with exit status 241
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 242
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 243
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 244
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 245
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 246
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 247
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 248
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 249
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 250
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 251
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 252
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 253
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with exit status 254
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.
0x35af3dff  Program terminated with exit status 255
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e00  Program terminated with signal 0
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e01  Program terminated with signal 1
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e02  Program terminated with signal 2
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e03  Program terminated with signal 3
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e04  Program terminated with signal 4
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e05  Program terminated with signal 5
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e06  Program terminated with signal 6
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e07  Program terminated with signal 7
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e08  Program terminated with signal 8
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e09  Program terminated with signal 9
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e0a  Program terminated with signal 10
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e0b  Program terminated with signal 11
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e0c  Program terminated with signal 12
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.
0x35af3e0d  Program terminated with signal 13
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e0e  Program terminated with signal 14
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e0f  Program terminated with signal 15
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e10  Program terminated with signal 16
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e11  Program terminated with signal 17
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e12  Program terminated with signal 18
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e13  Program terminated with signal 19
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e14  Program terminated with signal 20
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e15  Program terminated with signal 21
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e16  Program terminated with signal 22
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e17  Program terminated with signal 23
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e18  Program terminated with signal 24
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e19  Program terminated with signal 25
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e1a  Program terminated with signal 26
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.
<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Explanation</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x35af3e1b</td>
<td>Program terminated with signal 27</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3e1c</td>
<td>Program terminated with signal 28</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3e1d</td>
<td>Program terminated with signal 29</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3e1e</td>
<td>Program terminated with signal 30</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3e1f</td>
<td>Program terminated with signal 31</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3e20</td>
<td>Program terminated with signal 32</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3e21</td>
<td>Program terminated with signal 33</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3e22</td>
<td>Program terminated with signal 34</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3e23</td>
<td>Program terminated with signal 35</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3e24</td>
<td>Program terminated with signal 36</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3e25</td>
<td>Program terminated with signal 37</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3e26</td>
<td>Program terminated with signal 38</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3e27</td>
<td>Program terminated with signal 39</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3e28</td>
<td>Program terminated with signal 40</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
</tbody>
</table>
Program terminated with signal 41
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 42
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 43
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 44
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 45
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 46
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 47
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 48
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 49
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 50
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 51
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 52
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 53
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 54
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.
<table>
<thead>
<tr>
<th>Code</th>
<th>Program Terminated with Signal</th>
<th>Explanation:</th>
<th>Action:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x35af3e37</td>
<td>Program terminated with signal 55</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3e38</td>
<td>Program terminated with signal 56</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3e39</td>
<td>Program terminated with signal 57</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3e3a</td>
<td>Program terminated with signal 58</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3e3b</td>
<td>Program terminated with signal 59</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3e3c</td>
<td>Program terminated with signal 60</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3e3d</td>
<td>Program terminated with signal 61</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3e3e</td>
<td>Program terminated with signal 62</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3e3f</td>
<td>Program terminated with signal 63</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3e40</td>
<td>Program terminated with signal 64</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3e41</td>
<td>Program terminated with signal 65</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3e42</td>
<td>Program terminated with signal 66</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3e43</td>
<td>Program terminated with signal 67</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>0x35af3e44</td>
<td>Program terminated with signal 68</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
</tbody>
</table>
Program terminated with signal 69
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 70
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 71
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 72
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 73
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 74
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 75
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.
D. Messages

0x35af3e53  Program terminated with signal 83
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e54  Program terminated with signal 84
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e55  Program terminated with signal 85
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e56  Program terminated with signal 86
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e57  Program terminated with signal 87
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e58  Program terminated with signal 88
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e59  Program terminated with signal 89
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e5a  Program terminated with signal 90
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e5b  Program terminated with signal 91
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e5c  Program terminated with signal 92
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e5d  Program terminated with signal 93
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e5e  Program terminated with signal 94
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e5f  Program terminated with signal 95
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e60  Program terminated with signal 96
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.
<table>
<thead>
<tr>
<th>0x35af3e61</th>
<th>Program terminated with signal 97</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong></td>
<td>Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>0x35af3e62</th>
<th>Program terminated with signal 98</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong></td>
<td>Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>0x35af3e63</th>
<th>Program terminated with signal 99</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong></td>
<td>Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>0x35af3e64</th>
<th>Program terminated with signal 100</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong></td>
<td>Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>0x35af3e65</th>
<th>Program terminated with signal 101</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong></td>
<td>Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>0x35af3e66</th>
<th>Program terminated with signal 102</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong></td>
<td>Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>0x35af3e67</th>
<th>Program terminated with signal 103</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong></td>
<td>Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>0x35af3e68</th>
<th>Program terminated with signal 104</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong></td>
<td>Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>0x35af3e69</th>
<th>Program terminated with signal 105</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong></td>
<td>Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>0x35af3e6a</th>
<th>Program terminated with signal 106</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong></td>
<td>Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>0x35af3e6b</th>
<th>Program terminated with signal 107</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong></td>
<td>Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>0x35af3e6c</th>
<th>Program terminated with signal 108</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong></td>
<td>Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>0x35af3e6d</th>
<th>Program terminated with signal 109</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong></td>
<td>Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>0x35af3e6e</th>
<th>Program terminated with signal 110</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Explanation:</strong></td>
<td>Audit Fail Status field of an audit record.</td>
</tr>
<tr>
<td><strong>Action:</strong></td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
</tbody>
</table>

Version 3.8
Program terminated with signal 111
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 112
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 113
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 114
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 115
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 116
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 117
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 118
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 119
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 120
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 121
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 122
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 123
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 124
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.
**Program terminated with signal 125**

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon's log file to determine the cause of the error and correct the problem.

---

**Program terminated with signal 126**

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon's log file to determine the cause of the error and correct the problem.

---

**Program terminated with signal 127**

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon's log file to determine the cause of the error and correct the problem.

---

**Program terminated with signal 128**

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon's log file to determine the cause of the error and correct the problem.

---

**Program terminated with signal 129**

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon's log file to determine the cause of the error and correct the problem.

---

**Program terminated with signal 130**

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon's log file to determine the cause of the error and correct the problem.

---

**Program terminated with signal 131**

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon's log file to determine the cause of the error and correct the problem.

---

**Program terminated with signal 132**

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon's log file to determine the cause of the error and correct the problem.

---

**Program terminated with signal 133**

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon's log file to determine the cause of the error and correct the problem.

---

**Program terminated with signal 134**

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon's log file to determine the cause of the error and correct the problem.

---

**Program terminated with signal 135**

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon's log file to determine the cause of the error and correct the problem.

---

**Program terminated with signal 136**

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon's log file to determine the cause of the error and correct the problem.

---

**Program terminated with signal 137**

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon's log file to determine the cause of the error and correct the problem.

---

**Program terminated with signal 138**

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon's log file to determine the cause of the error and correct the problem.
0x35af3e8b  Program terminated with signal 139
Explaination:  Audit Fail Status field of an audit record.
Action:  Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e8c  Program terminated with signal 140
Explaination:  Audit Fail Status field of an audit record.
Action:  Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e8d  Program terminated with signal 141
Explaination:  Audit Fail Status field of an audit record.
Action:  Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e8e  Program terminated with signal 142
Explaination:  Audit Fail Status field of an audit record.
Action:  Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e8f  Program terminated with signal 143
Explaination:  Audit Fail Status field of an audit record.
Action:  Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e90  Program terminated with signal 144
Explaination:  Audit Fail Status field of an audit record.
Action:  Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e91  Program terminated with signal 145
Explaination:  Audit Fail Status field of an audit record.
Action:  Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e92  Program terminated with signal 146
Explaination:  Audit Fail Status field of an audit record.
Action:  Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e93  Program terminated with signal 147
Explaination:  Audit Fail Status field of an audit record.
Action:  Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e94  Program terminated with signal 148
Explaination:  Audit Fail Status field of an audit record.
Action:  Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e95  Program terminated with signal 149
Explaination:  Audit Fail Status field of an audit record.
Action:  Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e96  Program terminated with signal 150
Explaination:  Audit Fail Status field of an audit record.
Action:  Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e97  Program terminated with signal 151
Explaination:  Audit Fail Status field of an audit record.
Action:  Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3e98  Program terminated with signal 152
Explaination:  Audit Fail Status field of an audit record.
Action:  Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.
<table>
<thead>
<tr>
<th>Program terminated with signal</th>
<th>Explanation:</th>
<th>Action:</th>
</tr>
</thead>
<tbody>
<tr>
<td>153</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>154</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>155</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>156</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>157</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>158</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>159</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>160</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>161</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>162</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>163</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>164</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>165</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
<tr>
<td>166</td>
<td>Audit Fail Status field of an audit record.</td>
<td>Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</td>
</tr>
</tbody>
</table>
Program terminated with signal 167

Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 168

Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 169

Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 170

Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 171

Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 172

Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 173

Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.
<table>
<thead>
<tr>
<th>Code</th>
<th>Program terminated with signal</th>
<th>Explanation: Audit Fail Status field of an audit record.</th>
<th>Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x35af3eb5</td>
<td>181</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x35af3eb6</td>
<td>182</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x35af3eb7</td>
<td>183</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x35af3eb8</td>
<td>184</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x35af3eb9</td>
<td>185</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x35af3eb9a</td>
<td>186</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x35af3ebb</td>
<td>187</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x35af3ebc</td>
<td>188</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x35af3ebd</td>
<td>189</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x35af3ebe</td>
<td>190</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x35af3ebf</td>
<td>191</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x35af3ec0</td>
<td>192</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x35af3ec1</td>
<td>193</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0x35af3ec2</td>
<td>194</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
0x35af3ec3  Program terminated with signal 195
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3ec4  Program terminated with signal 196
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3ec5  Program terminated with signal 197
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3ec6  Program terminated with signal 198
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3ec7  Program terminated with signal 199
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3ec8  Program terminated with signal 200
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3ec9  Program terminated with signal 201
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3ecca Program terminated with signal 202
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3ecb Program terminated with signal 203
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3ecc Program terminated with signal 204
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3ecd Program terminated with signal 205
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3ecf Program terminated with signal 206
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3ed0 Program terminated with signal 207
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3ed1 Program terminated with signal 208
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.
Program terminated with signal 209

Explanation: Audit Fail Status field of an audit record.

Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 210

Explanation: Audit Fail Status field of an audit record.

Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 211

Explanation: Audit Fail Status field of an audit record.

Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 212

Explanation: Audit Fail Status field of an audit record.

Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 213

Explanation: Audit Fail Status field of an audit record.

Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 214

Explanation: Audit Fail Status field of an audit record.

Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

Program terminated with signal 215

Explanation: Audit Fail Status field of an audit record.

Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.
**0x35af3edf**  Program terminated with signal 223

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

**0x35af3ee0**  Program terminated with signal 224

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

**0x35af3ee1**  Program terminated with signal 225

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

**0x35af3ee2**  Program terminated with signal 226

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

**0x35af3ee3**  Program terminated with signal 227

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

**0x35af3ee4**  Program terminated with signal 228

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

**0x35af3ee5**  Program terminated with signal 229

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

**0x35af3ee6**  Program terminated with signal 230

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

**0x35af3ee7**  Program terminated with signal 231

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

**0x35af3ee8**  Program terminated with signal 232

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

**0x35af3ee9**  Program terminated with signal 233

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

**0x35af3eea**  Program terminated with signal 234

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

**0x35af3eeb**  Program terminated with signal 235

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

**0x35af3eec**  Program terminated with signal 236

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.
0x35af3eed Program terminated with signal 237
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3eee Program terminated with signal 238
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3ef0 Program terminated with signal 240
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3ef1 Program terminated with signal 241
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3ef2 Program terminated with signal 242
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

0x35af3ef3 Program terminated with signal 243
Explanation: Audit Fail Status field of an audit record.
Action: Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.
**0x35af3efb**  Program terminated with signal 251

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

---

**0x35af3efc**  Program terminated with signal 252

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

---

**0x35af3efd**  Program terminated with signal 253

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

---

**0x35af3efe**  Program terminated with signal 254

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.

---

**0x35af3eff**  Program terminated with signal 255

**Explanation:** Audit Fail Status field of an audit record.

**Action:** Examine additional messages in the failing daemon’s log file to determine the cause of the error and correct the problem.
Index

A
access control
  login resource  35
  surrogate resources  41
access control lists  9
access control on file system resources  18
access controls  8
access restriction evaluation  15
access restrictions  15
accessor identity, determining  85
ACL  9
administration
  managing PDOS processes  75
  tuning  74
administrative tasks  71
attributes
  response file for configuration  74
audit viewing  145
auditor  62
authorization
  PDOS model  3
  authorization decision process  53
  authorization policy  4
  authorization roles
    for TACF tasks  90

B
backing up PDOS  87
books
  feedback xiv
  online xiv
  ordering xiv

C
checking PDOS daemon status  76
command
  pdosaudview  148
  pdosbkup  151
  pdoscfg  153
  pdosctl  158
  pdosdestroy  161
  pdosexempt  162
  pdoshla  164
  pdoslpadm  166
  pdosobjsig  170
  pdosrefresh  172
  pdosrevoke  173
  pdosrgyimp  175

command (continued)
  pdosrstr  179
  pdossudo  180
  pdossudo usage  45
  pdostecfg  181
  pdostecuefg  183
  pdosucfg  185
  pdosuidprog  187
  pdosunauth  190
  pdosversion  191
  pdoswhoami  192
  pdoswhois  194
commands
  wrunjob  91
  wruntask  91
  wschedjob  91
configuration
  options  154
configuration files
  backing up  88
  restoring  88
configuration options, PDOS  154
configuring the hostname look-aside database  86
controlling access  8
credentials
  explicitly destroying  85
  explicitly refreshing  84
credentials cache, tuning  84
credentials, managing  84
  Customer Support xv

D
daemon
  checking status  76
  PDOSAUDITD  56
  PDOSD  50
  PDOSWDD  57, 59
daemons
  functions  49
database
  hostname look-aside  86
databases
  backing up  88
  restoring  88
databases, PDOS  2
directory names, notation xvi
M
managing credentials 84
managing login activity policy 81
managing PDOS processes 75
managing the hostname look-aside database 87
managing the object signature database 81
managing the Trusted Computing Base 80
manuals
  feedback xiv
  online xiv
  ordering xiv
mapping command line options to attributes
  response file for configuration 74

N
namespace root 5
network policy 28
Non-local UNIX User Registry isolation 69
notation
  environment variables xvi
  path names xvi
  typeface xvi

O
object name 6
object name structure
  namespace root 5
  object name 6
  policy branch 6
  protected 5
  resource types 6
object signature database 81
online publications xv
options
  configuration 154
  ordering publications xv
osseal group 61
osseal user 61
osseal-admin group 60
osseal-audit 65
osseal-auditors group 61
osseal-credentials 65
osseal-default 65
osseal-default-file 66
osseal-default-login 66
osseal-default-net-incoming 66
osseal-default-net-outgoing 66
osseal-default-sudo 66
osseal-default-surrogate 66
osseal-hla 66
osseal-logs 66
osseal-open 66
osseal-privileged-user 66
osseal-restricted 67
osseal-restricted-read 67
osseal-tcb 67
osseal-umsg 67
osseal-unauth user 62

P
path names, notation xvi
PDOS
  configuration options 154
  databases 2
  identity 3
PDOS management tasks
  Add/Remove PDOS Auditors/Administrators 91
  Backup PDOS Database 93
  Certificate Transfer Utility 94
  Configure PDOS Auditing 96
  Configure PDOS Caching 97
  Configure PDOS Logging 98
  Configure PDOS Login and Password Policy 100
  Configure PDOS Server 101
  Configure PDOS TCB 103
  Display PDOS Hostname Cache 105
  Import UNIX TCB 106
  Import UNIX Users and Groups 107
  Manage PDOS Credential Cache 109
  Manage PDOS Server State 110
  Manage PDOS TCB 111
  Migrate TACF to PDOS 112
  Purge PDOS Hostname Cache 114
  Query PDOS Login and Password Policy 115
  Query PDOS Server State 117
  Query PDOS TCB 117
  Restore PDOS Database 118
  Set PDOS Server Audit Level 119
  Set PDOS Server Trace Level 121
  Show PDOS Auditing Configuration 124, 128
  Show PDOS Auditors/Administrators 125
  Show PDOS Caching Configuration 126
  Show PDOS Logging Configuration 126
  Show PDOS Server Audit Level 127
  Show PDOS Server Configuration 127
  Subscribe PDOS Endpoints 129
  Update PDOS Hostname Cache 129
PDOSAUDITD configuration 56
PDOSAUDITD daemon 56
pdosaudview command 148
pdoshkup command 151
pdoscfg command 153
pdosctl command 158
PDOSD authorization daemon 50
PDOSD log configuration attributes 55
pdosd-hostname user 62
pdosdestroy command 161
pdosexempt command 162
pdoshlacommand 164
pdospadm command 166
pdosobjsig command 170
pdosrefresh command 172
pdosrevoke command 173
pdosrgyimp command 175
pdosrstr command 179
pdossudo command 45, 180
pdosteccfg command 181
pdostecucfg command 183
pdosucfg command 185
pdosuidprog command 187
pdosunauth command 190
pdosversion command 191
PDOSWDD configuration 58, 59
PDOSWDD daemon 57, 59
pdoswhoami command 192
pdoswhois command 194
planning policy 5
policy
  authorization decision process 53
  hard links 21
  initial configuration 65
  login 31
  login activity 35
  network 28
  PDOS authorization 4
  planning 5
  security considerations 52
  sudo 42
  surrogate 39
  symbolic links 19
  warning modes 77
policy branch 6
Policy Director Management Server isolation 68
Policy Director User Registry isolation 68
policy warning modes 77
protected object name structure 5
protected object policies 13
  audit level 14
  time-of-day 14
  warning mode 13
protected system resources 16
publications
  feedback xiv
  online xiv
  ordering xiv

S
secure files 25
secure programs 25
security
  authorization decision process 53
  security considerations 52
starting pdos 75
stopping 76
stopping PDOS 76
Sudo
  wildcarding arguments 45
sudo policy 42
surrogate policy 39
surrogate resources
  access control 41
  symbolic links 19
  symbolic links example 20
  system resources 16
  file policy 17

T
TACF
  task authorization roles 90
  using wrunjob 91
  using wruntask 91
TACF tasks
  See also tasks 89
TACF tasks, authorization roles 90
  task overview, administration 71
TCB
  managing 80
  tuning monitoring 81
TCB monitoring 54
TCB resources 23
  immune programs 26
  impersonator programs 26
  login programs 24
  secure files 25
  secure programs 25
TEC logfile adapter 198, 202
time of day
  login restrictions 31
Tivoli Customer Support xv
Tivoli Enterprise Console
  integrating with Tivoli Security Management 197, 201
Tivoli Security Management
  integrating with Tivoli Enterprise Console 197, 201
traversal 12
trusted computing base resources 23
tuning
  credentials cache 84
  TCB monitoring 81
Tuning PDOS Configuration 74

R
resource managers 2
resource types 6
response file for configuration
  attributes 74
  mapping command line options to attributes 74
restoring PDOS 87
root user 61
rules
  TEC 209
runtime 49
runtime administrator 61
U
understanding PDOS 1
UNIX
  identity 3
  user identity 3
  users and groups 60

V
variables, notation for xvi
verifying policy 77

W
warning mode
  global 77
  global for a specific resource 78
warning modes
  policy 77
wildcard precedence 7
wildcarding 6
  Sudo arguments 45
wrunjob command 91
wruntask command 91
wschedjob command 91