IBM® SecureWay® Policy Director

# Migration Guide

*Version 3.0.1*

IBM® SecureWay® Policy Director

# Migration Guide

*Version 3.0.1*

**Note**

Before using this information and the product it supports, read the general information under "Appendix B. Notices" on page 37.

**First Edition (January 2000)**

This edition applies to version 3, release 0, modification 1 of IBM SecureWay Policy Director product and to all subsequent releases and modifications until otherwise indicated in new editions.

# Contents

# About this book

This book contains information about how to install and use the IBM® SecureWay® Policy Director (Policy Director) migration tool.

## Who should read this book

Administrators who are upgrading from previous releases of DASCOM IntraVerse or IBM SecureWay Policy Director versions should read this book. This book is also for Policy Director administrators who are backing up and restoring a current release of IBM SecureWay Policy Director.

Distributed Computing Environment (DCE) and IBM SecureWay Directory's lightweight directory access protocol (LDAP) are co-requisite products of Policy Director. Administrators should have some knowledge of IBM DCE and LDAP. Also, administrators should have basic working knowledge about installing and configuring DCE and LDAP servers.

## How this book is organized

This book contains the following chapters:

- "Chapter 1. IBM SecureWay" on page 1 provides an overview of the IBM SecureWay FirstSecure® set of integrated security products. It also provides an overview of the IBM SecureWay Policy Director product.
- "Chapter 2. Introducing the migration tool" on page 3 provides introduction information about the IBM SecureWay Policy Director migration tool. It discusses using the tool for upgrading from a previous release or using the tool to back up and restore a current version.
- "Chapter 3. Installing the migration tool" on page 5 describes how to locate and install the migration tool files.
- "Chapter 4. Editing the migrate.conf file" on page 7 explains the migrate.conf configuration file template and how to edit this file.
- "Chapter 5. Using the MIGRATE command" on page 9 shows the syntax of the **migrate** command and provides examples of migration commands.
- "Chapter 6. Migrating DCE data" on page 11 provides information about migrating (backing up and restoring) your DCE (Distributed COmputing Environment) user and group data, ACL (access control list), and WebSEAL data to the most current version of Policy Director, Version 3.0.1.
- "Chapter 7. Migrating LDAP data" on page 15 provides information about migrating your LDAP user and group data, ACL, and WebSEAL data to the most current version of Policy Director, Version 3.0.1.
- "Chapter 8. Editing XML input and output files" on page 21 provides examples and explanations of the Extensible Markup Language (XML) files for ACL, WebSEAL, and user data.
- "Chapter 9. Reviewing log and error files" on page 29 explains the migration.log file and the XML-format error output files.
- "Chapter 10. Removing the migration files" on page 31 describes how to remove the migration tool package after upgrading.

- "Appendix A. Document type definition" on page 33 provides an explanation of what a document type definition (DTD) is and provides the content of the DTD used by the Policy Director migration tool.

## What is new in this release

On the IBM SecureWay Policy Director Version 3.0.1 CD, you will find:

- IBM SecureWay Policy Director software updates and fixes to the version 3.0 product released in October 1999.
- A README file, version 3.0.1, in Hypertext Markup Language (HTML) format.
- An IBM SecureWay Policy Director Administration Guide: Additions and Corrections, version 3.0.1.
- An IBM SecureWay Policy Director Programming Guide, version 3.0.1.
- All IBM SecureWay Policy Director documentation for version 3.0 that was released in October 1999.

  See the *IBM SecureWay Policy Director Up and Running*, Version 3.0 book that provides information about what is new for version 3.0 of IBM SecureWay Policy Director.

At the IBM SecureWay Policy Director Web site, you will find the:

- *IBM SecureWay Policy Director Migration Guide*, Version 3.0.1, and related migration software for AIX®, Solaris, or Windows NT®.
- *IBM SecureWay Policy Director Authorization API: Java Reference*, Version 3.0.1, and related Authorization application programming interface (API) Java classes software.
- *IBM SecureWay Policy Director Quick Installation Guide for Windows NT*, Version 3.0.1.

See "Web information" on page vii for related Web addresses.

## Year 2000 readiness

This product is Year 2000 ready. When used in accordance with its associated documentation, it is capable of correctly processing, providing, and/or receiving date data within and between the twentieth and twenty-first centuries, provided that all products (for example, hardware, software, and firmware) used with the products properly exchange accurate date data with it.

## Service and support

Contact IBM for service and support for all the products included in the IBM SecureWay FirstSecure offering. Some of these products might refer to non-IBM support. If you obtain these products as part of the FirstSecure offering, contact IBM for service and support.

## Conventions

This book uses the following typographical conventions:

| Convention | Meaning |
|---|---|
| **bold** | User interface elements such as check boxes, buttons, and items inside list boxes. |
| `monospace` | Syntax, sample code, and any text that the user must type. |
| *Italic* | Emphasis and first use of special terms that are relevant to Policy Director. |
| → | Shows a series of selections from a menu. For example, click **File → Run** means click **File**, and then click **Run**. |

## Web information

Information about last-minute updates to Policy Director is available at the following Web address:

`http://www.ibm.com/software/security/policy/library`

You can download Policy Director migration tool software and other Policy Director software from this Web address:

`http://www.ibm.com/software/security/policy/downloads`

Information about updates to other IBM SecureWay FirstSecure products is available by starting at the following Web address:

`http://www.ibm.com/software/security/firstsecure/library`

# Chapter 1. IBM SecureWay

IBM SecureWay Policy Director (Policy Director) is available either as a component of IBM SecureWay FirstSecure or as a standalone product.

## What is IBM SecureWay FirstSecure?

IBM SecureWay FirstSecure (FirstSecure) is part of the IBM integrated security solution. FirstSecure is a comprehensive set of integrated products that help your company:

- Establish a secure e-business environment.
- Reduce the total cost of security ownership by simplifying security planning.
- Implement security policy.
- Create an effective e-business environment.

The IBM SecureWay products include:

**Policy Director**
IBM SecureWay Policy Director (Policy Director) provides authentication, authorization, data security, and Web resource management.

**Boundary Server**
IBM SecureWay Boundary Server (Boundary Server) provides:

- The critical firewall functions of filtering, proxy, and circuit level gateway.
- A virtual private network (VPN) connection to the IBM Firewall.
- The components for Internet security.
- A mobile code security solution.

A configuration graphical user interface (GUI) ties together the Policy Director's proxy user function with the Boundary Server's Firewall product.

**Intrusion Immunity**
Intrusion Immunity provides intrusion detection and antivirus protection.

**Trust Authority**
IBM SecureWay Trust Authority (Trust Authority) supports public key infrastructure (PKI) standards for cryptography and interoperability. Trust Authority provides support for issuance, renewal, and revocation of digital certificates. These certificates provide a means to authenticate users and to ensure trusted communications.

**Toolbox**
The IBM SecureWay Toolbox (Toolbox) is a set of application programming interfaces (API) with which application programmers can incorporate security into their software. You can obtain the Toolbox as part of FirstSecure. Both Policy Director and the Toolbox include the Policy Director API library and documentation. The Toolbox README file contains installation instructions for the Policy Director application development kit (ADK).

You can install each IBM SecureWay FirstSecure product independently. You can plan a controlled move toward a secure environment. This capability reduces the complexity and cost of securing your environment and speeds the deployment of Web applications and resources.

See the FirstSecure *Planning and Integration* documentation for more information about the FirstSecure components and for a list of documentation for all of the IBM SecureWay products.

## What is IBM SecureWay Policy Director?

Policy Director is a standalone authorization and security management solution. Policy Director provides end-to-end security of resources over geographically dispersed intranets and *extranets*. An *extranet* provides access control and security features to restrict the use of one or more intranets attached to the Internet to selected subscribers.

Policy Director provides authentication, authorization, data security, and resource-management services. You can use Policy Director in conjunction with standard Internet-based applications to build secure and well-managed intranets and extranets.

Policy Director runs on the following operating systems:

- Windows NT operating system (Windows)
- AIX operating system version 4.3 (AIX)
- Sun Solaris operating system version 2.6 (Solaris)

# Chapter 2. Introducing the migration tool

The administrator uses the IBM SecureWay Policy Director migration tool to perform the following tasks:

- when upgrading Policy Director—to migrate critical system databases and other information from previous versions to the current version of Policy Director.
- as a general administration tool—to back up existing critical system databases and other information and later allow the restoration of this data.

## Migrating data to an upgraded version of Policy Director

You can use the Policy Director migration tool to migrate critical system databases and other information to the most current version of Policy Director, Version 3.0.1. The Policy Director migration tool supports migration from these previous versions:

- IntraVerse Version 2.1 (Solaris)
- IntraVerse Version 3.0 evaluation installations (Solaris, AIX, and Windows NT)
- IBM SecureWay Policy Director Version 1.0, which consists of IntraVerse Version 2.1.2 and IBM Global Sign-On (GSO) Version 2.0.200 (Solaris, AIX, and Windows NT)

If you are using Policy Director Version 3.0 or higher, you do not need to use the migration tool to migrate LDAP registry or GSO information. The LDAP user and group data remains on the LDAP server. See "Chapter 7. Migrating LDAP data" on page 15 for complete instructions.

The migration tool extracts the following vital information from an existing system:

- ACL (security policy) database information
- WebSEAL (a Security Manager component) junction database information
- DCE user registry information

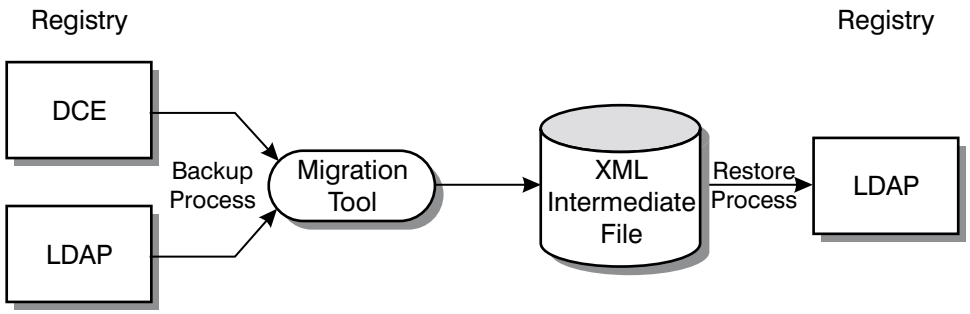
**Note:** You can migrate LDAP user and group registry information and GSO user information without using the Policy Director migration tool. See "Chapter 7. Migrating LDAP data" on page 15.

The migration tool stores the information in an intermediate format (XML file). After upgrading to Policy Director Version 3.0.1, use the migration tool to restore this information to the new environment.

The migration tool allows you to reconfigure your protected cell with minimal configuration data loss. You can restore user, ACL, and WebSEAL data to the same server in the DCE cell. Or, you can restore this data to a server that is in a different DCE cell from the original (backup) server. However, you can only migrate WebSEAL junctions data between WebSEAL servers in the same DCE cell.

## Backing up and restoring data

In addition to migrating data, the migration tool allows you to read from and write to the same version of Policy Director. This feature makes the tool a backup and restore tool as well. Restore the data when there is unpredicatable damage that has been sustained to the cell. The administrator can extract configuration information for currently installed versions of Policy Director.




The migration tool performs the following backup and restore tasks:

- Extracting data from a previous IntraVerse or Policy Director installation.
- Storing the data as a hierarchy of objects into an intermediate XML output file.
- Extracting the data from the intermediate XML output file.
- Restoring the data to another Policy Director installation.

# Chapter 3. Installing the migration tool

Before you begin installing the IBM SecureWay Policy Director migration tool package, these rules apply:

1. You must run the tool on the same server as the ivmgrd process.
2. You must perform the commands as an administrative user of the local server, such as `root`.
3. IntraVerse or Policy Director must be installed correctly and operating.
4. DCE must be installed correctly and operating.
5. The LDAP server must be installed correctly and operating.
6. Ensure that all other servers that the administrator needs to connect to in addition to the LDAP server, including ivmgrd and secmgrd are installed correctly and operating. Administrators should check to see if all servers of these types, and in the current cell, are operating and responding to requests.
7. As a standard precaution when upgrading between versions, consider backing up all Policy Director servers before you begin.

To install the migration tool package:

1. Go to the following IBM Web location:

   `http://www.ibm.com/software/security/policy/downloads`
2. Select the migration package for the platform you want to download: AIX, Solaris, or Windows NT. Note that the migration tool runs on the same platform as the Policy Director servers.
3. Download and install the migration package. You must install the UNIX® version to the following location:

   `/opt/migration`

   You can install the Windows ® version to a subdirectory of your choice. For example, you could install to the following subdirectory:

   `c:\PD301\migration`
4. Uncompress or unzip the files and make sure that you have downloaded the files properly for the appropriate platform and ensure that the following files are available:

   **for Solaris:**

   ```
   libcdasauthn.so
   libdceauthn.so
   libdesauthn.so
   libgsomgmt.so
   libgsomgmtstub.so
   libgssauthn.so
   libira.so
   libirastub.so
   libivauthn.so
   libivauthzn.so
   libjdce.so
   libjniRpc.so
   libldap.so
   libldapauthn.so
   libnullauthn.so
   librpcauthn.so
   migrate
   migrate.conf
   ```

**for Windows NT:**

```
cdasauthn.dll
dceauthn.dll
desauthn.dll
dmtnt.dll
dssiconv.dll
dssloc1.dll
gsomgmt.dll
gsomgmtstub.dll
gssauthn.dll
ibmjndi.dll
ira.dll
irastub.dll
ivauthn.dll
ivauthzn.dll
jdce.dll
ldap.dll
ldap_plugin_sasl_cram-md5.dll
ldapauthn.dll
ldapjrt.dll
ldaploc1.dll
ldapunin.dll
libeay32.dll
migrate.conf
migrate.exe
nullauthn.dll
rpcauthn.dll
ssleay32.dll
locale\*
```

**for AIX:**

```
libcdasauthn.a
libgssauthn.a
libivmgmt.a
librpcauthn.a
libdceauthn.a
libira.a
libivmsg.a
libwebseal.a
libdesauthn.a
libirastub.a
libivobj.a
migrate
libdw.a
libivacl.a
libivstr.a
migrate.conf
libdwclient.a
libivaudit.a
libivsvr.a
libgsomgmt.a
libivauthn.a
libldap.a
libgsomgmtstatic.a
libivauthzn.a
libldapauthn.a
libgsomgmtstub.a
libivcore.a
libnullauthn.a
```

# Chapter 4. Editing the migrate.conf file

The Policy Director migration tool retrieves LDAP configuration information from these configuration files:

- The migrate.conf configuration file
- The iv.conf configuration file
- The secmgrd.conf configuration file

For DCE, the Cell Directory Service (CDS) automatically provides server information and other data that are required for migration.

The migrate.conf configuration file must be present and contain the appropriate configuration information. Policy Director provides a template migrate.conf configuration file with the migration tool package. This template serves as a guide for the format and content of the required configuration items.

Edit the migrate.conf file, which is the configuration file for the migration tool depending on your own Policy Director environment.

Following is an example of a migration configuration file:

```
################################################
#
# migration tool configuration file
#
[ldap]
domain = o=ibm,c=us
admin-dn = cn=root
admin-pwd = YhrT568b
################################################
```

Where:

**Domain**

Provides the base domain under which all migrated users and groups reside. Policy Director uses this domain value in the construction of distinguished names (DNs) for user and group entries. For DCE, this suffix is the suffix under which the Policy Director DCE users are added when migrating from a DCE registry and restoring to an LDAP registry.

For LDAP-migrated users, the migration tool handles multiple suffixes for data. When migrating from an LDAP registry and restoring to an LDAP registry, you do not need to specify the multiple suffixes.

```
domain=o=ibm,c=us
```

**LDAP database administrator's name**

Provides the distinguished name of the LDAP database administrator. This name should be the same name that was specified during the installation of the LDAP server. Typically, the administrator's DN is `cn=root` for Policy Director installations.

```
admin-dn = cn=root
```

**LDAP database administrator's password**

Provides a password of the LDAP database administrator. This plain text file containing the password must be protected and available only to appropriate users and groups.

```
admin-pwd = YhrT568b
```

# Chapter 5. Using the MIGRATE command

The migration tool follows the convention of standard command-line tools, providing command-line switches to control the operation of the tool.

Before performing migrations or backups, follow your standard practice for backing up servers.

Run the migration tool from the installation directory by typing the migration command:

**AIX and Solaris:**

```
installation-directory ./migrate -f output.xml -t [backup|restore] -[ademrsx] values
```

**Windows:**

```
installation-directory\migrate -f output.xml -t [backup|restore]
-r "C:\Program Files\IBM\Policy Director\lib\iv.conf" -[ademsx] values
```

Where these flags are required:

**-f** The name of the intermediate output file.

**-r** This flag is required only for Windows and provides the full path name for the Policy Director iv.conf configuration file. The default path is:
**AIX and Solaris:**
`/opt/intraverse/lib/iv.conf`
**Windows:** `"C:\Program Files\IBM\Policy Director\lib\iv.conf"`

The quotation marks and specifying the iv.conf file name are optional. For example, you can also specify the **-r** flag's path name as follows: `C:\Program Files\IBM\Policy Director\lib`.

**-t** The type of process (backup or restore). For DCE, you can restore other DCE component, other than DCE user and group information, such as ACL and WebSEAL junction information. DCE user and group information can only be restored to the LDAP DCE registry because of a DCE password limitation.

The following flags are optional. If you do not specify a value, the migration tool uses the default value.

**-a** The name of the log file. The default is to write to **migration.log**. See "Log file" on page 30 for more information.

**-d** The database in which the user information is currently stored (dce). The default is **dce**.

**Note:** The **-d** flag applies only to DCE user information. Do not use this flag for ACL or WebSEAL Smart Junction information. LDAP user information does not need to be migrated. The LDAP user information is stored on the LDAP server.

**-e** The name of the XML-formatted error file, which the administrator specifies. Policy Director only requires this flag when restoring. See "Error file" on page 29 for more information.

**-m** The form the user wants the data converted to before writing (ldap). Use the **-m** flag whenever you want to view data that has been backed up from a DCE registry. At this point, you can manually edit the XML file. It is not until the restoration process that the migration tool converts the user data from the DCE registry into an LDAP registry-acceptable format.

**-s** The level of the migration. The choices are all, acls, webseal, or users (DCE only). There is no default.

**-v** Prints the build version of the migration tool and date built. For example:

**AIX and Solaris:**

```
./migrate -v

3.0.1 (Build 87, TRDCE, SSL 40bit, Debug) Feb 8 2000
```

**-x** The indication of whether to force or not force the restoration of an action.

# Chapter 6. Migrating DCE data

The Policy Director migration tool lets you migrate, or back up and restore your DCE data: DCE users and groups, ACLs, and WebSEAL Smart Junctions information. You can migrate this data individually or you can migrate all of the data at one time using the **migrate** command syntax (see "Chapter 5. Using the MIGRATE command" on page 9).

For DCE user and group registry data, use the migration tool to migrate this data.However, you can only restore these DCE user registry entries to the LDAP user registry format. The migration tool does not perform DCE user restorations because the recent versions of Policy Director recommend using the LDAP registry for user and group entries. Other than DCE user information, you can restore other types of DCE information by using the migration tool.

## Backing up your Policy Director data

Back up your Policy Director data:

1. Copy the following Policy Director configuration files to a temporary directory. This information will be used later during the restoration process.
   - ivmgrd.conf
   - secmgrd.conf
   - ivacld.conf
   - ldap.conf
   - iv.conf
   - cdas.conf
2. Back up the Policy Director \certs directory for your platform. This information will be restored later.
   **AIX and Solaris:**
   ```
   /opt/intraverse/lib/certs
   ```
   **Windows:** `C:\Program Files\IBM\Policy Director\lib\certs`

## Backing up users from a DCE registry

The following example demonstrates how to back up users and groups from a DCE registry to an intermediate file named dce_backup.xml. Type:

**AIX and Solaris:**
```
./migrate -f dce_backup.xml -t backup -d dce -s users
```
**Windows:**
```
migrate.exe -f dce_backup.xml -t backup -r C:\Program
Files\IBM\Policy Director\lib -d dce -s users
```

## Backing up the ACL data

The following example demonstrates how to back up ACL information to an intermediate file named dce_backup.xml. Type:

**AIX and Solaris:**
```
./migrate -f dce_backup.xml -t backup -s acls
```
**Windows:**
```
migrate.exe -f dce_backup.xml -t backup -r C:\Program
Files\IBM\Policy Director\lib -s acls
```

## Backing up the WebSEAL Smart Junction data

The following example demonstrates how to back up WebSEAL Smart Junction information to an intermediate file named dce_backup.xml. Type:

**AIX and Solaris:**

```
./migrate -f dce_backup.xml -t backup -s webseal
```

**Windows:**

```
migrate.exe -f dce_backup.xml -t backup -r C:\Program
Files\IBM\Policy Director\lib -s webseal
```

## Restoring DCE users to an LDAP registry

Before restoring, be sure to upgrade the Policy Director installation to the appropriate version.

To restore from a DCE backup intermediate file:

**AIX and Solaris:**

```
./migrate -f dcep_backup.xml -d ldap -t restore -s users
-e dce_usererr.xml
```

**Windows:**

```
migrate.exe -f dce_backup.xml -d ldap -t restore -r
C:\Program Files\IBM\Policy Director\lib -s users -
e dce_usererr.xml
```

Note that Policy Director will assume the DCE registry by default if you do not use the **-d** switch for user or group data.

## Restoring the ACL data

Before restoring, be sure to upgrade to the appropriate version of Policy Director.

To restore previously backed up ACLs, type:

**AIX and Solaris:**

```
./migrate -f dce_backup.xml -t restore -s acls -e dce_aclerror.xml
```

**Windows:**

```
migrate.exe -f dce_backup.xml -t restore -r C:\Program
Files\IBM\Policy Director\lib -s acls -e dce_aclerror.xml
```

## Restoring the WebSEAL Smart Junction data

If you change from your previous server to a new and different server, you must change the WebSEAL server object entry. Edit the .XML intermediate file and type the name of the new WebSEAL server object before restoring the WebSEAL Smart Junction data.

Before restoring, be sure to upgrade to the appropriate version of Policy Director.

To restore previously backed up ACLs, type:

**AIX and Solaris:**

```
./migrate -f dce_backup.xml -t restore -s webseal -e
dce_weberror.xml
```

**Windows:**

```
migrate.exe -f dce_backup.xml -t restore -r C:\Program
Files\IBM\Policy Director\lib -s webseal -e dce_weberror.xml
```

## Restoring the Policy Director data

Be sure to restore the migration data on the same server where you log in as the cell administrator (cell_admin). After restoring the DCE data, restore the Policy Director data.

To restore the data:

1. Stop the Policy Director-related servers by using the iv script to stop all Policy Director servers on a particular machine in the correct order.

   See the *Policy Director Administration Guide* for more information on the iv script.

2. Restore the Policy Director configuration files.
   a. Using a comparison tool, compare the two sets of Policy Director configuration files (Version 3.0 and Version 3.0.1 files). The Version 3.0 files were copied in step 1 of "Backing up your Policy Director data" on page 11.
   b. As a precaution, back up the newly installed Policy Director Version 3.0.1 configuration files.
   c. Edit the following Policy Director Version 3.0.1 files, as necessary.
      - ivmgrd.conf
      - secmgrd.conf
      - ivacld.conf
      - ldap.conf
      - iv.conf
      - cdas.conf

      **Note:** Keep the Version 3.0.1 user ID and password information in these files: ivmgrd.conf, iv.conf, and ivacld.conf files. Update the Version 3.0.1 files to match all the other configuration information in these six Version 3.0 configuration files.

3. Restore the Policy Director \certs directory:
   a. As a precaution, back up the newly installed Policy Director Version 3.0.1 \certs directory.
   b. Copy the Policy Director Version 3.0 \certs directory files, which you previously backed up in step 2 in "Backing up your Policy Director data" on page 11, over the Version 3.0.1 \certs directory.

4. Restart Policy Director by using the iv script to start all Policy Director servers in the correct order.

   See the *Policy Director Administration Guide* for more information on the iv script.

# Chapter 7. Migrating LDAP data

The Policy Director migration tool lets you migrate, or back up and restore your LDAP data: ACLs and WebSEAL Smart Junctions information. You can migrate this data individually or you can migrate all of the data at one time using the **migrate** command syntax (see "Chapter 5. Using the MIGRATE command" on page 9).

If you are using Policy Director Version 3.0 or higher, you do not need to use the migration tool to migrate LDAP user and group registry data or GSO information This data already resides on the LDAP server.

- Follow the instructions in "Upgrading to Policy Director 3.0.1" if you are using the same LDAP server and only upgrading to Policy Director Version 3.0.1.
- If you are moving to a new LDAP Server and upgrading to Policy Director 3.0.1, then perform both of the following steps (in the order shown):
  1. Follow the instructions in "Upgrading to Policy Director 3.0.1" to upgrade from Policy Director 3.0.
  2. Follow the instructions in "Using a different LDAP server when upgrading" on page 19. You must backup specific LDAP and Policy Director information on the current LDAP server before you change servers.

## Upgrading to Policy Director 3.0.1

Use the following steps to upgrade to Policy Director Version 3.0.1 if you are using the same LDAP and Policy Director servers. You preserve the existing Policy Director and GSO data, the current system configuration, and the current levels of other servers in the configuration.

**Note:** Before performing migrations or backups, follow your standard practice for backing up your LDAP server. For example, you might back up your system to tape.

### Backing up your LDAP data

As a precaution, back up your LDAP data.

1. Back up the LDAP database by using the **db2 backup** command, or back up the LDAP directory data by using the LDAP DB2LDIF program.

   To use the **db2 backup** command, first stop the SecureWay Directory (LDAP) server and then type:

   ```
   db2 backup database dbname to directory_or_device
   ```

   Where *dbname* is the database name. For LDAP, `ldapdb2` is the default name of the database.

   LDAP provides the DB2LDIF program as part of the LDAP server installation. To use the DB2LDIF program:

   a. On the LDAP server that you are currently using for Version 3.0, change to one of the following subdirectories appropriate for your installation:
      **AIX:** `/usr/ldap/sbin`
      **Solaris:**
      `/opt/IBMldaps/sbin`

**Windows:**

```
C:\Program Files\IBM\LDAP\bin
```

b. On the LDAP server, type:

```
db2ldif -o v30backup
```

Where *v30backup* is the name of the output file. Save this file. This file will be used later in the restoration process.

2. Back up your LDAP configuration files. These files are included in the /etc subdirectory of your installation path:
   **AIX:** `/usr/ldap/etc`
   **Solaris:**
   `/opt/IBMldaps/etc`
   **Windows:**
   `C:\Program Files\IBM\LDAP\etc`

## Backing up your Policy Director data

Back up your Policy Director data:

1. Copy the following Policy Director configuration files to a temporary directory. This information will be used later during the restoration process.
   - ivmgrd.conf
   - secmgrd.conf
   - ivacld.conf
   - ldap.conf
   - iv.conf
   - cdas.conf
2. Back up the Policy Director \certs directory for your platform. This information will be restored later.
   **AIX and Solaris:**
   `/opt/intraverse/lib/certs`
   **Windows:** `C:\Program Files\IBM\Policy Director\lib\certs`

## Backing up the ACL data

Using the **migrate** command, back up the Policy Director ACL data.

To back up ACL information, type:
**AIX and Solaris:**

```
./migrate -f ldap_backup.xml -t backup -s acls
```

**Windows:**

```
migrate.exe -f ldap_backup.xml -t backup -r C:\Program
Files\IBM\Policy Director\lib -s acls
```

## Backing up the WebSEAL Smart Junction data

Using the **migrate** command, back up the Policy Director WebSEAL Smart Junction data.

To back up WebSEAL information, type:
**AIX and Solaris:**

```
./migrate -f ldap_backup.xml -t backup -s webseal
```

**Windows:**

```
migrate.exe -f ldap_backup.xml -t backup -r C:\Program
Files\IBM\Policy Director\lib -s webseal
```

## Upgrading your Policy Director version

To upgrade your Policy Director version:

1. Make sure that LDAP and DCE servers are running.
2. Uninstall Policy Director as described in the *IBM SecureWay Policy Director Up and Running*, Version 3.0 book.
3. Install Policy Director Version 3.0.1, following the same instructions used for installing Version 3.0 in the *IBM SecureWay Policy Director Up and Running* book.
4. Start Policy Director. Use the iv script to start all Policy Director servers in the correct order.

   See the *Policy Director Administration Guide* for more information on the iv script.
5. Log in as the cell administrator (`cell_admin`):

   ```
   dce_login cell_admin password
   ```

   Remember that restoration of migration data must be completed on the same server where you log in as the cell administator.

## Restoring the ACL data

Using the **migrate** command, restore the ACL information:

To restore previously backed up ACLs, type:

**AIX and Solaris:**

```
./migrate -f ldap_backup.xml -t restore -s acls -e ldap_aclerror.xml
```

**Windows:**

```
migrate.exe -f ldap_backup.xml -t restore -r C:\Program
Files\IBM\Policy Director\lib -s acls -e ldap_aclerror.xml
```

## Restoring the WebSEAL Smart Junction data

If you change from your previous server to a new and different server, you must change the WebSEAL server object entry. Edit the .XML intermediate file and type the name of the new WebSEAL server object before restoring the WebSEAL Smart Junction data.

Using the **migrate** command, restore the WebSEAL Smart Junction information.

To restore previously backed up WebSEAL Smart Junction data, type:

**AIX and Solaris:**

```
./migrate -f ldap_backup.xml -t restore -s webseal -e
ldap_weberror.xml
```

**Windows:**

```
migrate.exe -f ldap_backup.xml -t restore -r C:\Program
Files\IBM\Policy Director\lib -s webseal -e ldap_weberror.xml
```

## Restoring the Policy Director data

Be sure to restore the migration data on the same server where you log in as the cell administrator (cell_admin).

To restore the Policy Director data:

1. Stop the Policy Director-related servers by using the iv script to stop all Policy Director servers on a particular machine in the correct order.

   See the *Policy Director Administration Guide* for more information on the iv script.
2. Restore the Policy Director configuration files.

a. Using a comparison tool, compare the two sets of Policy Director configuration files (Version 3.0 and Version 3.0.1 files). The Version 3.0 files were copied in step 1 of "Backing up your Policy Director data" on page 16.
b. As a precaution, back up the newly installed Policy Director Version 3.0.1 configuration files.
c. Edit the following Policy Director Version 3.0.1 files, as necessary, to match the contents of the Version 3.0 files, except for user ID and password information.
   - ivmgrd.conf
   - secmgrd.conf
   - ivacld.conf
   - ldap.conf
   - iv.conf
   - cdas.conf

   **Note:** Keep the Version 3.0.1 user ID and password information in the these files: ivmgrd.conf, iv.conf, and ivacld.conf files.

3. Restore the Policy Director \certs directory:
   a. As a precaution, back up the newly installed Policy Director Version 3.0.1 \certs directory.
   b. Copy the Policy Director Version 3.0 \certs directory files that you previously backed up in step 2 in "Backing up your Policy Director data" on page 16 over the Version 3.0.1 \certs directory.
4. Restart Policy Director by using the iv script to start all Policy Director servers in the correct order.

   See the *Policy Director Administration Guide* for more information on the iv script.

## Restoring the LDAP data

You only need to restore the LDAP data if LDAP information has been lost during the migration.

1. Restore the LDAP directory data using either the **db2 restore** command or the LDAP **ldif2db** command.

   To use the db2 restore command, make sure the SecureWay Directory (LDAP) server is running and then type:

   ```
   db2 restore database dbname from directory_or_device
   ```

   Where *dbname* is the database name. For LDAP, `ldapdb2` is the default name of the database.

   LDAP provides the LDIF2DB program as part of the LDAP server installation. To use the **ldif2db** command:

   a. On the LDAP server that you are currently using for Version 3.0, change to one of the following subdirectories appropriate for your installation:

      **AIX:** `/usr/ldap/sbin`

      **Solaris:** `/opt/IBMldaps/sbin`

      **Windows:** `C:\Program Files\IBM\LDAP\bin`

   b. On the LDAP server, type the following command:

      ```
      ldif2db -i v30backup
      ```

Where *v30backup* is the name of the input file.

2. Compare the different versions of your LDAP configuration files, and restore as necessary. These files are included in the /etc subdirectory of your installation path:

   **AIX:** `/usr/ldap/etc`

   **Solaris:** `/opt/IBMldaps/etc`

   **Windows:** `C:\Program Files\IBM\LDAP\etc`

3. Start the LDAP server.

## Using a different LDAP server when upgrading

If you change to a different LDAP server for Policy Director Version 3.0.1 from the LDAP server you are now using but keep the same Policy Director server machine, use this procedure.

To change to a different LDAP server when migrating:

1. Stop the Policy Director-related servers.

   Be sure to use the iv script to stop all Policy Director servers on a particular machine in the correct order. See the *IBM SecureWay Policy Director Administration Guide, Version 3.0* for more information on the iv script.

2. When moving to a different LDAP server, refer to the "General Notes for Migrating Across Platforms" section of the *IBM SecureWay Directory Installation and Configuration, Version 3.1.1* documentation for instructions. There is a separate version of this book in HTML format for each of the supported operating systems. The book for each operating system is on the appropriate CD at /doc/wparent.htm.

   Also, review the Policy Director Version 3.0.1 README file for the most recent information on installing LDAP.

3. Change the ldap.conf configuration file located on the Policy Director server to point to the name of the new LDAP server (hostname), if necessary.

4. Restart the Policy Director servers.

   Be sure to use the iv script to start all Policy Director servers on a particular machine in the correct order. See the *IBM SecureWay Policy Director Administration Guide, Version 3.0* for more information on the iv script.

# Chapter 8. Editing XML input and output files

Migration requires that you specify an intermediate file, or files, for input when backing up and for output when restoring. During the migration or backup/restore processes, intermediate files are created that contain the data that must be upgraded, backed up or restored.

The intermediate file is an XML-formatted file.

- The XML file is a tagged, human-readable, and machine-parsable file.
- The XML file stores an entire representation of a configuration in a fashion that is independent from the Policy Director installation.
- The XML file's Document type definition (DTD) supports references (names or unique IDs). See "Appendix A. Document type definition" on page 33 for information about the specific DTD used by the Policy Director migration tool.
- The XML file can be edited when known bad records exist. When editing, be sure to maintain correct XML syntax.
- The XML file handles special characters such as > and < characters on backup and restore.

The Policy Director administrator can specify the following levels of migration by using the **-s** flag:

- all (which includes acls, webseal, and users)
- acls
- webseal
- users (DCE users and groups only)

**Note:** The current migration tool, version 3.0.1, does not support migration of NetSEAL information.

## Access control lists

Access control lists (ACLs) are objects within the Policy Director space that let you specify a security policy by enabling fine-grained access control to resources. These objects contain members (users or groups) for which you can provide permissions.

Policy Director restores ACL data to a server that is either in or not in the DCE cell of the original (backup) server. You can back up ACL information on one server and restore it on another server. None of the data is cell-dependent.

The restoration process makes information about all ACLs that are present on the system available, which includes:

**ACLNAME**
The name of the ACL.

**ATTACHED**
The reference to objects that are attached to the ACL.

**DESCRIPTION**
The description of the ACL.

**ACLINFO**

The information pertaining to the ACL, such as classes, names of classes, and permissions.

Permissions include:

| | |
|---|---|
| a | Attach, Base |
| A | Audit, Base |
| b | Browse, Base |
| c | Control, Base |
| C | Connect, NetSEAL |
| g | Delegation, Base |
| d | Delete, Generic |
| x | Execute, WebSEAL |
| f | Forward, NetSEAL |
| I | Integrity, Base |
| l | List Directory, WebSEAL |
| m | Modify, Generic |
| P | Privacy, Base |
| p | Proxy, NetSEAL |
| r | Read, WebSEAL |
| s | Server Admin, Generic |
| T | Traverse, Base |
| v | View, Generic |

**Note:** The proxy permission is not valid for the current version of Policy Director; however, this permission was used in previous versions.

The ACLs should be of this form:

```
<acldata>
    <aclname>testACL287</aclname>
    <description>This is a test ACL</description>
    <aclinfo>
        <class>Any-other</class>
        <permissions>
            <attach>
            <browse>
            <control>
            <traverse>
         </permissions>
    </aclinfo>
    <attached ID="8" OBJTYPE="PROTECTEDOBJ">
</acldata>
```

## Protected objects

A protected object is an object that exists within the object space that has an ACL attached to it.

Protected objects should be of the form:

```
<ivobj ID="0293" OBJTYPE="PROTECTEDOBJ">
    <path>/WebSEAL/296</path>
</ivobj>
```

## Actions

Non-default actions are actions that the administrator defines. You can use non-default actions over and above the Policy Director default permissions. Each non-default XML action entry must have a letter, label, and type associated with it. Non-default actions appear in the XML intermediate file.

Each default action has a unique ID associated with the XML entry. Default actions do not appear in the XML intermediate file.

If the **-x** flag is used with the migrate command, the action can force the restoration. The action and the dependent ACL information is written to a file that is named by the administrator, such as fail.xml. When you use the**-x** flag, the action in the database is replaced by the action information in the XML file. If you do not use the **-x** flag, the action will continue to fail.

You can restore action data to a server that is in the same DCE cell as the original (backup) server. Or, you can restore the data to a server that is in a different DCE cell. You can back up action information on one server and restore it to another server. None of the data is cell-dependent.

Policy Director extracts all information about non-default actions, writes the information to the XML file, and makes the information available to the restoration process. Policy Director does not write default actions to the XML file.

Actions should be of the form:

```
<ivobj ID="04" OBJTYPE="ACTION">
    <letter>Q</letter>
    <label>query information</label>
    <type>Query</type>
</ivobj>
```

# WebSEAL

WebSEAL Smart Junctions provide an HTTP junction to a third party or Policy Director Web server.

You can back up and restore all junction types. Policy Director extracts all information about Smart Junctions that is present on the system, and makes this information available to the restoration process.

You can only migrate WebSEAL junctions data between WebSEAL servers in the same DCE cell. When migrating WebSEAL junctions, the restoration of junctions must take place on a server that is within the same cell as the backup. This is because WebSEAL allows multiple servers within the same cell to contain junctions to other Web servers. Policy Director records these server names in the XML file.

This data includes junction-specific information that is needed to restore the junction. For example, as applicable, the migration tool includes the following WebSEAL information:

**ACTION**
The non-default actions that the administrator defines , which consists of LETTER, LEVEL, TYPE

**BASICAUTH**
The basic authentication handling values, which are the minimum acceptable level of security by which the Policy Director servers communicate —for Transmission Control Protocol (TCP) only.

**CASEINS**
The case-insensitive junction—for TCP only.

**CLIENTID**
The client identity used in the headers—for TCP only.

**DFSLOCDIR**
The location of the Distributed File Service (DFS) directory.

**GSOTARGET**
The name of the GSO resource.

**HOST** The host name of the target WebSEAL server.

**LABEL**
The descriptive label assigned to the none-default action.

**LETTER**
The letter assigned to the non-default action.

**MINQOP**
The Quality of Protection level.

**PATH** The file path name, such as /WebSEAL/296.

**PORT** The port number to junction to.

**SERVERNAME**
The name of the Web server.

**STATEFUL**
The option that defines a stateful TCP junction.

**TARGETIV**
The Policy Director server name that is being used as the junctioned server.

**TCPHOST**
The fully qualified host name of the TCP junctioned server.

**TYPE** The type of non-default action.

**URLQC**
The base HTTP URL of the server, such as /cgi-bin/query_contents.

**UUID** The universally unique identifier assigned to the user or group.

**VIRTHOSTNM**
The name of the junction as seen in the Web space.

**WIN32SUP**
The Win32 switch that tells WebSEAL to recognize two different file name extensions.

WebSEAL Smart Junctions should be of the form:

```
<IVMIG REGISTRY="DCE" DATE="Jan  6 2000">
 <IVOBJ ID="02" OBJTYPE="RROOT">
  <IVOBJ ID="03" OBJTYPE="WROOT">
   <IVOBJ ID="04" OBJTYPE="WEBSERVER">
    <SERVERNAME>bluering</SERVERNAME>
    <IVOBJ ID="05" OBJTYPE="WSROUTE">
     <NAME>/</NAME>
     <JUCTYPE>local</JUCTYPE>
     <DFSLOCDIR>/opt/intraverse/www/docs</DFSLOCDIR>
    </IVOBJ>
    <IVOBJ ID="06" OBJTYPE="WSROUTE">
     <NAME>/ibm.com</NAME>
     <JUCTYPE>tcp</JUCTYPE>
     <BASICAUTH>filter</BASICAUTH>
     <CLIENTID>do not insert</CLIENTID>
     <STATEFUL>no</STATEFUL>
     <UUID>8f297fd8-b2b2-11d3-8f4e-0a80007daa77</UUID>
     <HOST>webhost.surf.ibm.com</HOST>
     <PORT>80</PORT>
     <VIRTHOSTNM>webhost.surf.ibm.com:80</VIRTHOSTNM>
     <URLQC>/cgi-bin/query_contents</URLQC>
     <CASEINS>no</CASEINS>
     <WIN32SUP>no</WIN32SUP>
    </IVOBJ>
    <IVOBJ ID="07" OBJTYPE="WSROUTE">
     <NAME>/mulga</NAME>
     <JUCTYPE>tcp</JUCTYPE>
     <BASICAUTH>filter</BASICAUTH>
     <CLIENTID>do not insert</CLIENTID>
     <STATEFUL>no</STATEFUL>
     <UUID>43a6a2e8-b2b7-11d3-859d-0a80007daa77</UUID>
     <HOST>mulga.surf.ibm.com</HOST>
     <PORT>80</PORT>
     <VIRTHOSTNM>mulga.surf.ibm.com:80</VIRTHOSTNM>
     <URLQC>/cgi-bin/query_contents</URLQC>
     <CASEINS>no</CASEINS>
     <WIN32SUP>no</WIN32SUP>
    </IVOBJ>
   </IVOBJ>
  </IVOBJ>
 </IVOBJ>
</IVMIG>
```

The migration tool then restores all Smart Junctions from the backup source.

## Users

The migration tool allows these types of backup and restoration of Policy Director users and groups:

**DCE backup — LDAP restore**
For DCE backups, the migration tool provides a list of names of users and of groups as well as the details for the users or groups. When backing up DCE registry information about users and groups, you might need to edit the DCE data in the intermediate XML file. You can manually remove any user or group entries used for DCE internal purposes. During the restore process, DCE data is converted into a format that is acceptable as LDAP registry entries.

**Note:** The migration tool does not perform DCE user restorations because the recent versions of Policy Director recommend using the LDAP registry for user and group entries. Also, a limitation of the Policy Director migration tool concerns user password data. The migration tool does not migrate DCE password information. However, other than DCE user information, you can restore other types of DCE information, such as ACL and WebSEAL information, by using the migration tool.

**LDAP backup — LDAP restore**
For LDAP backups, information comes from ivmgrd.

The administrator must have `cell_admin` (or equivalent) authorization to perform the backup of DCE users. Also, when performing any LDAP migrations, you must perform the commands as an administrative user (such as `root`) of the local server.

Policy Director can restore user data to a server that is or is not in the DCE cell of the original (backup) server. Policy Director backs up user information on one server and restores it to any other server. None of the data is cell-dependent.

The tool extracts all information from the registry, including accounts, principals, and so forth. The migration tool has no upper limit on the number of users and groups it can migrate. RAM and virtual memory could limit the total number of entries the backup tool can handle.

## User password data

You can migrate LDAP user information into the LDAP registry. When you migrate or update LDAP user and group data and then restore to an LDAP registry, user password data is preserved.

Also, you can migrate DCE user information into the LDAP registry. When you migrate or update DCE user and group data and then restore to an LDAP registry, a hash value for the user's DCE password data is used instead. The migration tool extracts a user's password from DCE, creates, and uses the hash value for the DCE password.

You cannot migrate DCE user information back into a DCE registry. The most recent versions of Policy Director use the LDAP registry as the preferred directory, and so the migration tool restores user and group information only to the LDAP registry.

All users in the LDAP registry must specify a desired authentication method. When the user attempts to authenticate, Policy Director uses the specified authentication method to determine success or failure of the operation. When a DCE user is migrated into the LDAP registry, the authentication methods is set to `dce-migrate`. The dce-migrate authentication method initially uses the DCE registry for authentication. When successful, the migration tool saves the password for the user and sets the authentication method to `ldap` for all subsequent authentication attempts. The ldap authentication method uses normal password-style authentication. The password supplied must match the password stored for the user in LDAP.

After the first successful authentication, a migrated DCE user begins to use LDAP authentication. There is little or no administrator intervention required.

**Note:** This process requires that the original DCE registry remain in existence with the new LDAP registry until all users have successfully authenticated under the new LDAP registry.

## Example XML output file for DCE users and groups

For DCE users and groups, the XML file has headers similar to the following:

```
<ivobj ID="06" OBJTYPE="GROUPLIST">
    <ivobj ID="040" OBJTYPE="GROUP">
  <attr ATTRIBUTE="name" VALUE="group_0">
      <attr ATTRIBUTE="uuid" VALUE="000000c8-a90e-21d3-9801-005056820001">
<attr ATTRIBUTE="gid" VALUE="200">
      <attr ATTRIBUTE="alias" VALUE="no">
<attr ATTRIBUTE="inprojlist" VALUE="yes">
    </ivobj>
</ivobj>
<ivobj ID="043" OBJTYPE="USERLIST">
  <ivobj ID="066" OBJTYPE="USER">
      <attr ATTRIBUTE="name" VALUE="user_0">
<attr ATTRIBUTE="uuid" VALUE="000003e8-a90e-21d3-9800-005056820001">
<attr ATTRIBUTE="uid" VALUE="1000">
      <attr ATTRIBUTE="alias" VALUE="no">
<attr ATTRIBUTE="quota" VALUE="-1">
  <attr ATTRIBUTE="fullname" VALUE="BLOGGFEST">
<attr ATTRIBUTE="groups" VALUE="group_0">
  <attr ATTRIBUTE="acctvalid" VALUE="yes">
<attr ATTRIBUTE="client" VALUE="yes">
  <attr ATTRIBUTE="home" VALUE="/home/user_0">
<attr ATTRIBUTE="created" VALUE="/.../v2mulga/cell_admin 1999-12-02-23:16:42.000+00:00I-----">
<attr ATTRIBUTE="description" VALUE="test_user_user_0">
<attr ATTRIBUTE="dupkey" VALUE="no">
  <attr ATTRIBUTE="forwardabletkt" VALUE="yes">
<attr ATTRIBUTE="goodsince" VALUE="1999-12-02-23:16:42.000+00:00I-----">
<attr ATTRIBUTE="group" VALUE="group_0">
  <attr ATTRIBUTE="lastchange" VALUE="/.../v2mulga/cell_admin 1999-12-02-23:16:42.000+00:00I-----"
<attr ATTRIBUTE="organization" VALUE="org_0">
  <attr ATTRIBUTE="postdatedtkt" VALUE="no">
<attr ATTRIBUTE="proxiabletkt" VALUE="no">
  <attr ATTRIBUTE="pwdvalid" VALUE="yes">
<attr ATTRIBUTE="renewabletkt" VALUE="yes">
  <attr ATTRIBUTE="server" VALUE="yes">
<attr ATTRIBUTE="shell" VALUE="/bin/sh">
  <attr ATTRIBUTE="stdtgtauth" VALUE="yes">
</ivobj>
</ivobj>
```

## Example XML output file for LDAP users

For LDAP users, the XML file has headers similar to the following:

```
<ivobj ID="01025529171" OBJTYPE="USERLIST">
<ivobj ID="02" OBJTYPE="USER">
      <attr ATTRIBUTE="dn" VALUE="cn=user_fn_0000 user_sn_0,o=ibm,c=us">
<attr ATTRIBUTE="objectclass" VALUE="inetorgperson*eperson*organizationalperson*person*top">
<attr ATTRIBUTE="cn" VALUE="user_fn_0000 user_sn_0">
<attr ATTRIBUTE="sn" VALUE="user_sn_0">
<attr ATTRIBUTE="userpassword" VALUE="passwd">
<attr ATTRIBUTE="uid" VALUE="user_fn_0000">
<attr ATTRIBUTE="seclogintype" VALUE="Default:DCE-MIGRATE">
<attr ATTRIBUTE="secuuid" VALUE="019e66b0-ae02-11d3-b8e7-00062921db04">
</ivobj>
</ivobj>
```

## Example XML output file for LDAP groups

For LDAP groups, the XML file has headers similar to the following:

```
<ivobj ID="03" OBJTYPE="GROUPLIST">
<ivobj ID="04" OBJTYPE="GROUP">
<attr ATTRIBUTE="dn" VALUE="cn=group_0,cn=Access Groups,systemname=IBMGSO,o=ibm,c=us">
<attr ATTRIBUTE="objectclass" VALUE="accessGroup*top">
<attr ATTRIBUTE="cn" VALUE="group_0">
<attr ATTRIBUTE="member" VALUE="cn=user_fn_1000 user_sn_0,o=ibm,c=us">
<attr ATTRIBUTE="gid" VALUE="group_0">
<attr ATTRIBUTE="secuuid" VALUE="0261f5f8-ae02-11d3-b8e7-00062921db04">
</ivobj>
</ivobj>
```

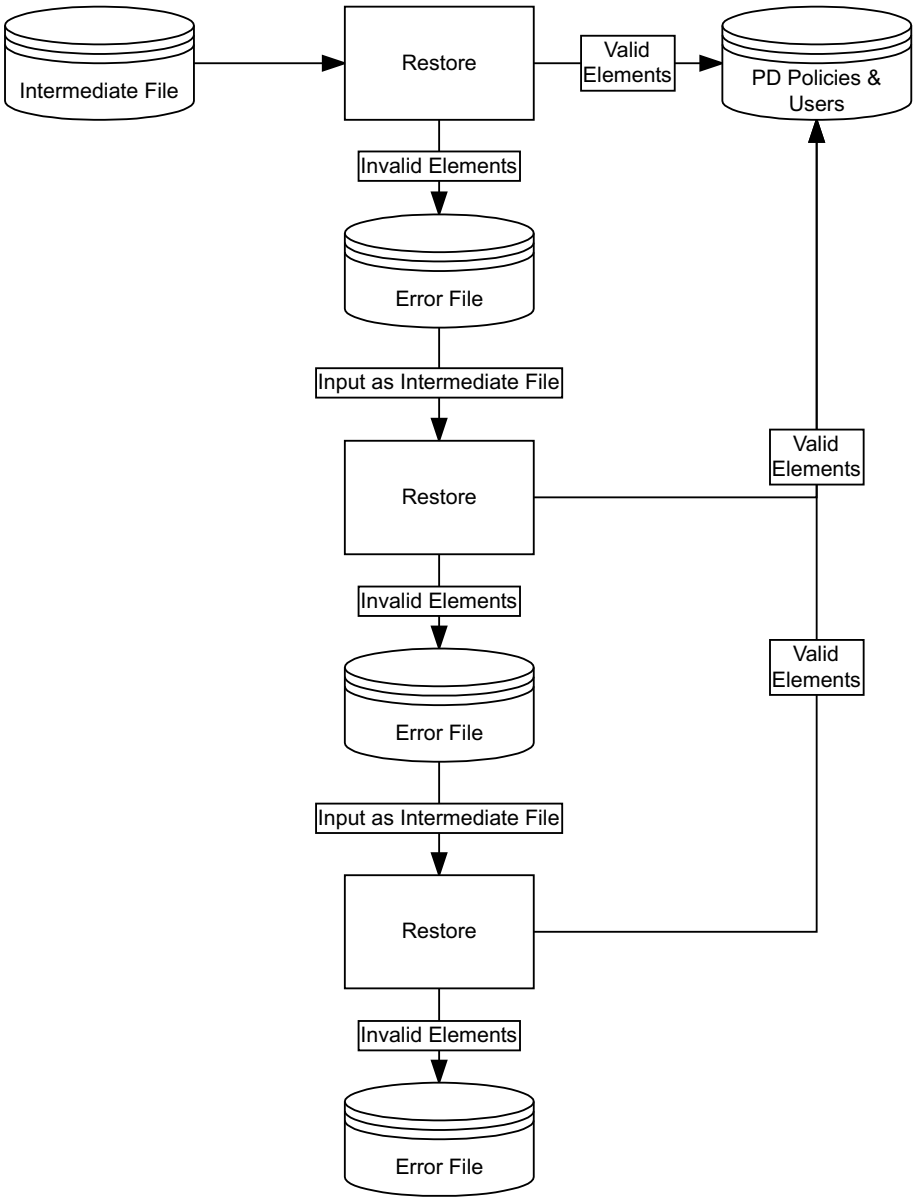
# Chapter 9. Reviewing log and error files

The migration tool provides these types of output files:

- Error file
- Log file

## Error file

The migration tool provides for error logging to an administrator-defined file. If no error file name is specified, the **migrate** command using the **-e** flag will fail. The administrator must specify an error file name.



The migration tool outputs the data into an XML-format error file. The error file is a partial copy of a full intermediate XML file. This error file captures a record of only the ACL, WebSEAL junction, user and group elements that fail to restore as well as any elements that the failed element depend on.

The administrator evaluates the errors in the partial error file, fixes the conditions that caused the errors, and then retries the restoration with only the elements that caused the errors. Following this process, the error file is the input file on each iterative round of error validation until the restoration is successful. and runs without errors.

## Log file

Log files are plain text files. If you do not specify a log file name when using the **-a** flag, the default name of the log file is migration.log.

The log files record all successful operations and all failed operations. Following is an example of a log record for successful completion:

```
SUCCESS: ivACLent - Successfully retrieved ACL from database: default-root
```

Also, following is an example of a log record where completion of an operation was not successful:

```
ERROR in ivactionent::restore():Command Dispatcher failed: Error trying to create action
```

# Chapter 10. Removing the migration files

Immediately after migrating or performing a successful backup, remove all the migration files to avoid shared library conflicts. You can save the backup XML files, as needed.

**AIX and Solaris:** Type the following to remove the migration tool files:

```
rm -fr installation-directory
```

Where the recommended *installation-directory* is the following subdirectory::

```
/opt/migration
```

**Windows:** Use the Windows Explorer utility to remove the installation directory. For example:

```
c:\PD301\migration
```

If you should ever need to perform another backup of a current installation, you will need to download, reinstall, and run the migration tool again. Or, you can save the migration .zip or .tar files.

# Appendix A. Document type definition

Extensible Markup Language (XML) lets you to create your own language. XML is a meta language that is used to create markup languages that describe data. XML is a database-neutral and device-neutral format.

You can target data that is marked up in XML to different devices by using Extensible Style Language (XSL). XML is truly extensible, rather than a fixed set of elements such as those that are used by HTML.

To construct your own XML language (also called a *vocabulary*), you supply a specific Document Type Definition (DTD). A DTD is a file (or several files to be used together) that is written in XML. The file contains a formal definition for a particular type of document. A DTD provides the rules that define the elements and structure of your new language. It sets out what names can be used for element types, where they can occur, and how they can all fit together. DTDs consist of elements and attributes. DTDs define the elements, element attributes, and relationship between elements in a XML document.

For example, in an employee record, the DTD might include a rule that states that the element consists of three other elements called ″first″, ″middle,″ and ″last.″ The rule would also indicate whether any of the nested elements is optional, can be repeated, or has a default value.

XML is the formal specification language that processors read to automatically parse the DTD. Any browser or application with an XML parser can interpret this employee document instance by learning the rules defined by the DTD. No prior knowledge of the sender application is necessary because the syntax of an XML document instance describes the relationships among the various elements by using the DTD.

The information in the DTD identifies where every element type comes. The DTD information identifies how each element relates to another so that stylesheets, navigators, browsers, search engines, databases, printing routines, and other applications can be used. In effect, a DTD provides applications with advance notice of what names and structures can be used in a particular document type. Using a DTD means that you can be certain that all documents, which belong to a particular type, are constructed and named in a conforming manner.

HTML describes document structure and visual presentation. In contrast, XML describes data in a human-readable format with no indication of how the data is to be displayed. How data appears in print or on the screen depends on your stylesheet. Typically, you do not put anything in the XML that affects formatting.

Following is the DTD that describes the data that is backed up and restored by the Policy Director migration tool:

```
<?xml version="1.0"?>
<!DOCTYPE IVMIG [
<!--Top-level element: IVMIG -->
<!ELEMENT IVMIG ( IVOBJ?, ACLLIST? )* >
<!ATTLIST IVMIG REGISTRY CDATA #REQUIRED
              DATE CDATA #REQUIRED >
<!-- Records -->
<!-- ACL List element -->
<!ELEMENT ACLLIST ( ACLDATA )* >
<!-- ACLDATA record  -->
<!ELEMENT ACLDATA ( ACLNAME, DESCRIPTION, ACLINFO*, ATTACHED* ) >
<!ELEMENT ACLNAME ( #PCDATA ) >
<!ELEMENT DESCRIPTION ( #PCDATA ) >
<!-- ACLINFO record -->
<!ELEMENT ACLINFO ( CLASS, NAME?, PERMISSIONS ) >
<!ELEMENT CLASS ( #PCDATA ) >
<!ELEMENT NAME ( #PCDATA ) >
<!ELEMENT PERMISSIONS ( (ATTACH?| AUDIT?| BROWSE?| CONTROL?| DELEGATION?|
                        INTEGRITY?| PRIVACY?| TRAVERSE?| DELETE?| MODIFY?|
                        SERVERADM?| VIEW?| CONNECT?| PROXY?| LIST?| READ?|
                        EXECUTE?| FORWARD?| IVOBJ )* ) >
<!-- ACL permission tags -->
<!ELEMENT ATTACH EMPTY >
<!ELEMENT AUDIT EMPTY >
<!ELEMENT BROWSE EMPTY >
<!ELEMENT CONTROL EMPTY >
<!ELEMENT DELEGATION EMPTY >
<!ELEMENT INTEGRITY EMPTY >
<!ELEMENT PRIVACY EMPTY >
<!ELEMENT TRAVERSE EMPTY >
<!ELEMENT DELETE EMPTY >
<!ELEMENT MODIFY EMPTY >
<!ELEMENT SERVERADM EMPTY >
<!ELEMENT VIEW EMPTY >
<!ELEMENT CONNECT EMPTY >
<!ELEMENT PROXY EMPTY >
<!ELEMENT LIST EMPTY >
<!ELEMENT READ EMPTY >
<!ELEMENT EXECUTE EMPTY >
<!ELEMENT FORWARD EMPTY >
<!-- ATTACHED record.  Lists a reference to attached objects.-->
<!ELEMENT ATTACHED EMPTY >
<!ATTLIST ATTACHED ID CDATA #REQUIRED
                   OBJTYPE CDATA #REQUIRED >
<!-- IVOBJ record.  This is for everything that is not an ACL. -->
<!ELEMENT IVOBJ ( ((
   LETTER|LABEL|TYPE|NAME|PATH|ATTR|SERVERNAME|JUCTYPE|
   BASICAUTH|DFSLOCDIR|CLIENTID|STATEFUL|UUID|HOST|PORT|
   VIRTHOSTNM|URLQC|CASEINS|WIN32SUP )? | IVOBJ)* )>
<!ATTLIST IVOBJ ID CDATA #REQUIRED
                OBJTYPE (WSROUTE|WEBSERVER|USERLIST|GROUPLIST|
   GROUP|USER|RROOT|MROOT|WROOT|ACTION|PROTECTEDOBJ) #REQUIRED >
<!ELEMENT ATTR EMPTY >
<!ATTLIST ATTR ATTRIBUTE CDATA #REQUIRED
    VALUE CDATA #REQUIRED >
<!ELEMENT WEBSERVER ( SERVERNAME, IVOBJ* )>
<!ELEMENT WEBROUTE ( NAME, JCTTYPE, ( BASICAUTH?, CLIENTID?, CASEINS?,
     TCPHOST?, TCPPORT?, URLQC?, STATEFUL?, GSOTARGET?,
     VIRTHOSTNM?, WIN32SUP?, MINQOP?, TAGRGETIV?, UUID?,
     DFSLOCDIR )* ) >
<!ELEMENT PROTECTEDOBJ ( PATH ) >
```

```
<!-- WebSEAL junction information -->
<!ELEMENT BASICAUTH ( #PCDATA ) >
<!ELEMENT CLIENTID ( #PCDATA ) >
<!ELEMENT CASEINS ( #PCDATA ) >
<!ELEMENT TCPHOST ( #PCDATA ) >
<!ELEMENT TCPPORT ( #PCDATA ) >
<!ELEMENT URLQC ( #PCDATA ) >
<!ELEMENT STATEFUL ( #PCDATA ) >
<!ELEMENT GSOTARGET ( #PCDATA ) >
<!ELEMENT VIRTHOSTNAME ( #PCDATA ) >
<!ELEMENT WIN32SUP ( #PCDATA ) >
<!ELEMENT MINQOP ( #PCDATA ) >
<!ELEMENT TARGETIV ( #PCDATA ) >
<!ELEMENT DFSLOCDIR ( #PCDATA ) >
<!ELEMENT SERVERNAME ( #PCDATA ) >
<!ELEMENT ACTION ( LETTER, LEVEL, TYPE ) >
<!ELEMENT LETTER ( #PCDATA ) >
<!ELEMENT LABEL ( #PCDATA ) >
<!ELEMENT TYPE ( #PCDATA ) >
<!ELEMENT UUID ( #PCDATA ) >
<!ELEMENT HOST ( #PCDATA ) >
<!ELEMENT PORT ( #PCDATA ) >
<!ELEMENT VIRTHOSTNM ( #PCDATA ) >
<!ELEMENT PATH ( #PCDATA ) >
] >
```

# Appendix B. Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

**The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:**
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the information. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this information at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Department LZKS
11400 Burnet Road
Austin, TX 78758
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. *_enter the year or years._* All rights reserved.

## Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, or other countries, or both:

AIX
FirstSecure
IBM
SecureWay

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark in the United States, other countries, or both and is licensed exclusively through The Open Group.

Other company, product, and service names may be trademarks or service marks of others.

# Index

## Special Characters



## A



## B



## C



## D



## E

# T



# U



# V



# W



# X



# Y

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