

# **Tivoli Policy Director - Version 3.8 Installation Guidelines/Cookbook**

## **Windows, AIX and Solaris**

***Vaughan Harper***  
***EMEA Tivoli Security Product Manager***

Vaughan Harper/UK/IBM@IBMGB  
vaughan\_harper@uk.ibm.com

IBM United Kingdom Limited  
76 Upper Ground  
London  
SE1 9PZ  
United Kingdom

Tel +44 20 7202 3127

***Martin Borrett***  
***EMEA Tivoli Security Specialist***

Martin Borrett/UK/IBM@IBMGB  
borretm@uk.ibm.com

Tel +44 1962 817232



Version 0.8 – 25 September, 2001

## Preface

This is not a formal document, so please notify the authors of any errors, omissions or suggested changes.

This publication is intended to help solution architects, planners and system administrators to understand and implement security features on their intranet and on the Internet based on technology provided by Tivoli Policy Director. The information in this publication is not intended as the specification of any programming interfaces that are provided by Tivoli Policy Director, or any other products mentioned. See the PUBLICATIONS section of the IBM Programming Announcement for the IBM products, or contact the vendors for non-IBM products for more information about what publications are considered to be product documentation.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM ("vendor") products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

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 the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, NY 10594 USA.

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, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA. Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries: AIX®, AIX/6000®, IBM®, RISC System/6000®, DB2®, SecureWay®, WebSphere (TM) .

The following terms are trademarks of other companies: Microsoft, Windows, Windows NT, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation. UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited. Other company, product, and service names may be trademarks or service marks of others.

### **Acknowledgements**

Very few of the ideas here are original. In particular, thanks to the following people for their input: David Lin, Tony Lai and George Dever from IBM Austin, Avery Salmon from the PIC at IBM Hursley, Sanjiev Chattopadhyaya from the PKI Solutions Team, Gaithersburg, Jorge Ferrari from the WW Security Competency Center, Julie Peet Szafranski from the IBM Design Center for e-Transaction Processing in Poughkeepsie, Chris Hockings from IBM Australia and Shali Goradia.

In addition, special thanks to Jon Harry from the PIC at IBM Hursley for his work on the Easy Install processes and Gary Linker from the Level 2 team in Austin for his work on Windows 2000 installation.

---

## Table of Contents

Table of Contents .....	iii
<b>Part I - Introduction and Roadmaps.....</b>	<b>1</b>
<b>1. Introduction .....</b>	<b>1</b>
<b>2. Installation Road Maps.....</b>	<b>2</b>
<b>Part II - Windows Environment.....</b>	<b>7</b>
<b>3. Windows System preparation (operating system,etc) .....</b>	<b>7</b>
<b>4. Easy Install.....</b>	<b>8</b>
4.1 Easy Install of the IBM SecureWay Directory.....	8
4.2 Easy Install of Policy Director Management Server (PDMgr).....	13
4.3 Easy Install of Policy Director WebSEAL (PDWeb) .....	17
<b>5. Easy Install process to Set up Policy Director components on a remote machine.....</b>	<b>19</b>
5.1 Easy Install of Policy Director WebSEAL (PDWeb) .....	19
5.2 Easy Install of Web Portal Manager (PDWPM) .....	24
5.3 Changing ports for Web Portal Manager .....	30
<b>6. Native installation process .....</b>	<b>33</b>
6.1 GSKit installation (Windows).....	33
6.2 LDAP Server installation (Windows) .....	36
6.3 LDAP Client installation (Windows).....	44
6.4 Policy Director Servers installation (Windows).....	48
6.5 Install Policy Director Runtime Environment (PDRTE) (Windows).....	51
6.6 Install WebSEAL (Windows) .....	54
6.7 LDAP Server configuration (Windows) .....	57
6.8 Directory Management Tool steps .....	66
6.9 Policy Director Configuration (Windows).....	69
6.10 Policy Director RTE + WebSEAL Configuration (Windows).....	75
6.11 Web Portal Manager Installation & Configuration (Windows) .....	79
<b>Part III - AIX Environment .....</b>	<b>90</b>
<b>7. AIX System Preparation and general AIX Notes .....</b>	<b>90</b>
<b>8. LDAP Server installation/configuration (AIX).....</b>	<b>92</b>
8.1 Operating system pre-requisites .....	92
8.2 Install the IBM HTTP Server .....	92
8.3 Install GSKit .....	94
8.4 Install IBM Universal Database (DB2).....	94
8.5 Install IBM SecureWay Directory.....	95
8.6 Configure LDAP .....	96
8.7 Add Policy Director Suffixes .....	98
8.8 Directory Management Tool steps .....	101
<b>9. Policy Director Server installation (AIX).....</b>	<b>105</b>
<b>10. WebSEAL Installation (AIX).....</b>	<b>106</b>
<b>11. Policy Director Configuration (AIX).....</b>	<b>107</b>
<b>12. Useful commands for Policy Director in the AIX environment.....</b>	<b>112</b>
LDAP .....	112
PD .....	112

Policy Director Processes.....	112
AIX .....	112
<b>Part IV - Solaris Environment .....</b>	<b>113</b>
<b>13. Solaris System Preparation and general Solaris Notes.....</b>	<b>113</b>
<b>14. Easy Installation Process for Solaris .....</b>	<b>113</b>
14.1 IBM SecureWay Directory and Prerequisite Installation and Configuration .....	113
14.2 Policy Director RTE and Mgr Installation and Configuration .....	116
14.3 WebSEAL Install and Configuration .....	119
<b>15. Policy Director Component Configuration &amp; Unconfiguration (Solaris).....</b>	<b>121</b>
<b>16. Useful commands for Policy Director in the Solaris environment .....</b>	<b>121</b>
LDAP .....	121
Directory Management Tool steps .....	121
PD .....	122
Solaris .....	122
<b>Part V - Generic Product Configuration .....</b>	<b>123</b>
<b>17. Initial Policy Director Validation .....</b>	<b>123</b>
<b>18. Further Policy Director Configuration .....</b>	<b>128</b>
Directory Management Tool.....	133
<b>19. Query_contents – additional notes .....</b>	<b>134</b>
Query_contents with Lotus Domino Go Webserver .....	134
Query_contents with Netscape Enterprise Server under AIX .....	134
<b>20. Setting up a WebSEAL server certificate .....</b>	<b>135</b>
Approach (a) - Generating a self-signed certificate .....	135
Approach (b) - Certificate Signing Request sent to Tivoli PKI .....	139
Approach (c) - Certificate Signing Request sent to Entrust CA .....	150
Additional notes .....	160
<b>21. Setting up client certificate authentication .....</b>	<b>161</b>
<b>22. Setting up an SSL connection to the LDAP Directory .....</b>	<b>164</b>
LDAP Server - create the key database file .....	164
LDAP Client (Policy Director Server components) - create the key database file.....	170
LDAP Client (Policy Director Server) - install LDAP Server certificate .....	171
Configuring PDRTE for SSL communication to LDAP.....	174
<b>23. Installation of SecurID token support.....</b>	<b>176</b>
Problem Determination .....	186
Uninstalling.....	186
Problem:.....	186
<b>24. Sharing an LDAP Directory between Policy Director and Trust Authority .....</b>	<b>188</b>
<b>25. Useful LDAP commands .....</b>	<b>190</b>
<b>26. Troubleshooting... ..</b>	<b>191</b>
Policy Director won't start. . . . .	191
Problems once Policy Director has started. . . . .	191
Page Not Found problems. . . . .	192
Running IP traces.....	193
LDAP Problems .....	194
Policy Director Debug Mode .....	194
Other problem determination ideas - AIX.....	194

**27. Publications .....195**



# Part I - Introduction and Roadmaps

---

## 1. Introduction

This document should be read in conjunction with the formal product documentation. It is not an overview or description of Policy Director, but its scope is strictly limited to being a hands on guide designed to assist those installing Tivoli Policy Director. The aim is to share lessons learned from installation adventures with a wider audience.

It should be noted that this document is not comprehensive, and certainly does not cover all possible permutations - but it is hoped that it will be better than nothing...

**Note:** Before going any further, it is worth reviewing the latest README and the formal product documentation - see the **Publications** section at the end of this document for guidance on the location of these documents.

**Further note:** Please do feed back any comments on this document to the authors.

### **General note regarding LDAP and Policy Director**

It is worth noting that (unlike in previous releases) Policy Director will not start without LDAP running.

## 2. Installation Road Maps

First of all, you need to decide which components will be installed on which boxes. Some of the typical scenarios are as follows:

### Scenario (a) – everything on a single box

(This is fine for a demonstration system.)

Policy Director Servers LDAP WebSEAL
--

### Scenario (b) – WebSEAL on one box; Policy Director Servers and LDAP on a separate box

(The WebSEAL box(es) are likely to be in the DMZ, while the Policy Director Servers and LDAP are likely to be in the intranet (or a separate network).)

Policy Director Servers LDAP
---------------------------------

WebSEAL
---------

### Scenario (c) – everything on separate boxes

Policy Director Servers
-------------------------

LDAP
------

WebSEAL
---------

From this, you can determine which combinations of products need to be installed in which boxes.



Note that for Windows (that it Windows 2000 or Windows NT), the general approach described here is first to install all the required components, then to configure them all. This approach minimises the number of re-boots necessary. (Probably the WPM components could be installed and configured with the rest of Policy Directory – but we haven't tested this.) It is also worth noting that Web Portal Manager runs only on Windows (and hence does not appear on the AIX/Solaris sections of the combinations below.)

<p><b>Combination (i) – Policy Director Servers, IBM SecureWay Directory (LDAP), WPM and WebSEAL</b></p>
<p><i>Components required:</i></p> <ul style="list-style-type: none"> <li>• GSKit</li> <li>• IBM HTTP Server</li> <li>• IBM SecureWay Directory</li> <li>• Policy Directory Servers</li> <li>• WebSEAL</li> <li>• WebSphere Application Server (installed as part of the Web Portal Manager installation process)</li> <li>• Web Portal Manager (WPM) (Windows only)</li> </ul>
<p><i>Sequence of steps to follow on Windows:</i></p> <ul style="list-style-type: none"> <li>• Install GSKit</li> <li>• Install IBM HTTP Server</li> <li>• Install LDAP Server</li> <li>• Install Policy Director Server packages (pdrte, pdmgrd, pdacld, pdweb)</li> <li>• Re-boot</li> <li>• Configure LDAP</li> <li>• Configure Policy Director Server packages (pdrte, pdmgrd, pdacld, pdweb)</li> <li>• Install and Configure Web Portal Manager (WPM)</li> </ul>
<p><i>Sequence of steps to follow on AIX/Solaris:</i></p> <ul style="list-style-type: none"> <li>• Install GSKit</li> <li>• Install IBM HTTP Server</li> <li>• Install LDAP Server</li> <li>• Configure LDAP Server</li> <li>• Install Policy Director packages</li> <li>• Configure Policy Director packages</li> </ul>

**Combination (ii) – Policy Director Servers, IBM SecureWay Directory (LDAP), WPM but not WebSEAL**

*Components required:*

- GSKit
- IBM HTTP Server
- IBM SecureWay Directory
- Policy Directory Servers
- WebSphere Application Server (installed as part of the Web Portal Manager installation process)
- Web Portal Manager (WPM) (Windows only)

*Sequence of steps to follow on Windows:*

- Install GSKit
- Install IBM HTTP Server
- Install LDAP Server
- Install Policy Director Server packages (pdrte, pdmgrd, pdaclD)
- Re-boot
- Configure LDAP
- Configure Policy Director Server packages (pdrte, pdmgrd, pdaclD)
- Install and Configure Web Portal Manager (WPM)

*Sequence of steps to follow on AIX/Solaris:*

- Install GSKit
- Install IBM HTTP Server
- Install LDAP Server
- Configure LDAP Server
- Install Policy Director packages
- Configure Policy Director packages

### **Combination (iii) – Policy Director Servers and WPM**

*Components required:*

- GSKit
- IBM HTTP Server
- LDAP Client
- Policy Directory Servers
- WebSphere Application Server (installed as part of the Web Portal Manager installation process)
- Web Portal Manager (WPM) (Windows only)

*Sequence of steps to follow on Windows:*

- Install GSKit
- Install IBM HTTP Server
- Install LDAP Client
- Install Policy Director Server packages (pdrte, pdmgrd, pdacl)
- Re-boot
- Configure Policy Director Server packages (pdrte, pdmgrd, pdacl)
- Install and Configure Web Portal Manager (WPM)

*Sequence of steps to follow on AIX/Solaris:*

- Install GSKit
- Install IBM HTTP Server
- Install LDAP Client
- Install Policy Director packages
- Configure Policy Director packages

<b>Combination (iv) – WebSEAL only</b>
<i>Components required:</i> <ul style="list-style-type: none"><li>• GSKit</li><li>• LDAP Client</li><li>• WebSEAL</li></ul>
<i>Sequence of steps to follow on Windows:</i> <ul style="list-style-type: none"><li>• Install GSKit</li><li>• Install LDAP Client</li><li>• Install WebSEAL</li><li>• Re-boot</li><li>• Configure WebSEAL</li></ul>
<i>Sequence of steps to follow on AIX/Solaris:</i> <ul style="list-style-type: none"><li>• Install WebSEAL (including pre-requisite packages – this pulls in GSKit and LDAP Client)</li><li>• Configure WebSEAL</li></ul>

<b>Combination (v) – IBM SecureWay Directory (LDAP) only</b>
<i>Components required:</i> <ul style="list-style-type: none"><li>• GSKit</li><li>• IBM HTTP Server</li><li>• IBM SecureWay Directory</li></ul>
<i>Sequence of steps to follow on Windows:</i> <ul style="list-style-type: none"><li>• Install GSKit</li><li>• Install IBM HTTP Server</li><li>• Install LDAP Server</li><li>• Re-boot</li><li>• Configure LDAP</li></ul>
<i>Sequence of steps to follow on AIX/Solaris:</i> <ul style="list-style-type: none"><li>• Install GSKit</li><li>• Install IBM HTTP Server</li><li>• Install LDAP Server</li><li>• Configure LDAP Server</li></ul>

---

## Part II - Windows Environment

**Note:** the PD 3.8 installation process has been simplified considerably by the provision of a set of Easy Installation procedures. In this section we have documented here both the Easy Installation procedures and the Native installation procedures, as there may be occasions where the easy install may fail and you may need to revert to part of the Native process.

---

### 3. Windows System preparation (operating system,etc)

*Throughout this document the term **Windows** is used to refer to both **Windows NT** and **Windows 2000**. Note also that **Windows 2000 Server** or **Advanced Server** is required – **Windows 2000 Professional** is not supported.*

- Ensure that the date and time are set correctly across the environment you are using, this is a sensible step and may avoid problems later on.
- Ensure that Microsoft NT **Server** 4.0 is installed, with Service Pack 5 or higher, or else Windows 2000 **Server**.
- Ensure that you have IP connectivity (for example, attempt to 'ping' another machine).
- It is **much** easier to install Policy Director if you can start with a 'clean' machine with a fresh Windows install on it. Otherwise, if there are files left over from previous installs you are likely to hit more obstacles along the way. (Some of the ways of avoiding these problems have been documented – but there are sure to be more which are not documented.)

#### Loopback Adapter

If a stand-alone demonstration system is being set up, you may want to consider using the MS Loopback Adapter rather than a genuine LAN adapter. To install this, insert a Windows NT Server 4.0 CD-ROM in the CD-ROM drive; use Start -> Settings -> Network, click on '**Adapters**', click on '**Add...**', select '**MS Loopback Adapter**', click on '**OK**', click on '**OK**', click on '**Close**'. You will then need to specify an IP address for this adapter. You will probably also need to add an entry in C:\Winnt\system32\drivers\etc\hosts mapping IP address to fully qualified hostname in order to get reverse DNS to work.

## 4. Easy Install

Version 3.8 of Policy Director now provides a quick installation path using batch files for Windows environments such as Windows 2000 Server and Windows NT Server. These scripts make it easy to install Policy Director by automatically installing required software and prerequisites. They let you see what components are currently installed and prompt you for configuration information. Below is documented a basic install using these batch files.

### 4.1 Easy Install of the IBM SecureWay Directory

First we will use the **ezinstall\_idap\_server** batch file. This sets up a workstation with the following packages; IBM DB2 v6.1 + FP3, GSKit, IBM HTTP Server, IBM SecureWay Directory Client and Server v3.2.1 together with efix4.

- a. Insert the Tivoli SecureWay Policy Director Base for Windows Version 3.8 CD
- b. Using 'My Computer' or 'Windows Explorer' open the root directory of the CD and launch the ezinstall\_idap\_server.bat file by double-clicking on it.
- c. ezinstall starts in a command window:

```
IBM SecureWay Directory Server
Installation and Configuration

-----

Product                                Status
IBM DB2 ..... Not Installed
IBM HTTPD Server ..... Not Installed
IBM Global Security Toolkit 4 ..... Not Installed
IBM SecureWay Directory Client ..... Not Installed
IBM SecureWay Directory Server ..... Not Installed

Press ENTER to continue...
```

- d. This shows the current status of the components required for IBM SecureWay Directory. Press 'Enter'. The DB2 Configuration options are displayed

```
IBM DB2 Configuration Options
-----

Option                                Value
1. Administration Password ..... *****
2. Installation Directory ..... C:\SQLLIB

Enter the number of the option to modify or Y to continue: 1

Enter the Administration Password: *****

Re-enter the password for confirmation: *****
```

- e. Set the password for the db2admin Windows user that will be created (we used **Secure99**). If left as the default this would be db2admin. The configuration is updated.

```

IBM DB2 Configuration Options
-----
Option                                     Value
1. Administration Password ..... *****
2. Installation Directory ..... C:\SQLLIB

Enter the number of the option to modify or Y to continue:
    
```

- f. Enter **'y'** to confirm the displayed settings. The HTTP Server Configuration Options are displayed.

```

IBM HTTP Server Configuration Options
-----
Option                                     Value
1. Administration ID ..... administrator
2. Administration Password .....
3. HTTP Port ..... 80
4. Installation Directory ..... C:\Program Files\IBM HTTP Server

Enter the Administration Password:
    
```

- g. Enter the Windows Administrator password (which is **Secure99** in our case). This is what the HTTP Server will use to start as an Windows service. The options are re-displayed.

```

IBM HTTP Server Configuration Options
-----
Option                                     Value
1. Administration ID ..... administrator
2. Administration Password ..... *****
3. HTTP Port ..... 80
4. Installation Directory ..... C:\Program Files\IBM HTTP Server

Enter the number of the option to modify or Y to continue: 3

Enter the HTTP Server Port Number: 81
    
```

- h. At this point we selected (3) to change the HTTP listening port from 80 to 81 in our case. In order to avoid port conflicts with WebSEAL later on, which by default listens on port 80. The results of this change are shown below.

```

IBM HTTP Server Configuration Options
-----
Option                                     Value
1. Administration ID ..... administrator
2. Administration Password ..... *****
3. HTTP Port ..... 81
4. Installation Directory ..... C:\Program Files\IBM HTTP Server

Enter the number of the option to modify or Y to continue: y
    
```

- i. Press **'y'** to continue, the IBM GSKIT Configuration Options are displayed.

```

IBM Global Security Toolkit
-----
Option                                     Value
1. Installation Directory ..... C:\Program Files\IBM\GSK
    
```

```
Enter the number of the option to modify or Y to continue: y
```

j. Enter 'y' to accept the default installation directory for IBM GSKIT. The LDAP Client Configuration Options are displayed.

```
IBM SecureWay Directory Client
-----
Option                                     Value
1. Installation Directory ..... C:\Program Files\IBM\LDAP

Enter the number of the option to modify or Y to continue: y
```

k. Enter 'y' to accept the default installation directory for IBM LDAP Client. The LDAP Server Configuration Options are displayed.

```
IBM SecureWay Directory Server Configuration Options
-----
Option                                     Value
1. LDAP Administrator ID (DN) ..... cn=root
2. LDAP Administrator Password .....
3. LDAP Server Hostname ..... secure2.pisc.uk.ibm.com
4. Suffix .....
5. LDAP Server Port ..... 389
6. LDAP SSL Keyfile ..... D:\common\pd_ldapkey.kdb
7. LDAP SSL Key File Password .....
8. SSL Client Certificate Label ..... PDLLDAP
9. Installation Directory ..... C:\Program Files\IBM\LDAP

Enter the LDAP Administrator Password: *****
Re-enter the password for confirmation: *****
```

l. Enter the password to be used for the LDAP Admin user (cn=root). Type again to confirm. (We used **secure99**.)

```
IBM SecureWay Directory Server Configuration Options
-----
Option                                     Value
1. LDAP Administrator ID (DN) ..... cn=root
2. LDAP Administrator Password .....
3. LDAP Server Hostname ..... secure2.pisc.uk.ibm.com
4. Suffix .....
5. LDAP Server Port ..... 389
6. LDAP SSL Keyfile ..... D:\common\pd_ldapkey.kdb
7. LDAP SSL Key File Password .....
8. SSL Client Certificate Label ..... PDLLDAP
9. Installation Directory ..... C:\Program Files\IBM\LDAP

Enter the Suffix:
```

m. Enter the suffix you want to be created for storage of Policy Director users and groups (we used **o=ibm,c=gb**).

```
IBM SecureWay Directory Server Configuration Options
-----
```



```

Option                                     Value
1. LDAP Administrator ID (DN) ..... cn=root
2. LDAP Administrator Password ..... *****
3. LDAP Server Hostname ..... secure2.pisc.uk.ibm.com
4. Suffix ..... o=ibm,c=gb
5. LDAP Server Port ..... 389
6. LDAP SSL Keyfile ..... D:\common\pd_ldapkey.kdb
7. LDAP SSL Key File Password ..... *****
8. SSL Client Certificate Label ..... PDLLDAP
9. Installation Directory ..... C:\Program Files\IBM\LDAP

Enter the number of the option to modify or Y to continue: y
    
```

n. Enter ‘y’ to confirm the displayed settings. The LDAP keystore provided is copied onto the hard drive and you will see the message:

```

The SSL Client Keyfile: D:\common\pd_ldapkey.kdb will be copied to
c:\keytabs\pd_ldapkey.kdb.
Press ENTER to continue...
    
```

o. Press ‘Enter’ to continue. The installation and configuration begins. This takes a few minutes – but don’t go away because you need to be around to re-boot the machine. You will see screens similar to below.

```

IBM SecureWay Directory Server
Installation and Configuration
-----

Product                                     Status
IBM DB2 ..... Not Installed
IBM HTTPD Server ..... Not Installed
IBM Global Security Toolkit 4 ..... Not Installed
IBM SecureWay Directory Client ..... Not Installed
IBM SecureWay Directory Server ..... Not Installed

Installing DB2.

To complete the installation/configuration, the system must be restarted
Press ENTER to continue...
    
```

p. When the message shown above is displayed press ‘ENTER’ to re-boot the machine. Once the machine has finished re-booting sign in as Administrator (cfguser and Secure99 in our case). The ezinstall will automatically carry on where it left off with the installation of the HTTP Server:

```

IBM SecureWay Directory Server
Installation and Configuration
-----

Product                                     Status
IBM DB2 ..... Configured [6]
IBM HTTPD Server ..... Configured [1.3.12]
IBM Global Security Toolkit 4 ..... Configured [4.0.3.168]
IBM SecureWay Directory Client ..... Configured [3.2]
IBM SecureWay Directory Server ..... Not Installed

Installing IBM SecureWay Directory Server.
    
```

To complete the installation/configuration, the system must be restarted  
 Press ENTER to continue...

q. When the message shown above is displayed press '**ENTER**' to re-boot the machine. Once the machine has finished re-booting sign in as Administrator. The ezinstall will automatically carry on where it left off with the configuration of the IBM SecureWay Directory. You will see the progress in the command window as shown below:

```
*****
Some lines missing here...
*****

Creating the directory DB2 default database.
This operation may take a few minutes.

Configuring the database.
Adding user account: ldapdb2.
Adding user account, ldapdb2, to the Administrators group.
Adding account rights to account: ldapdb2.
Added account rights to account: ldapdb2.
Creating database instance: ldapdb2.
Created database instance: ldapdb2.
Logging on user: ldapdb2.
Logged on user: ldapdb2.
Impersonating user.
Impersonated user.
Logging on user: ldapdb2.
Logged on user: ldapdb2.
Impersonating user.
Impersonated user.
Cataloging node: ldapdb2.
Cataloged node: ldapdb2.
Starting database manager for instance: ldapdb2.
Started database manager for instance: ldapdb2.
Attaching to instance: ldapdb2.
Attached to instance: ldapdb2.
Creating database: ldapdb2.
Created database: ldapdb2.
Getting configuration for database: ldapdb2.
Got configuration for database: ldapdb2.
Updating configuration for database: ldapdb2.
Updated configuration for database: ldapdb2.
Completed configuration of the database.

IBM SecureWay Directory Configuration complete.

Starting slapd server. This may take a few minutes...
The IBM SecureWay Directory V3.2 service is starting.....
The IBM SecureWay Directory V3.2 service was started successfully.

Adding suffix o=ibm,c=gb ...
Adding suffix secAuthority=Default ...

Starting slapd server. This may take a few minutes...
The IBM SecureWay Directory V3.2 service is stopping...
The IBM SecureWay Directory V3.2 service was stopped successfully.

The IBM SecureWay Directory V3.2 service is starting..
The IBM SecureWay Directory V3.2 service was started successfully.

Adding organization o=ibm,c=gb...
adding new entry o=ibm,c=gb

Starting slapd server. This may take a few minutes...
The IBM SecureWay Directory V3.2 service is stopping...
The IBM SecureWay Directory V3.2 service was stopped successfully.
```

```

The IBM SecureWay Directory V3.2 service is starting...
The IBM SecureWay Directory V3.2 service was started successfully.

IBM SecureWay Directory Server
Installation and Configuration

-----

Product                               Status
IBM DB2 ..... Configured [6]
IBM HTTPD Server ..... Configured [1.3.12]
IBM Global Security Toolkit 4 ..... Configured [4.0.3.168]
IBM SecureWay Directory Client ..... Configured [3.2]
IBM SecureWay Directory Server ..... Configured [3.2]

ezinstall completed successfully.

Press ENTER to continue...
    
```

r. When the screen above is displayed it means that the IBM SecureWay Directory has been successfully installed and configured. In addition, IBM HTTP Server has been installed and configured for access to the LDAP Web console. Press 'ENTER' to exit ezinstall.

## 4.2 Easy Install of Policy Director Management Server (PDMgr)

Use the **ezinstall\_pdmgr** batch file to install the PDRTE and PDMgr components. This sets up a workstation with the following packages; GSKit, IBM SecureWay Directory client v3.2.1, PDRTE and PDMgr. We performed the steps documented here on the same machine as the previous install of the SecureWay Directory.

- a. Insert the Tivoli SecureWay Policy Director Base for Windows version 3.8 CD
- a. Use Windows Explorer to open the drive where **the Policy Director Base for Windows version 3.8** CD image is located. In the root directory of this drive launch the **ezinstall\_pdmgr.bat** file by double-clicking on it.
- b. ezinstall starts in a command window:

```

A response file was created for this process previously.
Do you want to use C:\TEMP\EZINSTALLL.RSP as the response file? [Y | N]:
    
```

c. ezinstall finds the response file that it generated when installing the IBM SecureWay Directory. This file contains information that can be reused to save your typing. Enter 'y' to use this file. The Policy Director Runtime Configuration Options are displayed

```

Tivoli SecureWay Policy Director Runtime Configuration Options
-----
Option                               Value
1. Configure Using This Registry Type ..... ldap
2. LDAP Server Hostname .....
3. LDAP Server Port ..... 389
4. Suffix .....
5. Enable SSL with LDAP Server .....
6. LDAP SSL Keyfile .....
7. LDAP SSL Keyfile DN .....
8. LDAP SSL Key File Password .....
9. LDAP Server SSL Port ..... 636
    
```

```
10. Installation Directory ..... C:\Program Files\Tivoli\Policy Director

Enter the LDAP Server Hostname:
```

d. Enter the LDAP Server Hostname. Since LDAP is installed locally this should be the DNS name of the local host (secure2.pisc.uk.ibm.com in our case).

```
Tivoli SecureWay Policy Director Runtime Configuration Options
-----
Option                                     Value
1. Configure Using This Registry Type ..... ldap
2. LDAP Server Hostname ..... secure2.pisc.uk.ibm.com
3. LDAP Server Port ..... 389
4. Suffix .....
5. Enable SSL with LDAP Server .....
6. LDAP SSL Keyfile .....
7. LDAP SSL Keyfile DN .....
8. LDAP SSL Key File Password .....
9. LDAP Server SSL Port ..... 636
10. Installation Directory ..... C:\Program Files\Tivoli\Policy Director

Enter the Suffix:
```

e. Enter the suffix where you want the GSO database to be created. To make life easy for yourself give the same suffix here as you did when configuring LDAP (so we used o=ibm,c=gb). If you wanted to use something else you would have to make sure that the object already existed in LDAP.

```
Tivoli SecureWay Policy Director Runtime Configuration Options
-----
Option                                     Value
1. Configure Using This Registry Type ..... ldap
2. LDAP Server Hostname ..... secure2.pisc.uk.ibm.com
3. LDAP Server Port ..... 389
4. Suffix ..... o=ibm,c=gb
5. Enable SSL with LDAP Server .....
6. LDAP SSL Keyfile .....
7. LDAP SSL Keyfile DN .....
8. LDAP SSL Key File Password .....
9. LDAP Server SSL Port ..... 636
10. Installation Directory ..... C:\Program Files\Tivoli\Policy Director

Enable SSL with LDAP Server? [Y|N]:
```

f. At this point you must decide if you will use SSL for communication with the LDAP Server. For this basic install we'll keep things simple by NOT using SSL. The Policy Director Management Server Configuration Options screen is re-displayed.

```
Tivoli SecureWay Policy Director Managment Server Configuration Options
-----
Option                                     Value
1. LDAP Administrator ID (DN) ..... cn=root
2. LDAP Administrator Password .....
3. Security Master Password .....
4. SSL Server Port ..... 7135
5. PDMGR SSL Certificate Lifetime ..... 365
6. Enable Download of Certificates .....
```

Enter the LDAP Administrator Password:

g. Enter the LDAP Administrator password. This is the password that you set for `cn=root` during LDAP configuration (`Secure99` in our case).

```
Tivoli SecureWay Policy Director Managment Server Configuration Options
-----
Option                                     Value
1. LDAP Administrator ID (DN) ..... cn=root
2. LDAP Administrator Password ..... *****
3. Security Master Password .....
4. SSL Server Port ..... 7135
5. PDMGR SSL Certificate Lifetime ..... 365
6. Enable Download of Certificates .....

Enter the Security Master Password: *****
Re-enter the password for confirmation: *****
```

h. Enter the password that will be used for the Policy Director master user, `sec_master`. Re-enter for confirmation (we used `Secure99`).

```
Tivoli SecureWay Policy Director Managment Server Configuration Options
-----
Option                                     Value
1. LDAP Administrator ID (DN) ..... cn=root
2. LDAP Administrator Password ..... *****
3. Security Master Password ..... *****
4. SSL Server Port ..... 7135
5. PDMGR SSL Certificate Lifetime ..... 365
6. Enable Download of Certificates .....

Allow other PD Client machines to download the certificate file? [ Y | N ]: y
```

i. You must now decide if other Policy Director machines will be able to download the Policy Director internal CA certificate from the management server. This saves a manual step when configuring remote Policy Director machines but removes the security of having a manual CA Certificate transfer. We choose ‘y’ for this install to keep things simple.

j. The installation and configuration begins. This takes a few minutes – but don’t go away because you need to be around to re-boot the machine.

```
Tivoli SecureWay Policy Director Management Server
Installation and Configuration
-----
Product                                     Status
IBM Global Security Toolkit 4 ..... Configured [4.0.3.168]
IBM SecureWay Directory Client ..... Configured [3.2]
Tivoli SecureWay Policy Director Runtime..... Not Installed
Tivoli SecureWay PD Management Server ..... Not Installed

Installing Tivoli SecureWay Policy Director Runtime.
```

k. IBM GSKIT and IBM SecureWay Directory client are already installed (because the LDAP Server is on the local machine, i.e all components are on the same machine here) so ezinstall starts with the installation of PD Runtime. If LDAP were installed on a different machine the

ezinstall would have installed IBM GSKIT and the LDAP Client at this point.

```
Tivoli SecureWay Policy Director Management Server
Installation and Configuration

-----

Product                                Status
IBM Global Security Toolkit 4 ..... Configured [4.0.3.168]
IBM SecureWay Directory Client ..... Configured [3.2]
Tivoli SecureWay Policy Director Runtime..... Installed [3.8]
Tivoli SecureWay PD Management Server ..... Not Installed

Installing Tivoli SecureWay Policy Director Management Server.

To complete the installation/configuration, the system must be restarted
Press ENTER to continue...
```

- I. When the message shown above is displayed press **ENTER** to re-boot the machine. Once the machine has finished re-booting sign in as **cfguser**. The ezinstall will automatically carry on where it left off with the configuration of Policy Director Runtime. You should see the installation progress as shown below:

```
Tivoli SecureWay Policy Director Management Server
Installation and Configuration

-----

Product                                Status
IBM Global Security Toolkit 4 ..... Configured [4.0.3.168]
IBM SecureWay Directory Client ..... Configured [3.2]
Tivoli SecureWay Policy Director Runtime..... Installed [3.8]
Tivoli SecureWay PD Management Server ..... Installed [3.8]

Configuring Tivoli SecureWay Policy Director Runtime...

The IBM SecureWay Directory V3.2 service is stopping..
The IBM SecureWay Directory V3.2 service was stopped successfully.

The IBM SecureWay Directory V3.2 service is starting...
The IBM SecureWay Directory V3.2 service was started successfully.

Tivoli SecureWay Policy Director Management Server
Installation and Configuration

-----

Product                                Status
IBM Global Security Toolkit 4 ..... Configured [4.0.3.168]
IBM SecureWay Directory Client ..... Configured [3.2]
Tivoli SecureWay Policy Director Runtime..... Configured [3.8]
Tivoli SecureWay PD Management Server ..... Installed [3.8]

Configuring Tivoli SecureWay Policy Director Management Server...

Tivoli SecureWay Policy Director Management Server
Installation and Configuration

-----

Product                                Status
IBM Global Security Toolkit 4 ..... Configured [4.0.3.168]
IBM SecureWay Directory Client ..... Configured [3.2]
Tivoli SecureWay Policy Director Runtime..... Configured [3.8]
Tivoli SecureWay PD Management Server ..... Configured [3.8]
```

```

ezinstall completed successfully.

Press ENTER to continue...
    
```

m. When the screen above is displayed it means that the Policy Director Management Server has been successfully installed and configured. Policy Director Runtime is also installed which means that you can use PDADMIN for command-line administration. Press **'ENTER'** to exit ezinstall.

### 4.3 Easy Install of Policy Director WebSEAL (PDWeb)

Use the **ezinstall\_pdweb** batch file to install WebSEAL. This sets up a workstation with the following packages; GSKit, IBM SecureWay Directory client v3.2.1, PDRTE and WebSEAL. Again we installed this on the same machine as the directory and PD Manager.

- a. Insert the Tivoli SecureWay Policy Director WebSEAL version 3.8 CD
- b. Use Windows Explorer to open the drive where the **Policy Director WebSEAL** CD image is located. In the root directory of this drive launch the **ezinstall\_pdweb.bat** file by double-clicking on it, ezinstall starts in a command window:

```

A response file was created for this process previously.
Do you want to use C:\TEMP\EZINSTALL.RSP as the response file? [Y | N]:
Y
    
```

c. ezinstall finds the response file that it previously generated. This file contains information that can be reused to save your typing. Enter y to use this file. The WebSEAL configuration options are displayed

```

Policy Director WebSEAL Server (PDWEB) Options
-----
Option                                     Value
1. Security Master Password ..... *****

Enter the Security Master Password: *****
    
```

d. Enter the Password you configured for **sec\_master** during the PD Management Server installation (we used **secure99**). The installation and configuration begins, this only take a few seconds.

```

Tivoli Policy Director WebSEAL Server (PDWEB)
Installation and Configuration
-----

Product                                     Status
IBM Global Security Toolkit 4 ..... Configured [4.0.3.168]
IBM SecureWay Directory Client ..... Configured [3.2]
Tivoli SecureWay Policy Director Runtime..... Configured [3.8]
Tivoli SecureWay WebSEAL Server ..... Not Installed

Installing Policy Director WebSEAL Server...
    
```

```
Tivoli Policy Director WebSEAL Server (PDWEB)
Installation and Configuration

-----

Product                               Status
IBM Global Security Toolkit 4 ..... Configured [4.0.3.168]
IBM SecureWay Directory Client ..... Configured [3.2]
Tivoli SecureWay Policy Director Runtime..... Configured [3.8]
Tivoli SecureWay WebSEAL Server ..... Configured [3.8]

ezinstall completed successfully.

Press ENTER to continue...
```

e. When the screen above is displayed it means that WebSEAL has been successfully installed and configured. Press '**ENTER**' to exit ezinstall.

The WebSEAL Server is now running on the machine and should respond to HTTP and HTTPS requests. It has been configured to use the default HTTP and HTTPS ports (80 and 443 respectively). See the later section on validating your PD installation.



## 5. Easy Install process to Set up Policy Director components on a remote machine

This section describes using the scripts to install the WebSEAL and then the WPM and their prerequisites on separate systems.

### 5.1 Easy Install of Policy Director WebSEAL (PDWeb)

Use the **ezinstall\_pdweb** batch file to install WebSEAL. This sets up a workstation with the following packages; GSKit, IBM SecureWay Directory client v3.2.1, PDRTE and WebSEAL.

- a. Insert the Tivoli SecureWay Policy Director WebSEAL Version 3.8 CD.
- b. Using 'My Computer' or 'Windows Explorer' open the root directory of the CD and launch the **ezinstall\_pdweb.bat** file by double-clicking on it. ezinstall starts in a command window:

```
Tivoli Policy Director WebSEAL Server (PDWEB)
Installation and Configuration

-----

Product                               Status
IBM Global Security Toolkit 4 ..... Not Installed
IBM SecureWay Directory Client ..... Not Installed
Tivoli SecureWay Policy Director Runtime..... Not Installed
Tivoli SecureWay WebSEAL Server ..... Not Installed

Press ENTER to continue...
```

- c. This shows the current status of the components required for WebSEAL. Press **ENTER**. The IBM GSKIT Configuration Options are displayed.

```
IBM Global Security Toolkit
-----
Option                               Value
1. Installation Directory ..... C:\Program Files\IBM\GSK

Enter the number of the option to modify or Y to continue: y
```

- d. Enter **'y'** to accept the default installation directory for IBM GSKIT. Then the LDAP Client Configuration Options are displayed.

```
IBM SecureWay Directory Client
-----
Option                               Value
1. Installation Directory ..... C:\Program Files\IBM\LDAP

Enter the number of the option to modify or Y to continue: y
```

- e. Enter **y** to accept the default installation directory for IBM LDAP Client. The Policy Director Runtime Configuration Options are displayed

```
Tivoli SecureWay Policy Director Runtime Configuration Options
-----
Option                                     Value
1. Configure Using This Registry Type ..... ldap
2. LDAP Server Hostname .....
3. LDAP Server Port ..... 389
4. Suffix .....
5. Enable SSL with LDAP Server .....
6. LDAP SSL Keyfile .....
7. LDAP SSL Keyfile DN .....
8. LDAP SSL Key File Password .....
9. LDAP Server SSL Port ..... 636
10. Installation Directory ..... C:\Program Files\Tivoli\Policy Director
11. Policy Director Management Server Hostname
12. SSL Server Port for PD Management Server.. 7135
13. Policy Director CA Certificate Filename ..

Enter the LDAP Server Hostname:
```

f. Enter the LDAP Server Hostname. This is the full DNS name of the machine where you installed the LDAP server (we used `secure2.pisc.uk.ibm.com`).

```
Tivoli SecureWay Policy Director Runtime Configuration Options
-----
Option                                     Value
1. Configure Using This Registry Type ..... ldap
2. LDAP Server Hostname ..... secure2.pisc.uk.ibm.com
3. LDAP Server Port ..... 389
4. Suffix .....
5. Enable SSL with LDAP Server .....
6. LDAP SSL Keyfile .....
7. LDAP SSL Keyfile DN .....
8. LDAP SSL Key File Password .....
9. LDAP Server SSL Port ..... 636
10. Installation Directory ..... C:\Program Files\Tivoli\Policy Director
11. Policy Director Management Server Hostname
12. SSL Server Port for PD Management Server.. 7135
13. Policy Director CA Certificate Filename ..

Enter the Suffix:
```

g. Enter the suffix where you specified the GSO database should be created when setting up the Policy Director Management Server. (We choose to use `o=ibm,c=gb`.)

```
Tivoli SecureWay Policy Director Runtime Configuration Options
-----
Option                                     Value
1. Configure Using This Registry Type ..... ldap
2. LDAP Server Hostname ..... secure2.pisc.uk.ibm.com
3. LDAP Server Port ..... 389
4. Suffix ..... o=ibm,c=gb
5. Enable SSL with LDAP Server .....
6. LDAP SSL Keyfile .....
7. LDAP SSL Keyfile DN .....
8. LDAP SSL Key File Password .....
9. LDAP Server SSL Port ..... 636
10. Installation Directory ..... C:\Program Files\Tivoli\Policy Director
11. Policy Director Management Server Hostname
12. SSL Server Port for PD Management Server.. 7135
13. Policy Director CA Certificate Filename ..

Enable SSL with LDAP Server? [Y|N]:
```

h. At this point you must decide if you will use SSL for communication with the LDAP Server. For

this install we'll keep things simple by NOT using SSL.

```
Tivoli SecureWay Policy Director Runtime Configuration Options
-----
Option                                     Value
1. Configure Using This Registry Type ..... ldap
2. LDAP Server Hostname ..... secure2.pisc.uk.ibm.com
3. LDAP Server Port ..... 389
4. Suffix ..... o=ibm,c=gb
5. Enable SSL with LDAP Server ..... n
6. LDAP SSL Keyfile .....
7. LDAP SSL Keyfile DN .....
8. LDAP SSL Key File Password .....
9. LDAP Server SSL Port ..... 636
10. Installation Directory ..... C:\Program Files\Tivoli\Policy Director
11. Policy Director Management Server Hostname
12. SSL Server Port for PD Management Server.. 7135
13. Policy Director CA Certificate Filename ..

Enter the host name of the Policy Director Management Server:
```

i. PD Runtime needs to where to contact the Management Server. Enter the full DNS name of the machine where the Policy Director Management server is installed (secure2.pisc.uk.ibm.com in our case).

```
Tivoli SecureWay Policy Director Runtime Configuration Options
-----
Option                                     Value
1. Configure Using This Registry Type ..... ldap
2. LDAP Server Hostname ..... secure2.pisc.uk.ibm.com
3. LDAP Server Port ..... 389
4. Suffix ..... o=ibm,c=gb
5. Enable SSL with LDAP Server ..... n
6. LDAP SSL Keyfile .....
7. LDAP SSL Keyfile DN .....
8. LDAP SSL Key File Password .....
9. LDAP Server SSL Port ..... 636
10. Installation Directory ..... C:\Program Files\Tivoli\Policy Director
11. Policy Director Management Server Hostname yourhost.pisc.uk.ibm.com
12. SSL Server Port for PD Management Server.. 7135
13. Policy Director CA Certificate Filename ..

If you have enabled PDMgr to allow the download of the certificate files,
leave this option blank. Otherwise, specify the pdcacert.b64 file
created by the PDMgr configuration.
Enter the path to the Policy Director Certificate File:
```

j. In order for PD Runtime to authenticate the other Policy Director servers it connects to it must have a copy of the PD CA Certificate that was generated by the Management Server when it was configured. This can either be manually copied to the local machine or downloaded as part of the configuration of PD Runtime. When we were configuring the Management Server we said we would allow the PD CA Certificate to be downloaded so we can simply press **ENTER** here to continue.

```
Tivoli SecureWay Policy Director Runtime Configuration Options
-----
Option                                     Value
1. Configure Using This Registry Type ..... ldap
2. LDAP Server Hostname ..... secure2.pisc.uk.ibm.com
3. LDAP Server Port ..... 389
4. Suffix ..... o=ibm,c=gb
5. Enable SSL with LDAP Server ..... n
6. LDAP SSL Keyfile .....
7. LDAP SSL Keyfile DN .....
8. LDAP SSL Key File Password .....
9. LDAP Server SSL Port ..... 636
10. Installation Directory ..... C:\Program Files\Tivoli\Policy Director
11. Policy Director Management Server Hostname yourhost.pisc.uk.ibm.com
12. SSL Server Port for PD Management Server.. 7135
13. Policy Director CA Certificate Filename ..
```

```

7. LDAP SSL Keyfile DN .....
8. LDAP SSL Key File Password .....
9. LDAP Server SSL Port ..... 636
10. Installation Directory ..... C:\Program Files\Tivoli\Policy Director
11. Policy Director Management Server Hostname secure2.pisc.uk.ibm.com
12. SSL Server Port for PD Management Server.. 7135
13. Policy Director CA Certificate Filename ..

Enter the number of the option to modify or Y to continue:

```

k. Enter 'y' to confirm the displayed settings. Next the WebSEAL configuration options begin:

```

Policy Director WebSEAL Server (PDWEB) Options
-----
Option                                     Value
1. Security Master Password ..... *****

Enter the Security Master Password: *****

```

l. Enter the Password you configured for **sec\_master** during the PD Management Server installation (we used **secure99**).

```

Policy Director WebSEAL Server (PDWEB) Options
-----
Option                                     Value
1. Security Master Password ..... *****

Enter the number of the option to modify or Y to continue:

```

m. Enter 'y' to confirm the displayed settings. The installation and configuration proceeds, this takes a little time and requires the machine to be rebooted once.

```

Tivoli Policy Director WebSEAL Server (PDWEB)
Installation and Configuration
-----

Product                                     Status
IBM Global Security Toolkit 4 ..... Not Installed
IBM SecureWay Directory Client ..... Not Installed
Tivoli SecureWay Policy Director Runtime..... Not Installed
Tivoli SecureWay WebSEAL Server ..... Not Installed

Installing IBM Global Security Toolkit.

Tivoli Policy Director WebSEAL Server (PDWEB)
Installation and Configuration
-----

Product                                     Status
IBM Global Security Toolkit 4 ..... Configured [4.0.3.168]
IBM SecureWay Directory Client ..... Configured [3.2]
Tivoli SecureWay Policy Director Runtime..... Installed [3.8]
Tivoli SecureWay WebSEAL Server ..... Not Installed

Installing Policy Director WebSEAL Server.

To complete the installation/configuration, the system must be restarted
Press ENTER to continue...

```

n. When the message shown above is displayed press 'ENTER' to re-boot the machine.

o. Once the machine has finished re-booting sign in as Administrator. The ezinstall will

automatically restart.

```
Policy Director WebSEAL Server (PDWEB) Options
-----
Option                                     Value
1. Security Master Password ..... *****

Enter the Security Master Password: *****
```

p. Enter the password for **sec\_master**. You are asked for this password again as it is required to complete the configuration and is not stored in the response file for security reasons (we used **Secure99**).

q. Now ezinstall can carry on where it left off with the configuration of Policy Director Runtime.

```
Tivoli Policy Director WebSEAL Server (PDWEB)
Installation and Configuration

-----

Product                                     Status
IBM Global Security Toolkit 4 ..... Configured [4.0.3.168]
IBM SecureWay Directory Client ..... Configured [3.2]
Tivoli SecureWay Policy Director Runtime..... Installed [3.8]
Tivoli SecureWay WebSEAL Server ..... Installed [3.8]

Configuring Tivoli SecureWay Policy Director Runtime...

Tivoli Policy Director WebSEAL Server (PDWEB)
Installation and Configuration

-----

Product                                     Status
IBM Global Security Toolkit 4 ..... Configured [4.0.3.168]
IBM SecureWay Directory Client ..... Configured [3.2]
Tivoli SecureWay Policy Director Runtime..... Configured [3.8]
Tivoli SecureWay WebSEAL Server ..... Configured [3.8]

ezinstall completed successfully.

Press ENTER to continue...
```

r. When the screen above is displayed it means that Policy Director WebSEAL has been successfully installed and configured. Press **ENTER** to exit ezinstall.

s. The WebSEAL Server is now running on the machine and should respond to HTTP and HTTPS requests. It has been configured to use the default HTTP and HTTPS ports (80 and 443 respectively).

t. Policy Director Runtime has also been installed on the machine so PDADMIN is available for command-line administration from this machine. Web Portal Manager

## 5.2 Easy Install of Web Portal Manager (PDWPM)

For this section we will install the Web Portal Manager onto another machine (one that does NOT have the Management Server installed). One good reason for doing this is that WebSphere (required by the WPM) has high memory requirements. It is important to have at least 256MB of ram available on a machine just running the WPM and preferably 512MB. There are no technical problems with installing the WPM on the same machine as the Management server provided you have enough memory. The only difference will be that some screens will not be shown as some components will already be installed and configured.

- a. Insert the **Tivoli SecureWay Policy Director Web Portal Manager version 3.8** CD
- b. Using 'My Computer' or 'Windows Explorer' open the root directory of the CD and launch the **ezinstall\_pdwpm.bat** file by double-clicking on it.
- c. ezinstall starts in a command window:

```
Tivoli SecureWay Policy Director Web Portal Manager

Installation and Configuration

-----

Product                                     Status
IBM Global Security Toolkit 4 ..... Not Installed
IBM HTTPD Server ..... Not Installed
IBM SecureWay Directory Client ..... Not Installed
Tivoli SecureWay Policy Director Runtime..... Not Installed
IBM WebSphere Application Server ..... Not Installed
Tivoli SecureWay PD Web Portal Manager ..... Not Installed

Press ENTER to continue...
```

- d. Press '**ENTER**' to continue. You will see the IBM Global Security Toolkit options displayed

```
IBM Global Security Toolkit
-----
Option                                     Value
1. Installation Directory ..... C:\Program Files\IBM\GSK

Enter the number of the option to modify or Y to continue:
```

- e. Type '**y**' to continue.

```
IBM HTTP Server Configuration Options
-----
Option                                     Value
1. Administration ID ..... administrator
2. Administration Password .....
3. HTTP Port ..... 80
4. Installation Directory ..... C:\Program Files\IBM HTTP Server

Enter the Administration Password:
```

- f. Enter the Windows Administrator password (**Secure99** in our case). This is what the HTTP Server will use to start as a service.

```

IBM HTTP Server Configuration Options
-----
Option                                     Value
1. Administration ID ..... administrator
2. Administration Password ..... *****
3. HTTP Port ..... 80
4. Installation Directory ..... C:\Program Files\IBM HTTP Server

Enter the number of the option to modify or Y to continue: 1

Enter the Administrative User ID:  cfguser
    
```

g. Enter '1' to change the Administration id. We changed this to `cfguser` the id we have been using which has administrative rights.

```

IBM HTTP Server Configuration Options
-----
Option                                     Value
1. Administration ID ..... cfguser
2. Administration Password ..... *****
3. HTTP Port ..... 80
4. Installation Directory ..... C:\Program Files\IBM HTTP Server

Enter the number of the option to modify or Y to continue:
    
```

h. Enter 'y' to continue. The IBM SecureWay Directory Client options are displayed

```

IBM SecureWay Directory Client
-----
Option                                     Value
1. Installation Directory ..... C:\Program Files\IBM\LDAP

Enter the number of the option to modify or Y to continue:
    
```

i. Enter 'y' to continue. The PD runtime configuration is displayed.

```

Tivoli SecureWay Policy Director Runtime Configuration Options
-----
Option                                     Value
1. Configure Using This Registry Type ..... ldap
2. LDAP Server Hostname .....
3. LDAP Server Port ..... 389
4. Suffix .....
5. Enable SSL with LDAP Server .....
6. LDAP SSL Keyfile .....
7. LDAP SSL Keyfile DN .....
8. LDAP SSL Key File Password .....
9. LDAP Server SSL Port ..... 636
10. Installation Directory ..... C:\Program Files\Tivoli\Policy Director
11. Policy Director Management Server Hostname
12. SSL Server Port for PD Management Server.. 7135
13. Policy Director CA Certificate Filename ..

Enter the LDAP Server Hostname:
    
```

j. Enter the LDAP Server Hostname. This is the full DNS name of the machine where you installed the LDAP server (`secure2.pisc.uk.ibm.com` in our case).

```

Tivoli SecureWay Policy Director Runtime Configuration Options
-----
Option                                     Value
1. Configure Using This Registry Type ..... ldap
2. LDAP Server Hostname ..... secure2.pisc.uk.ibm.com
3. LDAP Server Port ..... 389
4. Suffix .....
5. Enable SSL with LDAP Server .....
    
```

```

6. LDAP SSL Keyfile .....
7. LDAP SSL Keyfile DN .....
8. LDAP SSL Key File Password .....
9. LDAP Server SSL Port ..... 636
10. Installation Directory ..... C:\Program Files\Tivoli\Policy Director
11. Policy Director Management Server Hostname
12. SSL Server Port for PD Management Server.. 7135
13. Policy Director CA Certificate Filename ..

Enter the Suffix:
    
```

k. Enter the suffix where you specified the GSO database should be created when setting up the Policy Director Management Server. (We choose to use **o=ibm,c=gb**.)

```

Tivoli SecureWay Policy Director Runtime Configuration Options
-----
Option                                     Value
1. Configure Using This Registry Type ..... ldap
2. LDAP Server Hostname ..... secure2.pisc.uk.ibm.com
3. LDAP Server Port ..... 389
4. Suffix ..... o=ibm,c=gb
5. Enable SSL with LDAP Server .....
6. LDAP SSL Keyfile .....
7. LDAP SSL Keyfile DN .....
8. LDAP SSL Key File Password .....
9. LDAP Server SSL Port ..... 636
10. Installation Directory ..... C:\Program Files\Tivoli\Policy Director
11. Policy Director Management Server Hostname
12. SSL Server Port for PD Management Server.. 7135
13. Policy Director CA Certificate Filename ..

Enable SSL with LDAP Server? [Y|N]:
    
```

l. At this point you must decide if you will use SSL for communication with the LDAP Server. For this install we'll keep things simple by NOT using SSL. So enter 'n'.

```

Tivoli SecureWay Policy Director Runtime Configuration Options
-----
Option                                     Value
1. Configure Using This Registry Type ..... ldap
2. LDAP Server Hostname ..... secure2.pisc.uk.ibm.com
3. LDAP Server Port ..... 389
4. Suffix ..... o=ibm,c=gb
5. Enable SSL with LDAP Server ..... n
6. LDAP SSL Keyfile .....
7. LDAP SSL Keyfile DN .....
8. LDAP SSL Key File Password .....
9. LDAP Server SSL Port ..... 636
10. Installation Directory ..... C:\Program Files\Tivoli\Policy Director
11. Policy Director Management Server Hostname
12. SSL Server Port for PD Management Server.. 7135
13. Policy Director CA Certificate Filename ..

Enter the host name of the Policy Director Management Server:
    
```

m. PD Runtime needs to where to contact the Management Server. Enter the full DNS name of the machine where the Policy Director Management server is installed (secure2.pisc.uk.ibm.com in our case).

```

Tivoli SecureWay Policy Director Runtime Configuration Options
-----
Option                                     Value
1. Configure Using This Registry Type ..... ldap
    
```



```

2. LDAP Server Hostname ..... secure2.pisc.uk.ibm.com
3. LDAP Server Port ..... 389
4. Suffix ..... o=ibm,c=gb
5. Enable SSL with LDAP Server ..... n
6. LDAP SSL Keyfile .....
7. LDAP SSL Keyfile DN .....
8. LDAP SSL Key File Password .....
9. LDAP Server SSL Port ..... 636
10. Installation Directory ..... C:\Program Files\Tivoli\Policy Director
11. Policy Director Management Server Hostname yourhost.pisc.uk.ibm.com
12. SSL Server Port for PD Management Server.. 7135
13. Policy Director CA Certificate Filename ..

If you have enabled PDMgr to allow the download of the certificate files,
leave this option blank. Otherwise, specify the pdcacert.b64 file
created by the PDMgr configuration.
Enter the path to the Policy Director Certificate File:

```

n. In order for PD Runtime to authenticate the other Policy Director servers it connects to it must have a copy of the PD CA Certificate that was generated by the Management Server when it was configured. This can either be manually copied to the local machine or downloaded as part of the configuration of PD Runtime. When we were configuring the Management Server we said we would allow the PD CA Certificate to be downloaded so we can simply press **ENTER** here to continue.

```

Tivoli SecureWay Policy Director Runtime Configuration Options
-----
Option                                     Value
1. Configure Using This Registry Type ..... ldap
2. LDAP Server Hostname ..... secure2.pisc.uk.ibm.com
3. LDAP Server Port ..... 389
4. Suffix ..... o=ibm,c=gb
5. Enable SSL with LDAP Server ..... n
6. LDAP SSL Keyfile .....
7. LDAP SSL Keyfile DN .....
8. LDAP SSL Key File Password .....
9. LDAP Server SSL Port ..... 636
10. Installation Directory ..... C:\Program Files\Tivoli\Policy Director
11. Policy Director Management Server Hostname secure2.pisc.uk.ibm.com
12. SSL Server Port for PD Management Server.. 7135
13. Policy Director CA Certificate Filename ..

Enter the number of the option to modify or Y to continue:

```

o. Enter 'y' to continue. The IBM WebSphere Configuration Options are displayed.

```

IBM WebSphere Configuration Options
-----
Option                                     Value
1. Administration ID ..... Administrator
2. Administration Password .....
3. Installation Directory ..... C:\WebSphere\AppServer

Enter the Administration Password: *****

```

p. Enter the Windows Administrator password (which is **Secure99** in our case). This is what WebSphere will use to start as an Windows service. A summary of entries is shown.

```

IBM WebSphere Configuration Options
-----
Option                                     Value
1. Administration ID ..... Administrator
2. Administration Password ..... *****
3. Installation Directory ..... C:\WebSphere\AppServer

```

```

Enter the number of the option to modify or Y to continue: 1
Enter the Administrative User ID:  cfguser
    
```

q. Select '1' and change the administrator to **cfguser**. The configuration is then re-displayed.

```

IBM WebSphere Configuration Options
-----
Option                                     Value
1. Administration ID .....  cfguser
2. Administration Password .....  *****
3. Installation Directory .....  C:\WebSphere\AppServer

Enter the number of the option to modify or Y to continue
    
```

r. Press 'y' to continue and the installation begins. The components are installed and configured one by one, this process takes a few minutes and will require a reboot.

```

Tivoli SecureWay Policy Director Web Portal Manager
Installation and Configuration
-----

Product                                     Status
IBM Global Security Toolkit 4 .....  Configured [4.0.3.168]
IBM HTTPD Server .....  Not Installed
IBM SecureWay Directory Client .....  Configured [3.2]
Tivoli SecureWay Policy Director Runtime.....  Configured [3.8]
IBM WebSphere Application Server .....  Not Installed
Tivoli SecureWay PD Web Portal Manager .....  Not Installed

Installing IBM HTTPD Server.

Tivoli SecureWay Policy Director Web Portal Manager
Installation and Configuration
-----

Product                                     Status
IBM Global Security Toolkit 4 .....  Configured [4.0.3.168]
IBM HTTPD Server .....  Configured [1.3.12]
IBM SecureWay Directory Client .....  Configured [3.2]
Tivoli SecureWay Policy Director Runtime.....  Configured [3.8]
IBM WebSphere Application Server .....  Not Installed
Tivoli SecureWay PD Web Portal Manager .....  Not Installed

Installing IBM WebSphere Application Server.

WASHOME C:\WebSphere\AppServer
JDKHOME C:\WebSphere\AppServer\jdk
      1 file(s) copied.
"Installing the WebSphere Application Server Standard Edition 3.5 PTF 4"
2001/09/18 17:33:59 Extractor version: 01.20
2001/09/18 17:33:59
2001/09/18 17:33:59 Input Jar File      : C:/TEMP/was35_std_ptf_4.jar
...
1/09/18 17:37:10
2001/09/18 17:37:10 Installation completed with no errors.
2001/09/18 17:37:10
2001/09/18 17:37:10 Please view the activity log for details.

Tivoli SecureWay Policy Director Web Portal Manager
Installation and Configuration
-----
    
```

```

Product                               Status
IBM Global Security Toolkit 4 ..... Configured [4.0.3.168]
IBM HTTPD Server ..... Configured [1.3.12]
IBM SecureWay Directory Client ..... Configured [3.2]
Tivoli SecureWay Policy Director Runtime..... Installed [3.8]
IBM WebSphere Application Server ..... Configured [3.5]
Tivoli SecureWay PD Web Portal Manager ..... Not Installed

Installing Tivoli SecureWay Policy Director Web Portal Manager.

To complete the installation/configuration, the system must be restarted
Press ENTER to continue...
    
```

s. Press **'Enter'** to restart the system. The install will then continue once you login. The runtime environment is configured.

```

Tivoli SecureWay Policy Director Web Portal Manager
Installation and Configuration

-----

Product                               Status
IBM Global Security Toolkit 4 ..... Configured [4.0.3.168]
IBM HTTPD Server ..... Configured [1.3.12]
IBM SecureWay Directory Client ..... Configured [3.2]
Tivoli SecureWay Policy Director Runtime..... Configured [3.8]
IBM WebSphere Application Server ..... Configured [3.5]
Tivoli SecureWay PD Web Portal Manager ..... Installed [3.8]

Configuring Tivoli SecureWay Policy Director Web Portal Manager...
Starting configuration for PD Web Portal Manager..
Opening registry to update configuration value.
Setting the configuration value to working.
Update Registry succeeded
Start to run WAS command line
Running the command line: ...

Tivoli SecureWay Policy Director Web Portal Manager
Installation and Configuration

-----

Product                               Status
IBM Global Security Toolkit 4 ..... Configured [4.0.3.168]
IBM HTTPD Server ..... Configured [1.3.12]
IBM SecureWay Directory Client ..... Configured [3.2]
Tivoli SecureWay Policy Director Runtime..... Configured [3.8]
IBM WebSphere Application Server ..... Configured [3.5]
Tivoli SecureWay PD Web Portal Manager ..... Configured [3.8]

ezinstall completed successfully.

Press ENTER to continue...
    
```

t. When you see the message above the Web Portal Manager is installed and configured. If you have installed the WPM on its own machine as suggested you should be able to test the WPM by point your browser at: **https://hostname:port/pdadmin** . (This would be **https://secure2.pisc.uk.ibm.com/pdadmin** in our case.)

u. If you have other PD components like WebSEAL or other web servers on the same machine you may need to change the default port being used by WebSphere and the HTTP server for the WPM. See the following section to move the WPM to different ports.

## 5.3 Changing ports for Web Portal Manager

The WPM runs as a WebSphere application – a set of Java Server Pages. In order to use the WPM on non-standard ports the IBM HTTP Server and WebSphere must be re-configured.

- a. To modifying the HTTP server ports, use Windows Explorer to open C:\Program Files\IBM HTTP Server\conf\httpd.conf
- b. Find the *Port* parameter and change it to show a new HTTP port:

```
# Port: The port the standalone listens to.
Port 80
```

### Becomes

```
# Port: The port the standalone listens to.
Port 8080
```

- c. Next find the **Listen** and **VirtualHost** lines near the end of the file. These were added by the WPM configuration. Change both references to port 443 to 8443:

```
### BEGIN PDWPM CONFIG ENTRY ###
Listen 443
LoadModule ibm_ssl_module modules/IBMModuleSSL128.dll
<VirtualHost :443>
```

### Becomes

```
### BEGIN PDWPM CONFIG ENTRY ###
Listen 8443
LoadModule ibm_ssl_module modules/IBMModuleSSL128.dll
<VirtualHost :8443>
```


- d. Now save the file and the stop and start the IBM HTTP Server service.
- e. At this point you should be able to connect to the IBM HTTP Server on the new ports. You will be able to see the server homepage but not the WPM – in order for that to work WebSphere must be reconfigured with the new ports.
- f. Next modify the aliases in WebSphere configuration. In order to modify aliases that WebSphere is looking for (which include the port number) the WebSphere console must be used. This can be launched from

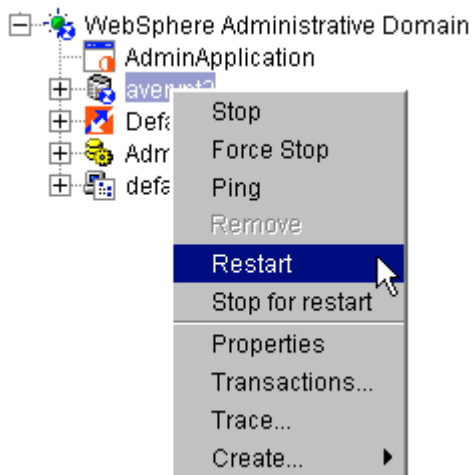
Start->Programs->IBM WebSphere->Application Server V3.5->Administrator's Console

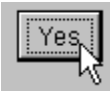


- g. Expand the **WebSphere Administrative Domain** and then click once on **default\_host** to highlight it as shown above. The panel on the Right will display the Host Aliases. These tell WebSphere which Webserver addresses it should accept requests on. In the default configuration this list contains a selection of localhost, 127.0.0.1, IP address, hostname and full DNS Name with either no port specified (which means port 80) or with 443 specified.
- h. Change all the items that have no port specified from xxxxxxx to xxxxxxx:8080 and change all the items that have port 443 specified from xxxxxxx:443 to xxxxxxx:8443 as shown below:



- i. Once they are all changed select the  button at the bottom
- j. On the Console explorer right-click on the line that shows your machine's hostname and select "Restart" from the pop-up menu:



- k. This will show a confirmation. Click on  and the Admin console will close.
- l. WAS is restarted in the background. Once WAS is up again (after a minute or two) you should be able to connect to the WPM on port 8443 using the URL: <https://hostname:8443/pdadmin>

---

## 6. Native installation process

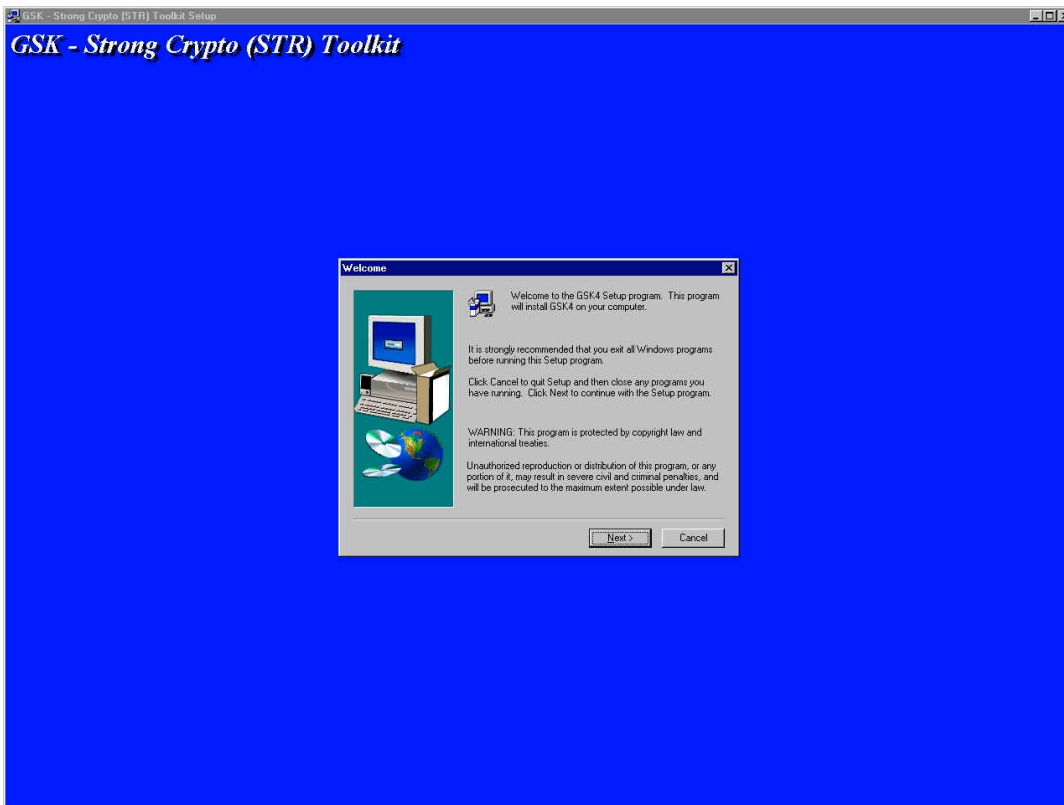
This section describes the techniques for installing Policy Director and its components without the easy install scripts. The approach we have taken here is to try and minimise reboots. So we install all the required components, re-boot and then configure the components as required.

---

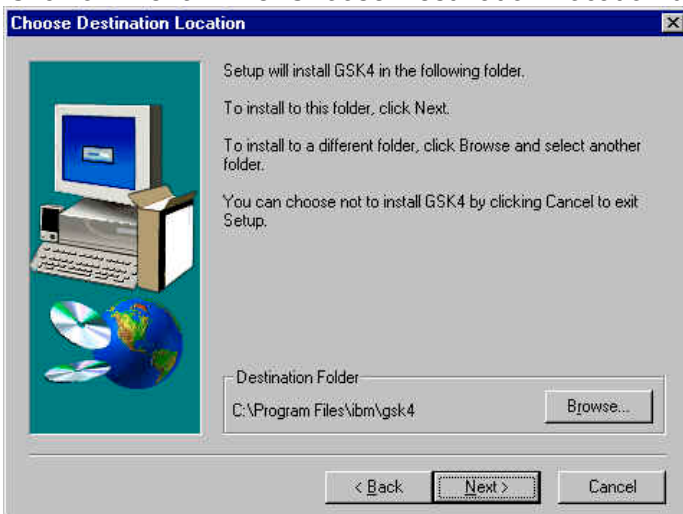
### 6.1 GSKit installation (Windows)

GSKit (Global Security Kit) is IBM's SSL support library. GSKit needs to be installed on any box which also includes WebSEAL, IBM SecureWay Directory, the Policy Director Servers or Web Portal Manager. If you currently have a version of GSKit installed on your system, verify the version is at **4.0.3.168 or above**. To determine the version you currently have installed, issue the **gskver** command from **C:\Program Files\IBM\gsk4\bin** and check the Product Version that is displayed.

- a. Log in as a user with administrator privileges. (We used a user ID of **cfguser**, password **Secure99**.)
- b. Insert the **Tivoli SecureWay Policy Director Base for Windows Version 3.8** CD.
- c. Using 'My Computer' or Windows Explorer find the **lwindows\gskit** directory on the CD, and double click on **setup.exe**. The GSKit welcome screen is displayed:



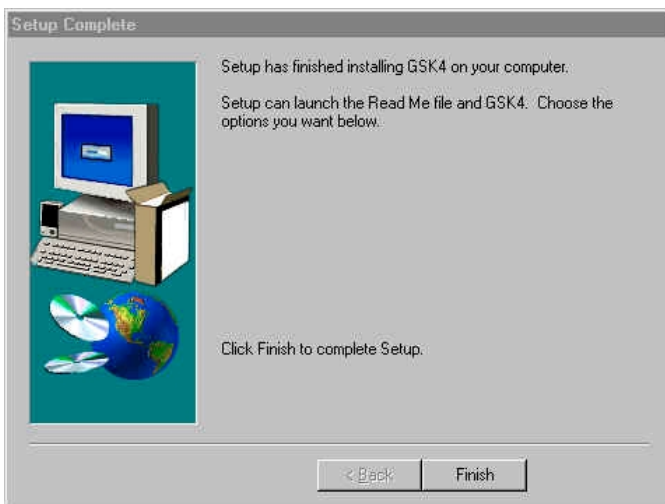
d. Click on 'Next'. The 'Choose Destination Location dialog box appears:



e. Click on 'Next'. A message is displayed indicating that Setup is loading the GSK4 Base Toolkit. Then the 'Setup Complete' dialog box is displayed:







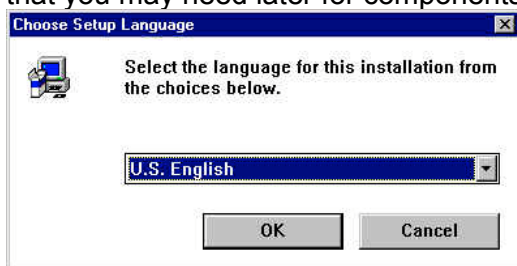
f. Click on '**Finish**'.

## 6.2 LDAP Server installation (Windows)

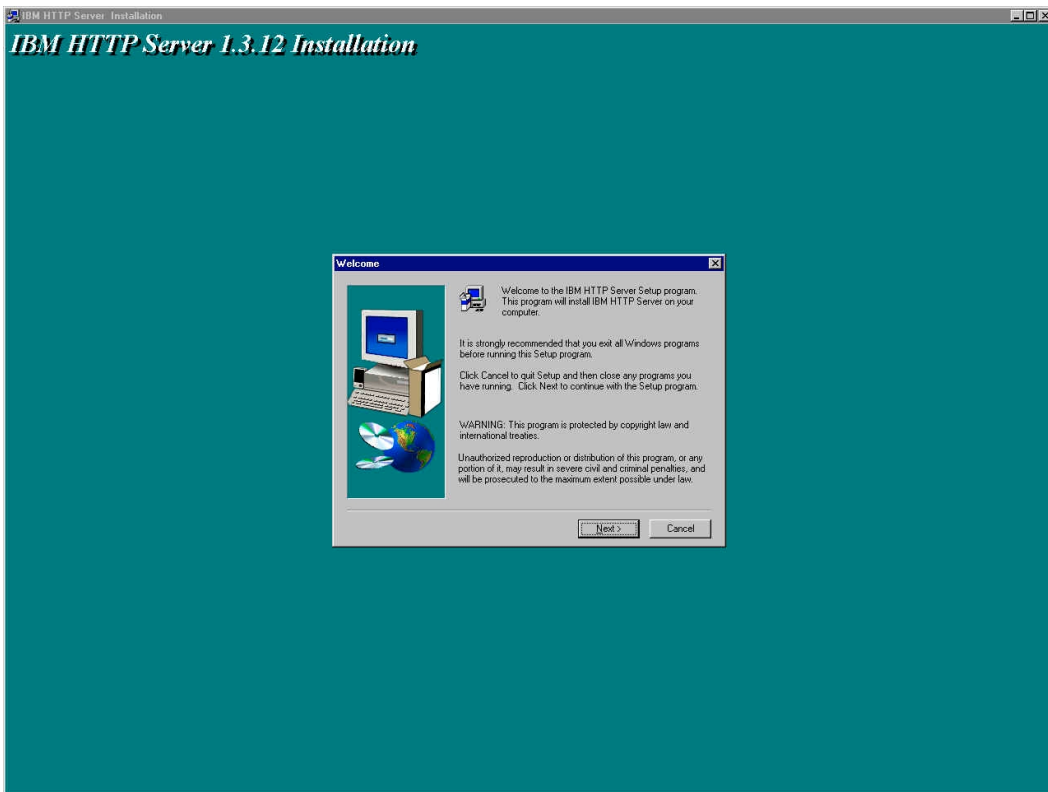
### General notes

- In Policy Director Version 3.6 and before, it was necessary to install DB2 with the appropriate fixpacks and a web server separately. This is no longer the case with PD 3.7 and above - they are installed as part of the IBM SecureWay Directory install.
- Note that installation of LDAP Server does not work on a Windows Backup Domain Controller (BDC). The only way we have found to work around this problem is to step down the Primary Domain Controller (PDC) and promote the BDC to a PDC. It is then possible to install the LDAP Server on the new DC.
- \*\*\* do a pointer to the troubleshooting section in the LDAP help pages \*\*\*

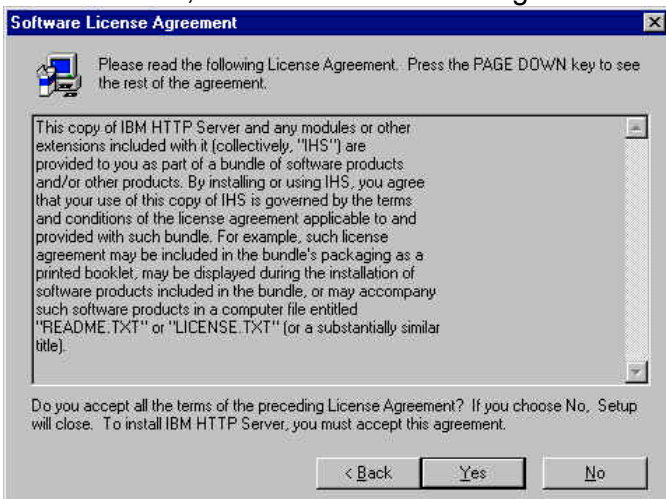
- a. Uninstall any previous versions of the SecureWay Directory or DB2.
- b. **If it exists, delete the \ldapdb2 folder.** (There appears to be a problem with installing the SecureWay Directory where there is already a database/instance present.)
- c. **Ensure that the db2admin and ldapdb2 userids do not exist.** (Use Start -> Programs -> Administrative Tools (Common) -> User Manager for Domains to check and, if necessary, remove them.) (As part of the LDAP install there is a silent install of DB2 – however if the db2admin userid already exists then there appears to be no mechanism for supplying the db2admin password, and a DB2 installation error will result.)
- d. If IBM HTTP Server is not currently installed, ensure that C:\Program Files\IBM HTTP Server\conf\httpd.conf does not exist.
- e. Insert the **Tivoli SecureWay Policy Director Base for Windows Version 3.8** CD.
- f. Using 'My Computer' or Windows Explorer find the **windows\Directory\ldap32\_us\ibmhttp** directory on the CD, and double click on **setup.exe**. The 'Choose Setup Language' dialog box appears. (**Note:** we install the HTTP server this way even though you can do it from the SecureWay Directory install; this is so that you get a complete install with all the SSL libraries that you may need later for components like the WPM.)



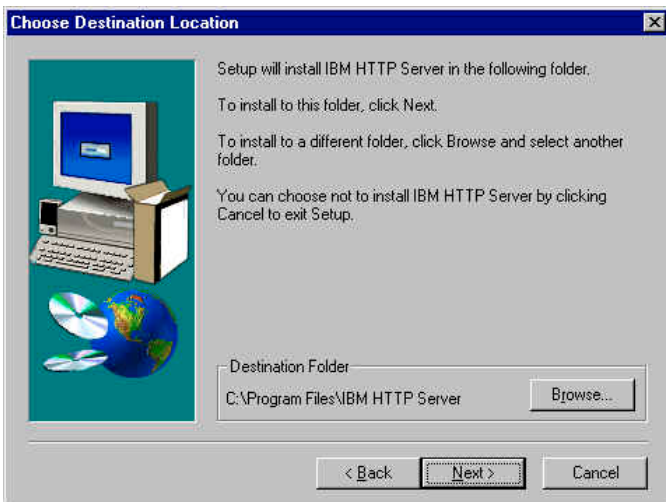
- g. Select a language and click on '**OK**'.
- h. The InstallShield runs and the IBM HTTP Server 1.3.12 Welcome screen is displayed:



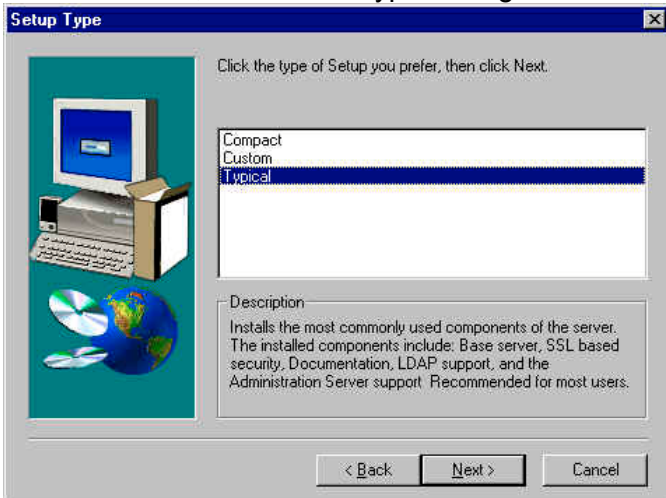
i. Click on **'Next'**; the Software License Agreement screen is displayed:



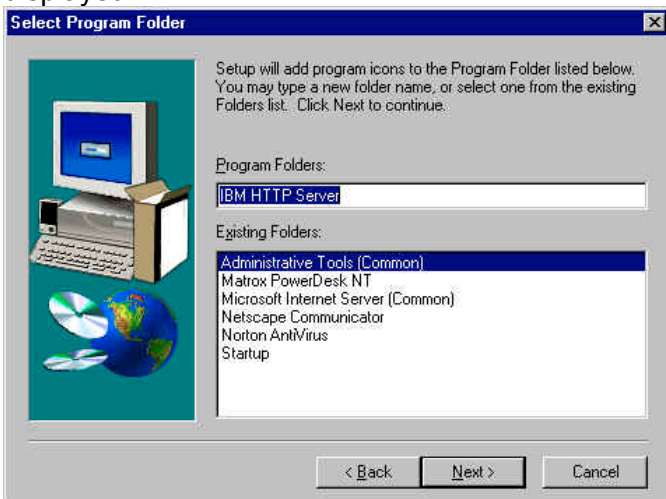
j. Click on **'Yes'**; the Choose Destination Location screen is displayed:



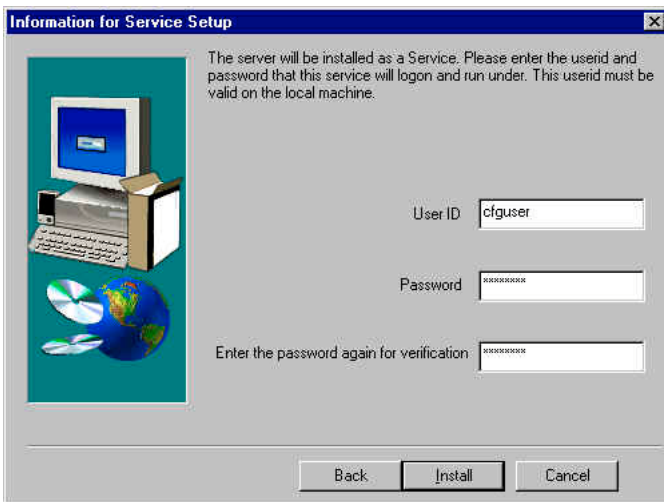
k. Click on 'Next'; the 'Select Type' dialog box is displayed:



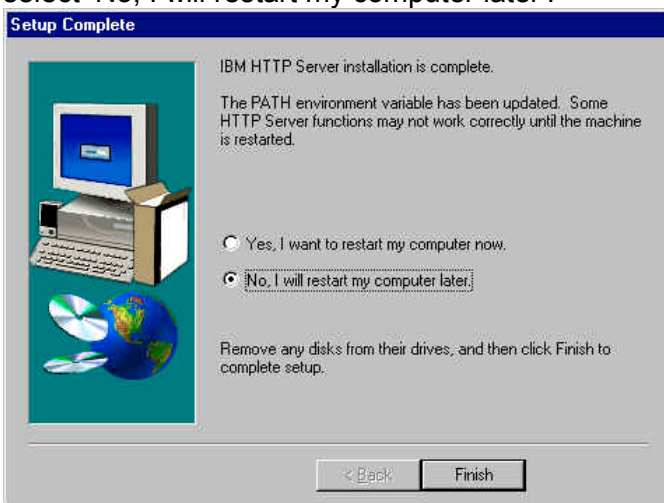
l. Leave 'Typical' selected and click on 'Next'; the 'Select Program Folder' dialog box is displayed:



m. Click on 'Next'; the 'Information for Service Setup' dialog box is displayed; enter the userid and password under which IBM HTTP Server will run. (We used a user ID of `cfguser`, password `secure99`.)



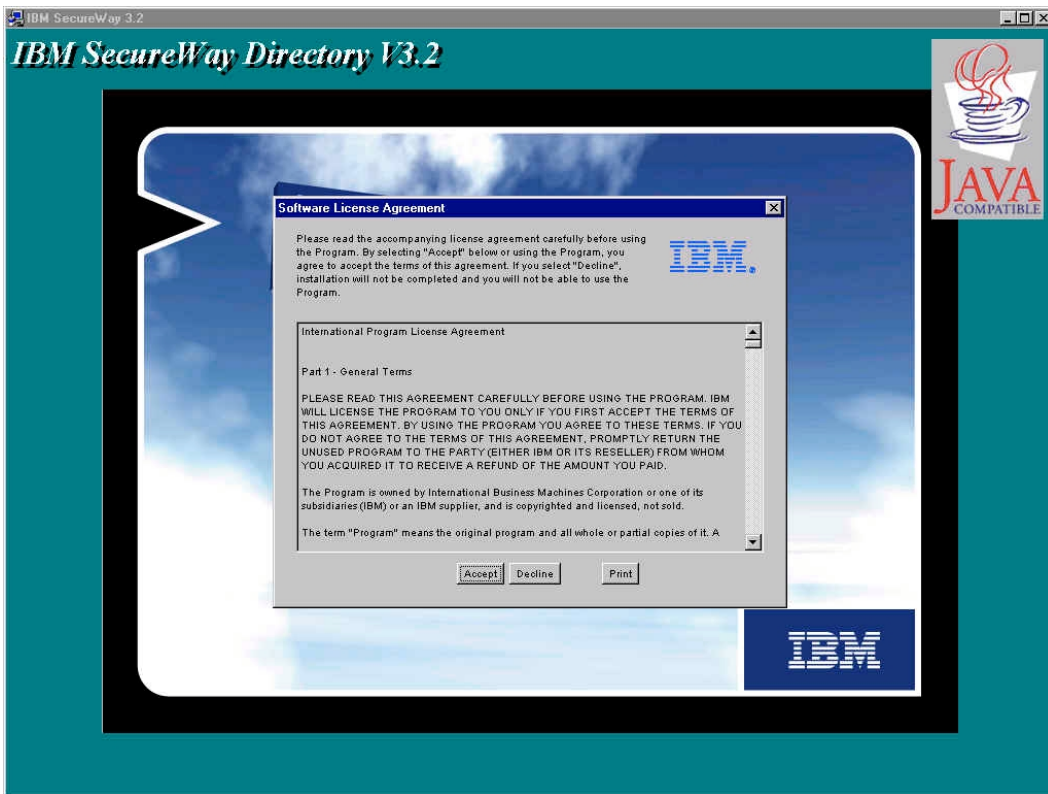
- n. Click on '**Install**'; the files are copied across, and the 'Setup Complete' panel is displayed; select 'No, I will restart my computer later':



- o. Click on '**Finish**'.
- p. Using 'My Computer' or Windows Explorer find the **Windows\Directory\ldap32\_us** directory on the CD, and double click on **setup.exe**. The 'Choose Setup Language' dialog box appears:



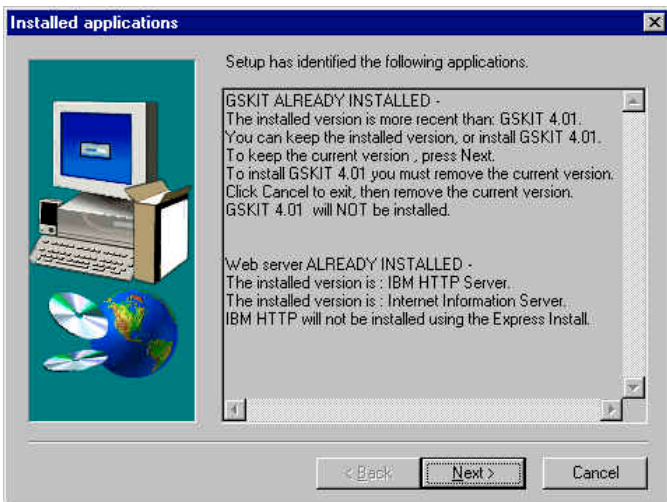
- q. Select a language and click on '**OK**'. The InstallShield runs and the IBM SecureWay Directory V3.2/Software License Agreement is displayed:



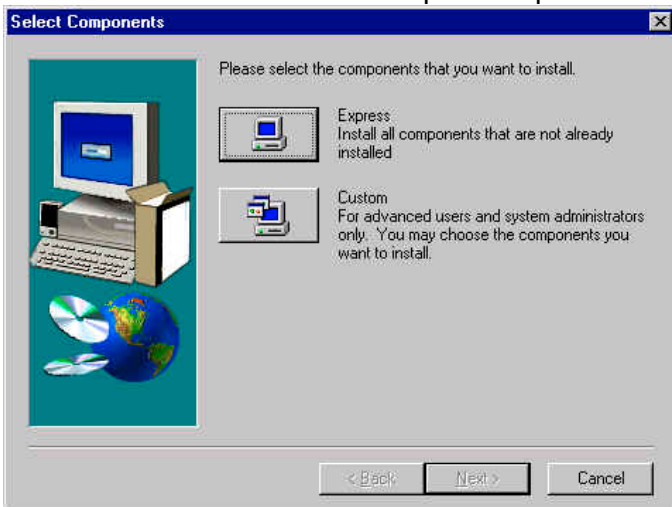
r. Click on '**Accept**'; the Welcome screen is displayed:



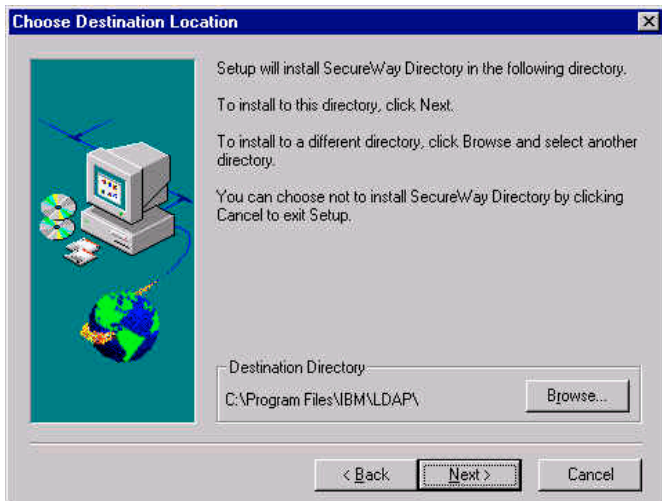
s. Click on '**Next**'. An 'Installed Applications' window will be displayed, warning you that a more recent version of GSKit is installed:



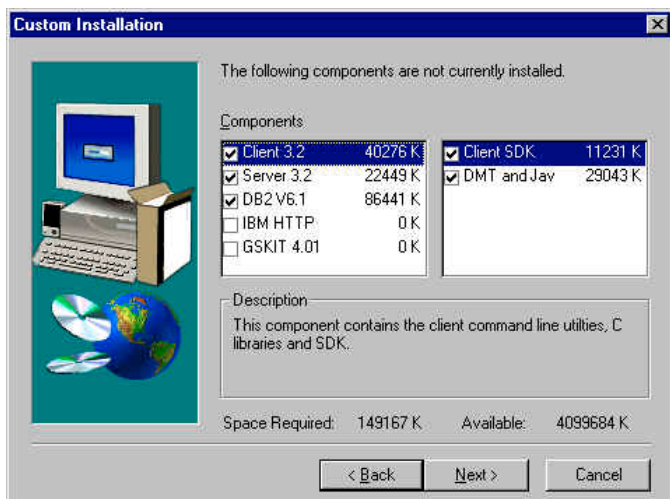
t. Click on '**Next**'. The Select Components panel will be displayed:



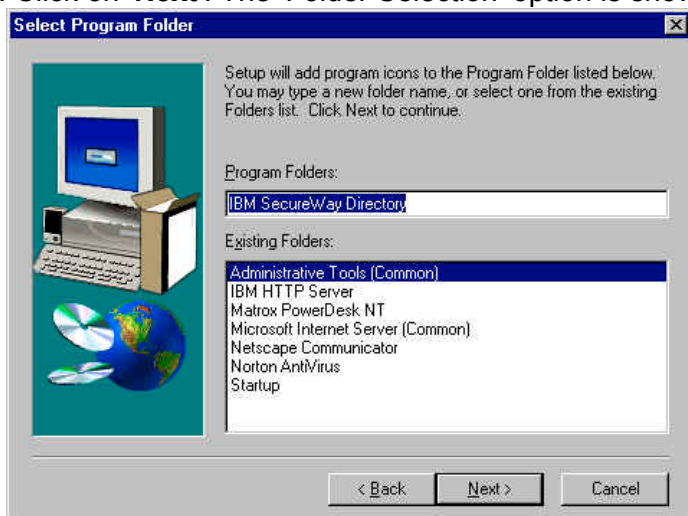
u. Click on '**Custom**'. The 'Choose Destination Location' panel is displayed:



v. Click on '**Next**'. The 'Custom Installation' panel is displayed. Ensure that the IBM HTTP and GSKIT 4.01 options are deselected (as we have already installed them):



w. Click on **'Next'**. The 'Folder Selection' option is shown:



x. Click on **'Next'**. The 'Configure' dialogue box is displayed; deselect all the options as we will perform these configuration steps later:

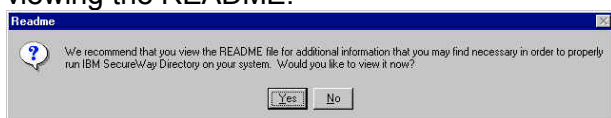


y. Click on **'Next'**. The summary screen is displayed:





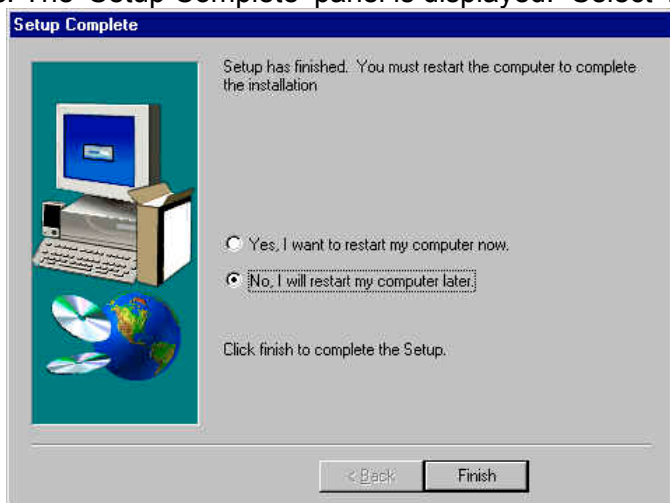
z. Review the settings and click on **'Next'**. The files are copied across, you are given the option of viewing the README:



aa. Select **'Yes'** or **'No'** as you feel appropriate.

bb. (The LDAP installation includes a silent DB2 install. In the event of a failure of the DB2 installation, it is worth referring to the installation log file C:\DB2LOG\db2.log.)

cc. The 'Setup Complete' panel is displayed. Select **'No'**, I will restart my computer later':



dd. Click on **'Finish'**.

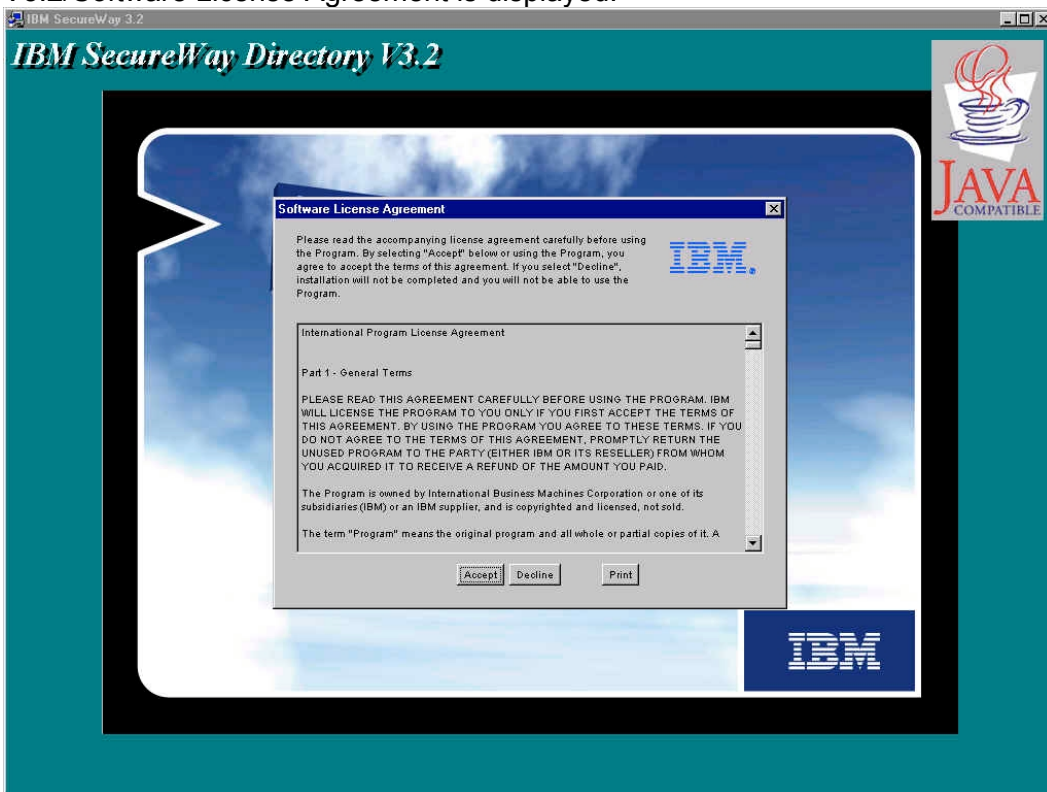
## 6.3 LDAP Client installation (Windows)

This sequence of steps should be followed on a box requiring connectivity to a LDAP Server but not running a LDAP Server. (It is a requisite of the PDRTE)

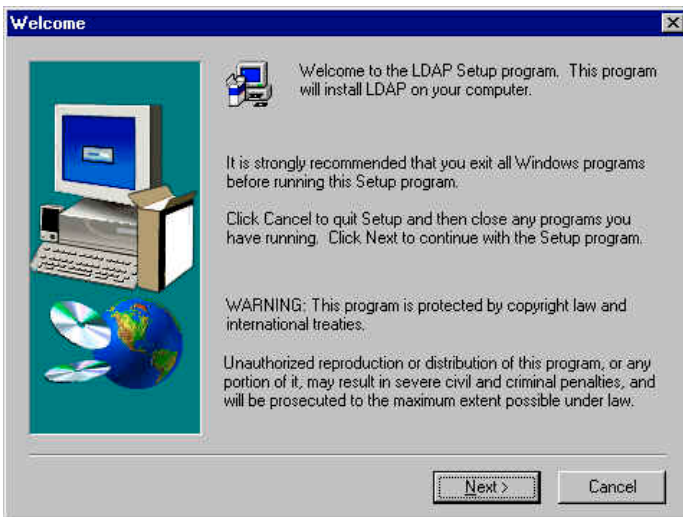
- a. Using 'My Computer' or Windows Explorer find the `\windows\Directory\ldap32_us` directory on the CD, and double click on `setup.exe`. The 'Choose Setup Language' dialog box appears:



- b. Select a language and click on '**OK**'. The InstallShield runs and the IBM SecureWay Directory V3.2/Software License Agreement is displayed:



- c. Click on '**Accept**'; the Welcome screen is displayed:

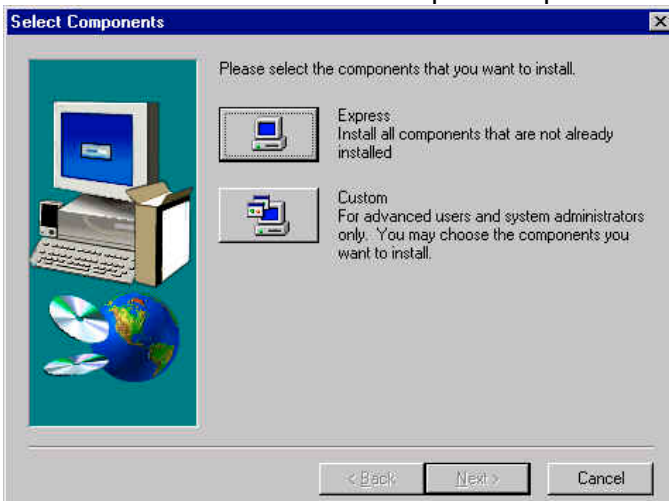


d. Click on **'Next'**. An **'Installed Applications'** window will be displayed, warning you that a more recent version of GSKit is installed:

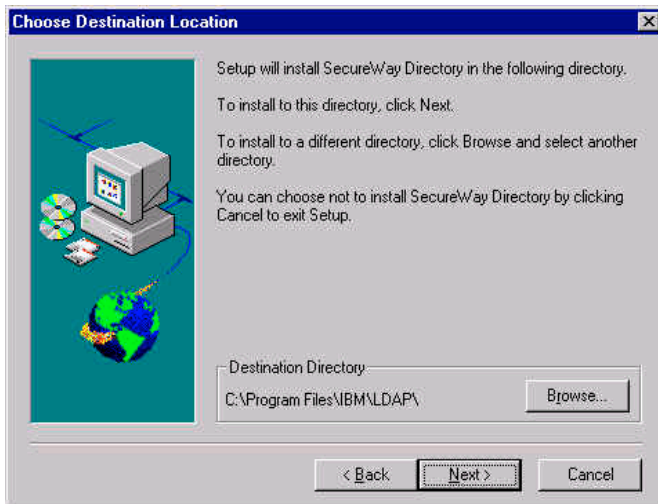


[what you see here will depend on exactly what you already have installed]

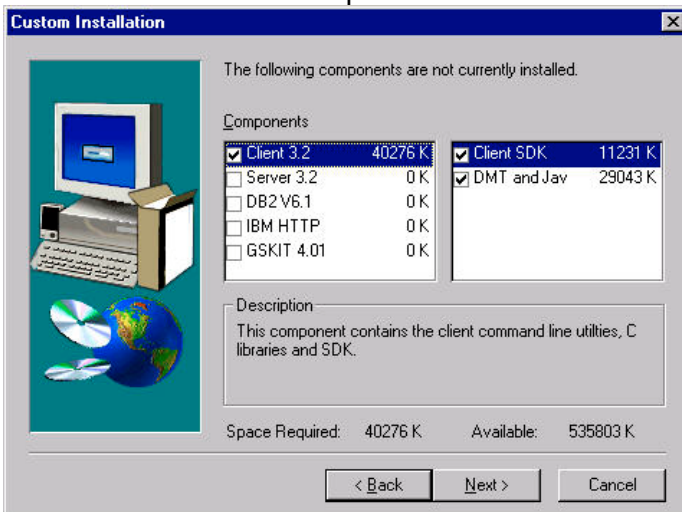
e. Click on **'Next'**. The **Select Components** panel will be displayed:



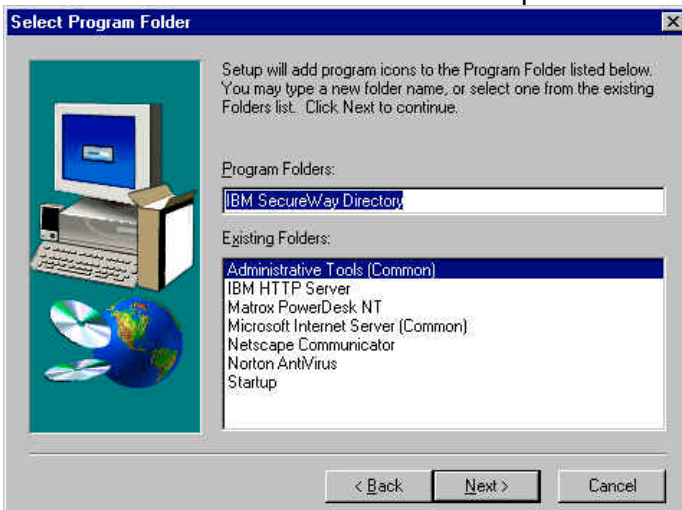
f. Click on **'Custom'**. The **'Choose Destination Location'** panel is displayed:



g. Click on **'Next'**. The **'Custom Installation'** panel is displayed. Select only the Client component, and deselect all other components:



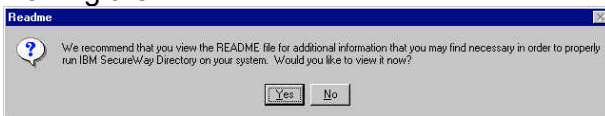
h. Click on **'Next'**. The **'Folder Selection'** option is shown:



i. Click on **'Next'**. The summary screen is displayed:

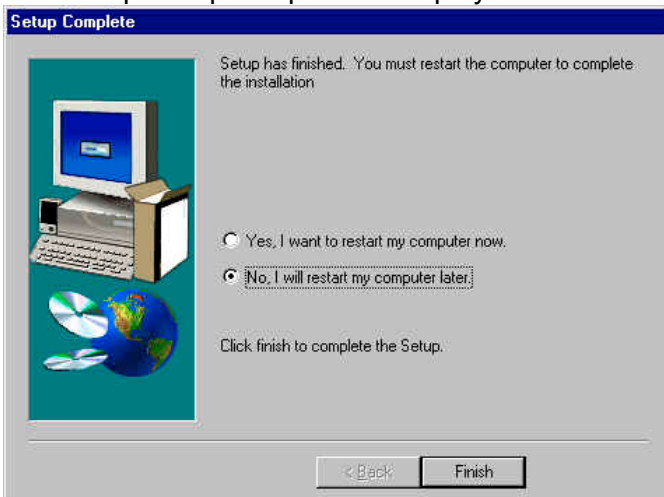


j. Review the settings and click on **'Next'**. The files are copied across, you are given the option of viewing the README:



k. Select 'Yes' or 'No' as you feel appropriate.

l. The 'Setup Complete' panel is displayed. Select 'No, I will restart my computer later':



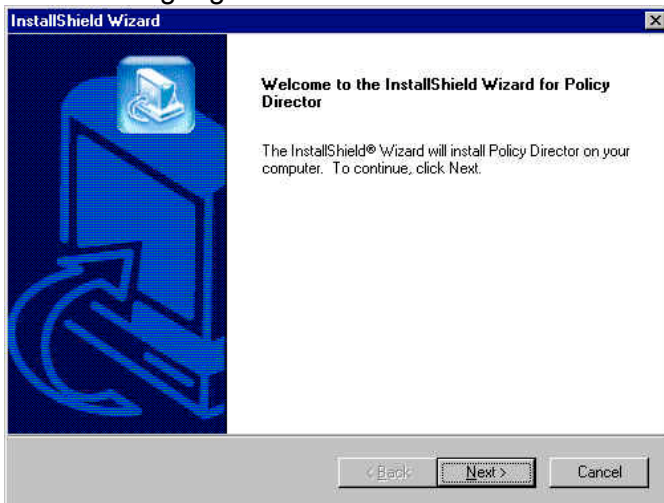
m. Click on **'Finish'**.

## 6.4 Policy Director Servers installation (Windows)

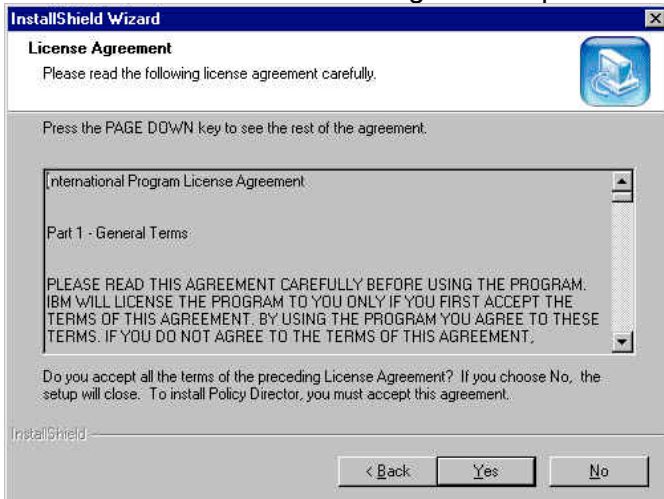
- a. Insert the **Tivoli SecureWay Policy Director Base for Windows Version 3.8** CD.
- b. Using 'My Computer' find the `\\windows\\PolicyDirector\\Disk Images\\Disk1` directory on the CD, and double click on `setup.exe`. The 'Choose Setup Language' dialogue box is displayed:



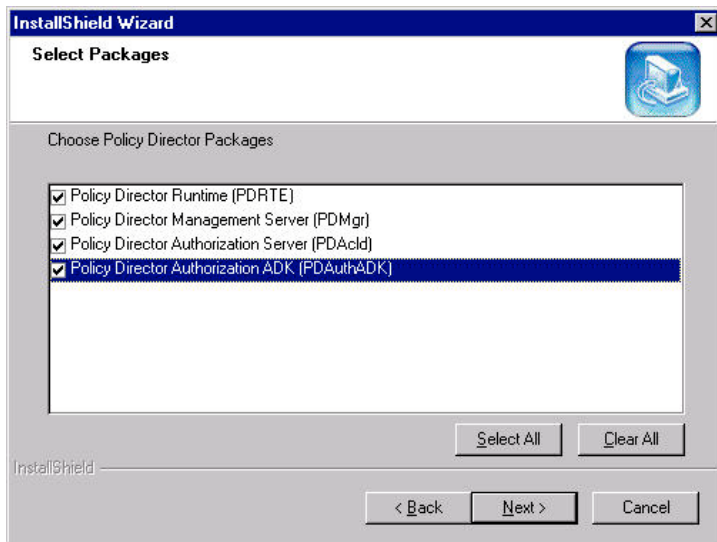
- c. Select a language and click on '**OK**'. The InstallShield Wizard panel will be displayed:



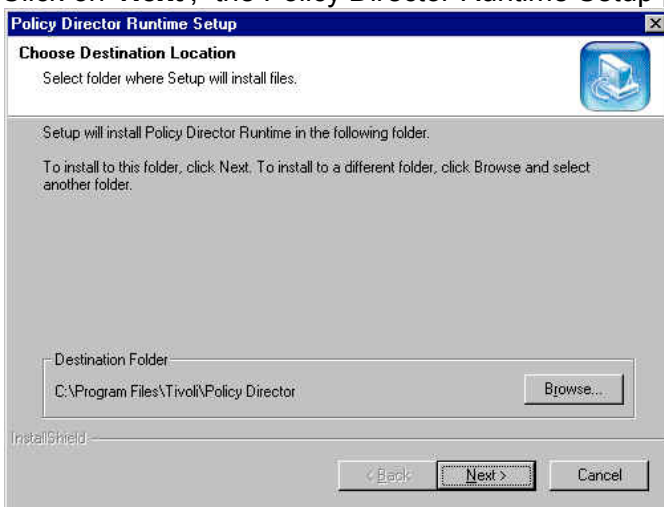
- d. Click on '**Next**'. The License Agreement panel is displayed:



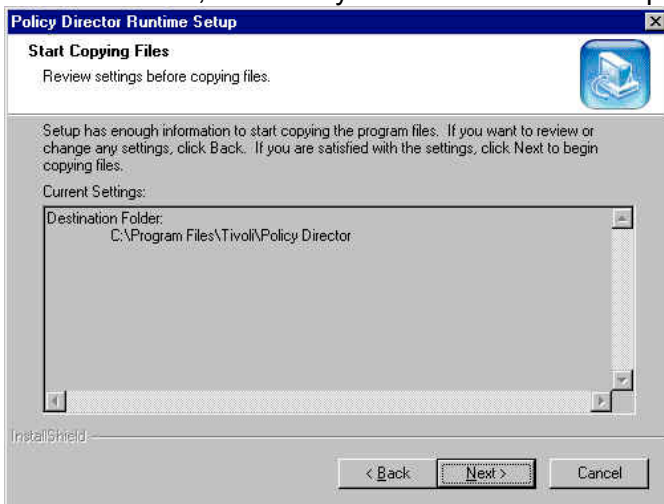
- e. Click on '**Yes**'. The 'Select Packages' panel will be displayed. Select the Policy Director packages you require (at a minimum the PDRTE and PDMgr, we chose all the packages here for our install):



f. Click on '**Next**'; the Policy Director Runtime Setup panel is displayed:



g. Click on '**Next**'; the Policy Director Runtime Setup summary screen is displayed:



h. Review the settings and click on '**Next**'; the files are copied across and the Policy Director Installation Complete panel is displayed. Select '**No, I will restart my computer later**' (unless

you do not plan to go on and install WebSEAL or other PD components on this machine in which case you can select **'Yes, I want to restart my computer now'**):



i. Click on **'OK'**.



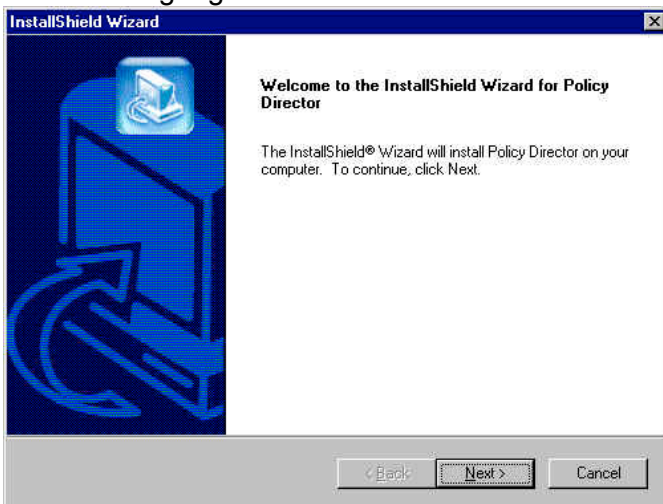
## 6.5 Install Policy Director Runtime Environment (PDRTE) (Windows)

This sequence of steps should be followed on a box requiring any of the PD servers.

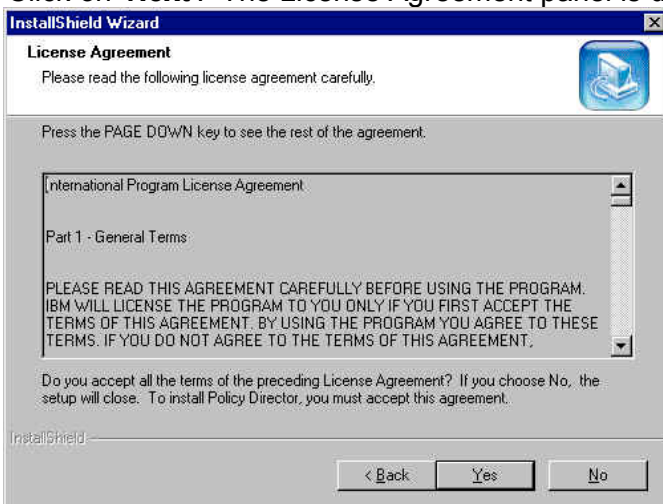
- a. Insert the Tivoli SecureWay Policy Director Base for Windows Version 3.8 CD.
- b. Using 'My Computer' find the \windows\PolicyDirector\Disk Images\Disk1 directory on the CD, and double click on `setup.exe`. The 'Choose Setup Language' dialogue box is displayed:



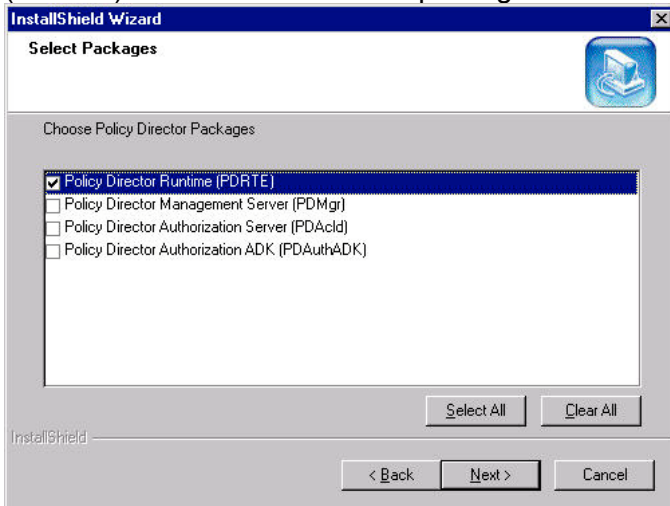
- c. Select a language and click on 'OK'. The InstallShield Wizard panel will be displayed:



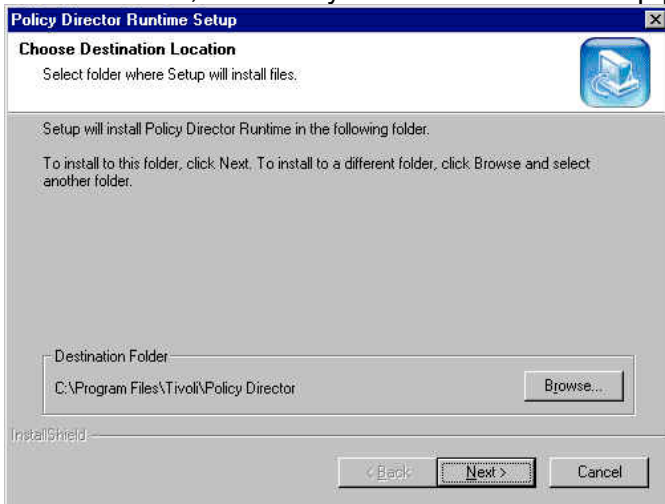
- d. Click on 'Next'. The License Agreement panel is displayed:



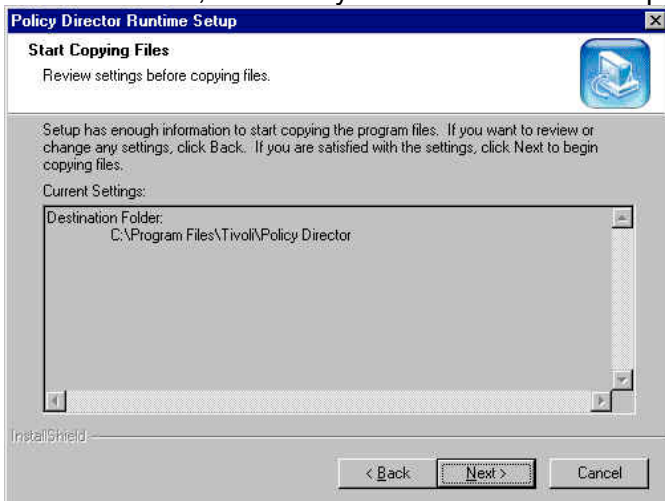
- e. Click on **'Yes'**. The 'Select Packages' panel will be displayed. Select Policy Director Runtime (PDRTE) and deselect all other packages:



- f. Click on **'Next'**; the Policy Director Runtime Setup panel is displayed:



- g. Click on **'Next'**; the Policy Director Runtime Setup summary screen is displayed:



- h. Review the settings and click on **'Next'**; the files are copied across and the Policy Director

Installation Complete panel is displayed. Select 'No, I will restart my computer later':



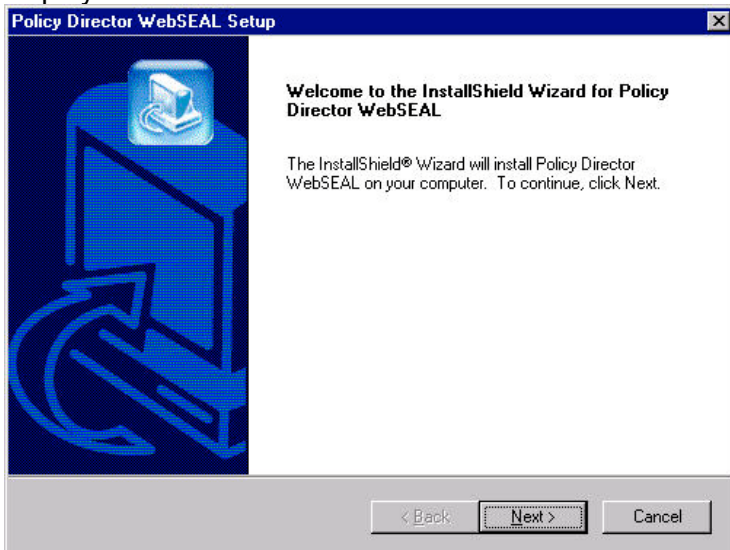
- i. Click on '**OK**'.
- j. If you are not going to install WebSEAL then the computer can be re-booted by issuing Start → Shut Down → Restart.

## 6.6 Install WebSEAL (Windows)

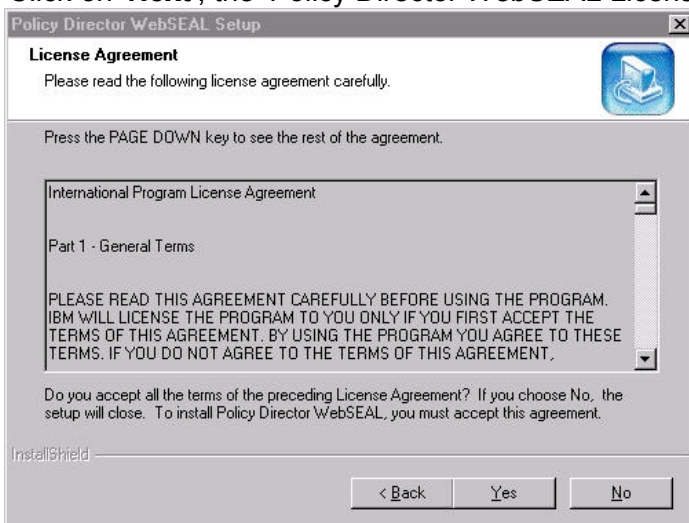
- a. Insert the Tivoli SecureWay Policy Director WebSEAL Version 3.8 CD.
- b. Using Windows Explorer find the **\Windows\PolicyDirector\Disk Images\Disk 1\WebSEAL\Disk Images\Disk1** directory on the CD and double click on **setup.exe**. The 'Choose Setup Language' panel is displayed:



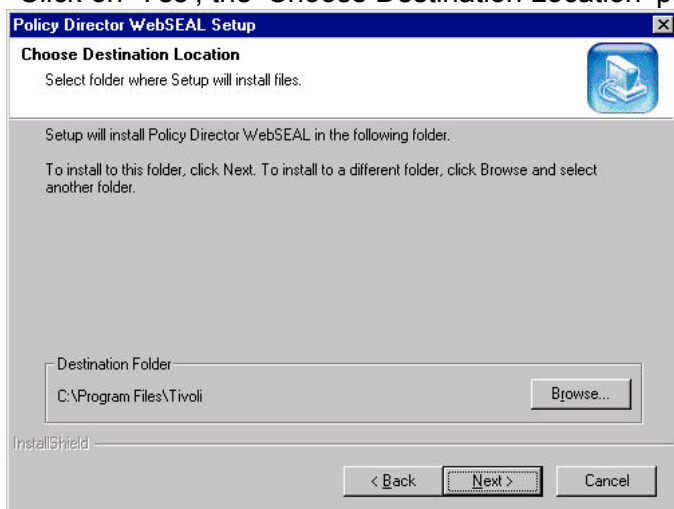
- c. Select a language and click on '**OK**'. The 'Policy Director WebSEAL Setup' panel will be displayed.



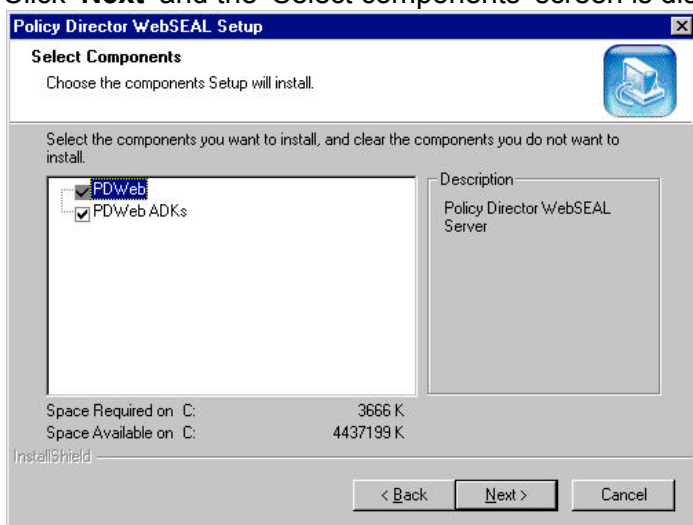
- d. Click on '**Next**', the 'Policy Director WebSEAL License Agreement' is displayed



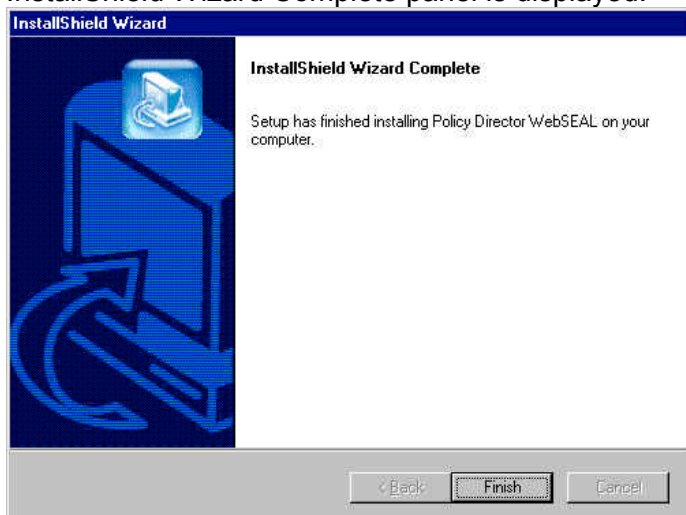
e. Click on 'Yes', the 'Choose Destination Location' panel is displayed.



f. Click 'Next' and the 'Select components' screen is displayed.



g. Select the components you want and click 'Next'. The files are copied across and the InstallShield Wizard Complete panel is displayed:

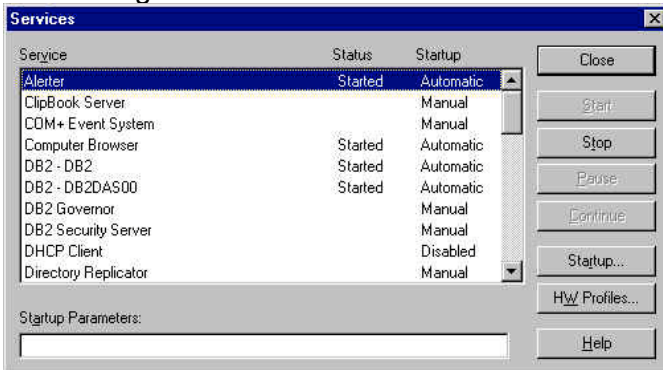


h. Click on 'Finish'.

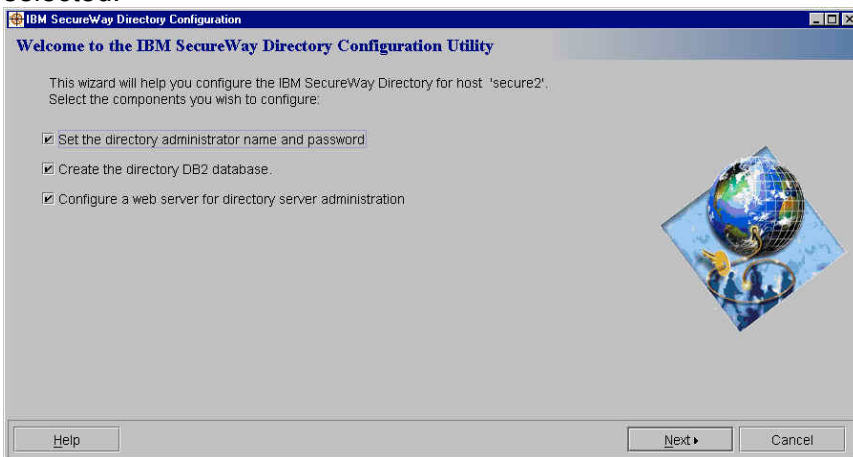
i. At this point the computer can be re-booted by issuing Start -> Shut Down -> 'Restart the computer'.

## 6.7 LDAP Server configuration (Windows)

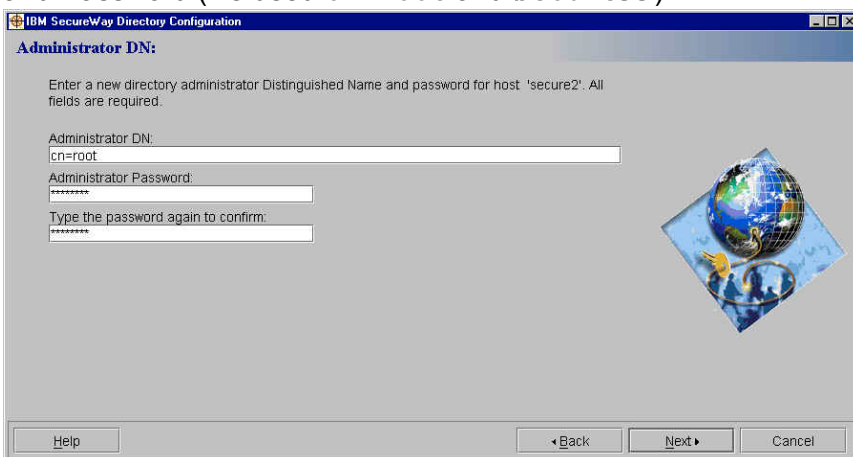
- a. Use Start → Settings → Control Panel → Services (NT) or Start → Administrator Tools → Services (Windows 2000) to ensure that DB2 – DB2, DB2 – DB2DAS00 and IBM HTTP Server are running:



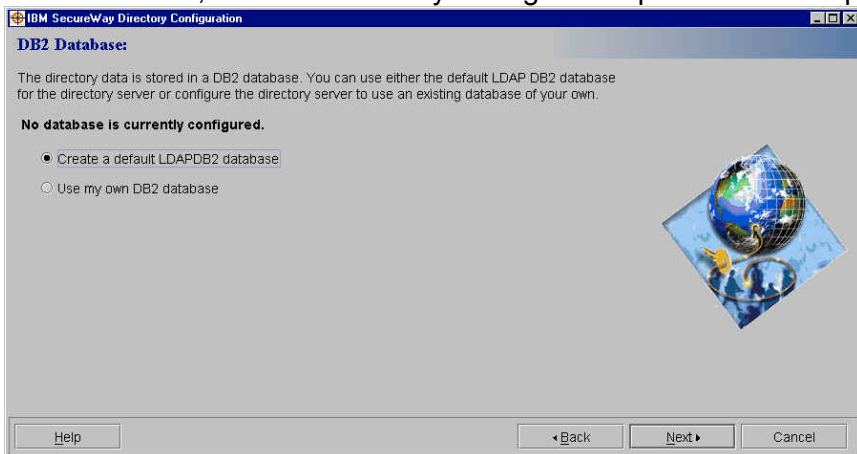
- b. Use Start → Programs → IBM SecureWay Directory → Directory Configuration; the IBM SecureWay Director Configuration Utility will be started. Ensure that all the operations are selected:



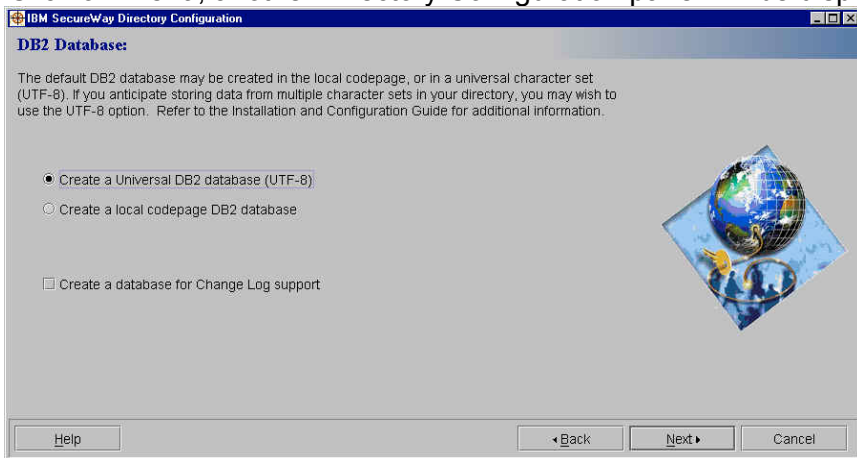
- c. Click on '**Next**'; the Directory Configuration panel will be displayed. Enter the Administrator DN and Password (we used `cn=root` and `Secure99`).



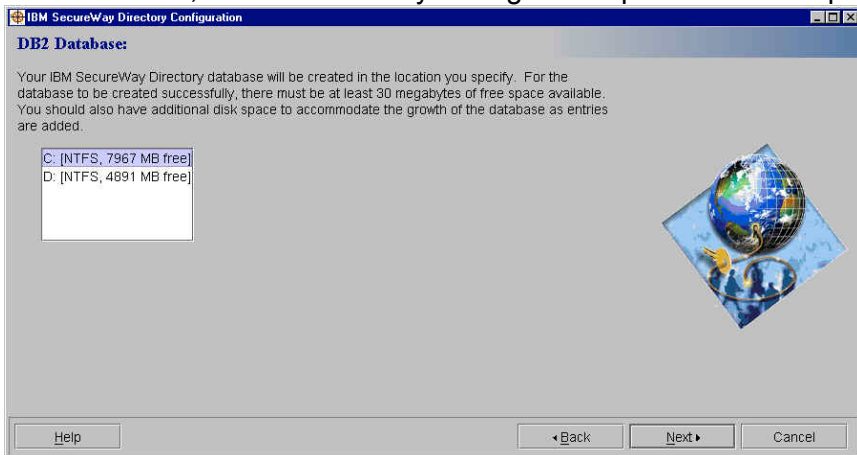
d. Click on '**Next**'; another Directory Configuration panel will be displayed:



e. Click on '**Next**'; another Directory Configuration panel will be displayed:

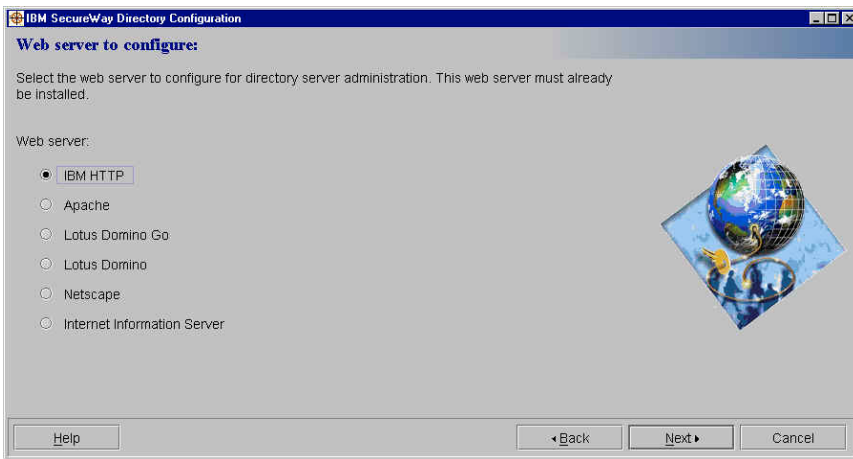


f. Click on '**Next**'; another Directory Configuration panel will be displayed:

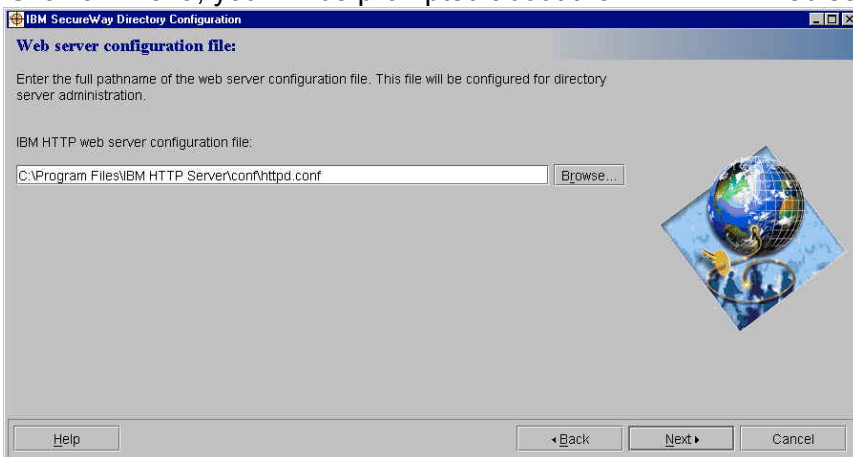


g. Click on '**Next**'; you will be asked which web server you want to configure for directory server administration. Ensure that 'IBM HTTP' is selected:

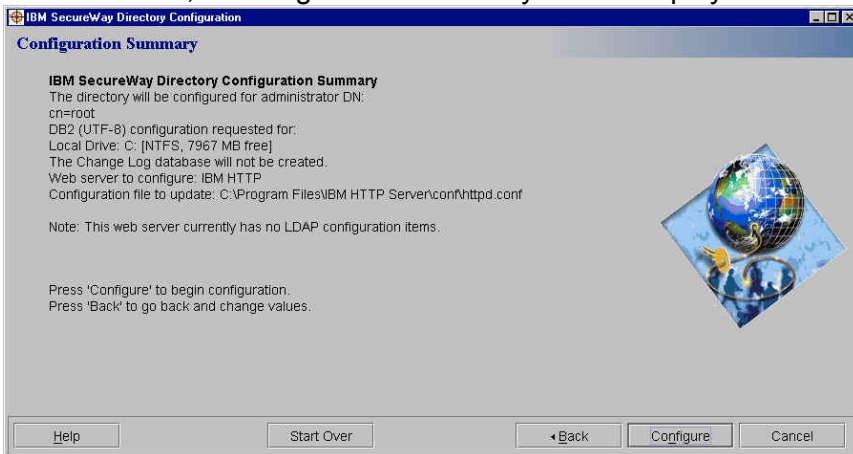




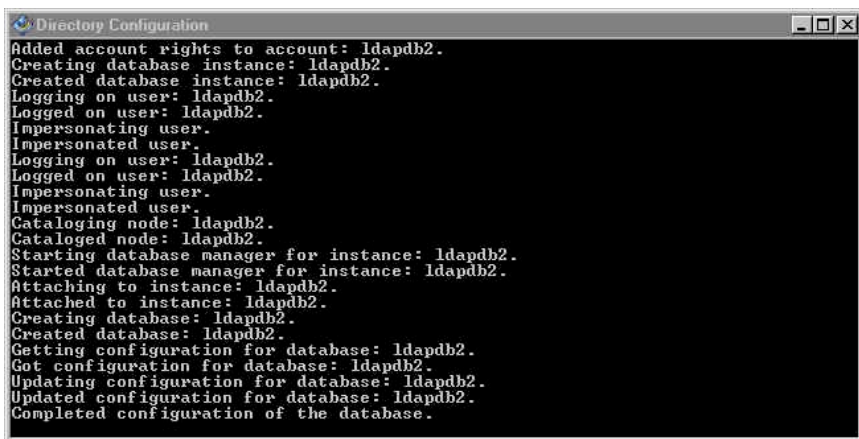
h. Click on 'Next'; you will be prompted about the IBM HTTP web server configuration file:



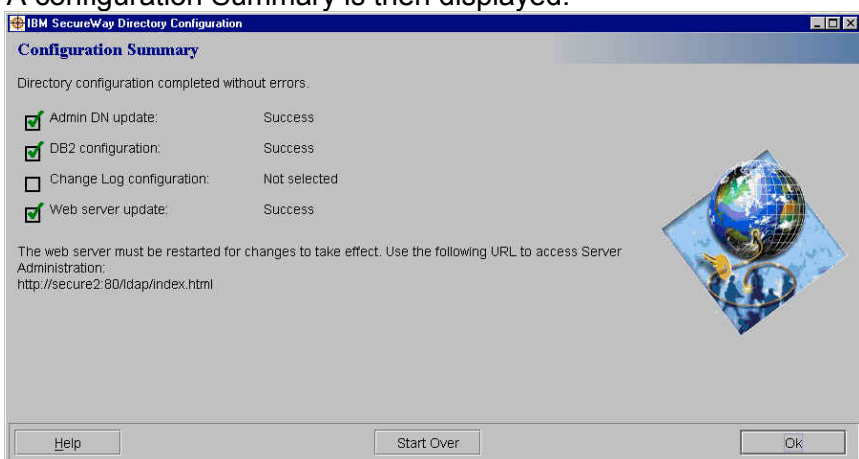
i. Click on 'Next'; a Configuration Summary will be displayed:



j. Review the settings and click on 'Configure'. A separate window will be started displaying messages regarding creating and configuring the ldapadb2 database:



k. A configuration Summary is then displayed:



l. Click on 'OK'.

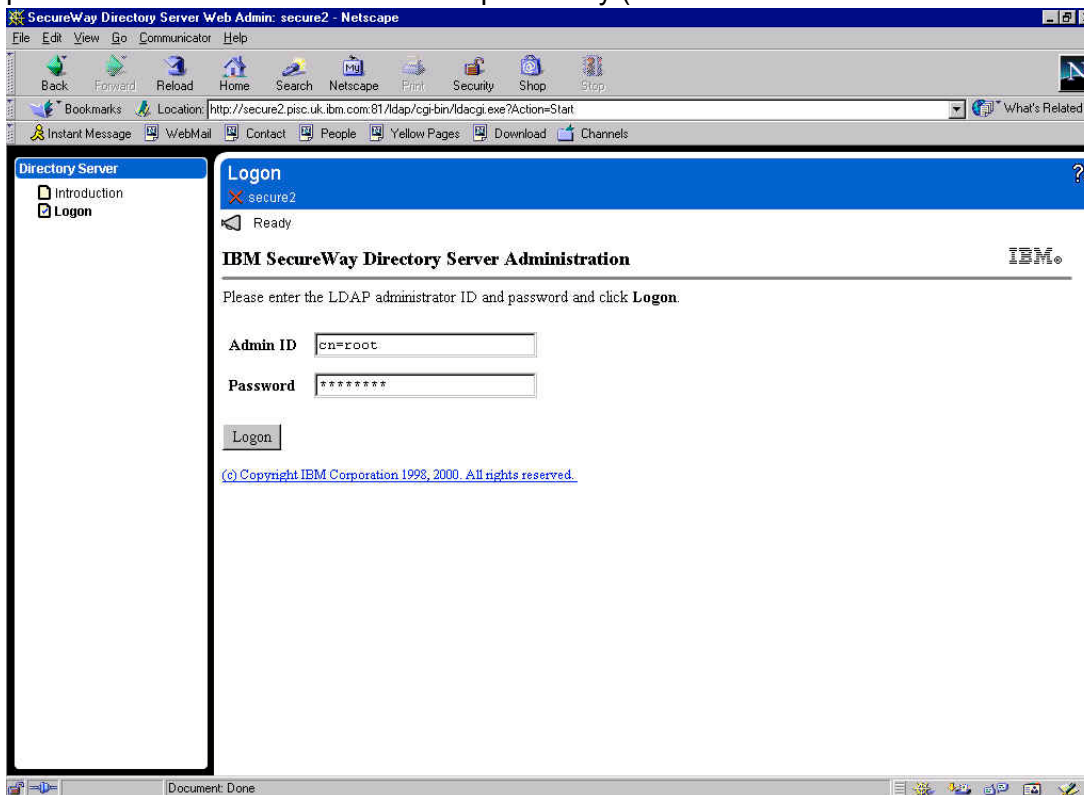
m. By default the IBM HTTP Server listens to port 80, the same as WebSEAL. To avoid port conflicts edit the HTTP configuration file, `httpd.conf`, by default found in the `C:\Program Files\IBM HTTP Server\conf` directory. Locate the port value in the `httpd.conf` file and change it from Port 80 to a different port number – we used Port 81.

n. Use **Start -> Settings -> Control Panel -> Services (NT)**, or **Start -> Programs -> Administrator Tools -> Services (2000)**, to start and restart HTTP Server for the changes made by the LDAP configuration, and the port number, to take effect.

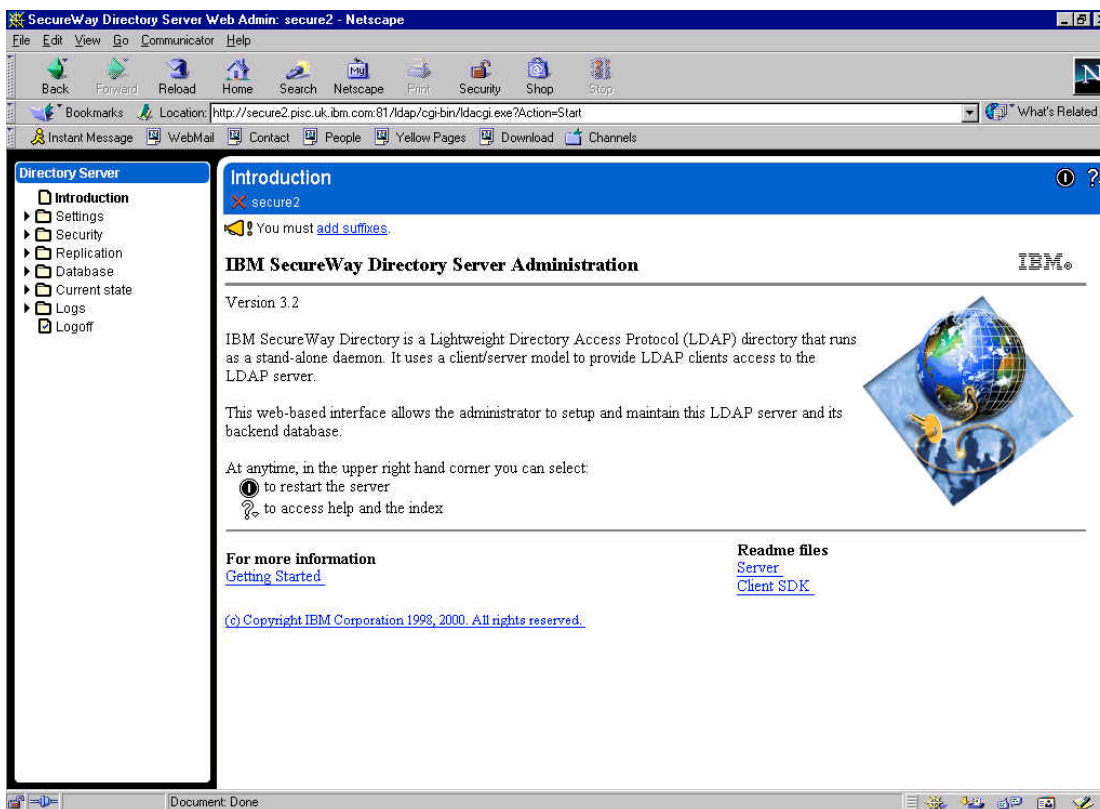
**Note:** If you have problems with the graphical interface, the LDAP configuration can be performed with the following manual commands:

- To configure the LDAP administrator id and password:  
`C:\Program Files\IBM\LDAP\bin\ldapcfg -u "cn=root" -p secure99`
- To configure the IBM HTTP Server for LDAP:  
`C:\Program Files\IBM\LDAP\bin\ldapcfg -s ibmhttp -f C:\Program Files\IBM HTTP Server\conf httpd.conf`
- To configure the default ldapdb2 instance and database:  
`C:\Program Files\IBM\LDAP\bin\ldapcfg -l C:\LDAPDB2\ (or any directory that has space for the database.)`

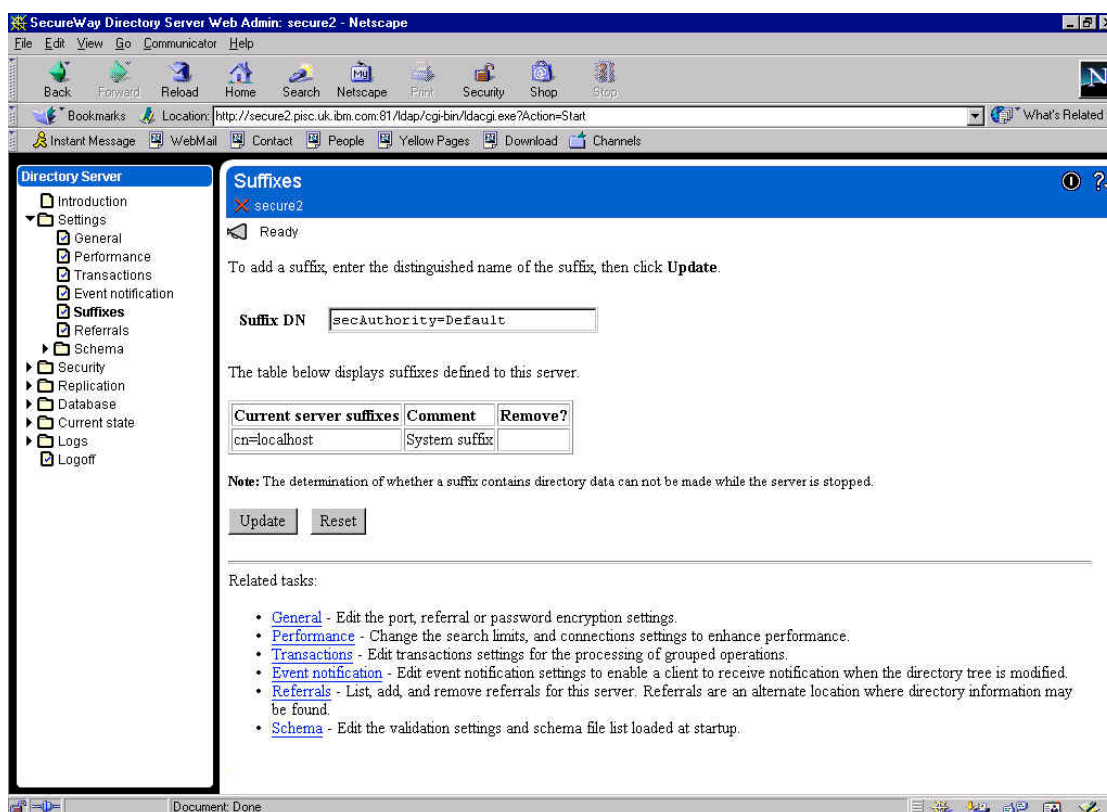
- o. Next to add the suffixes you need to LDAP, point a web browser at `http://hostname:port number/ldap/index.html` (the port number was 81 in our case). The SecureWay Directory Server Logon panel is displayed. Set the User ID to the LDAP Administrator ID and the password to that which was entered previously (`cn=root` and `secure99` in our case).



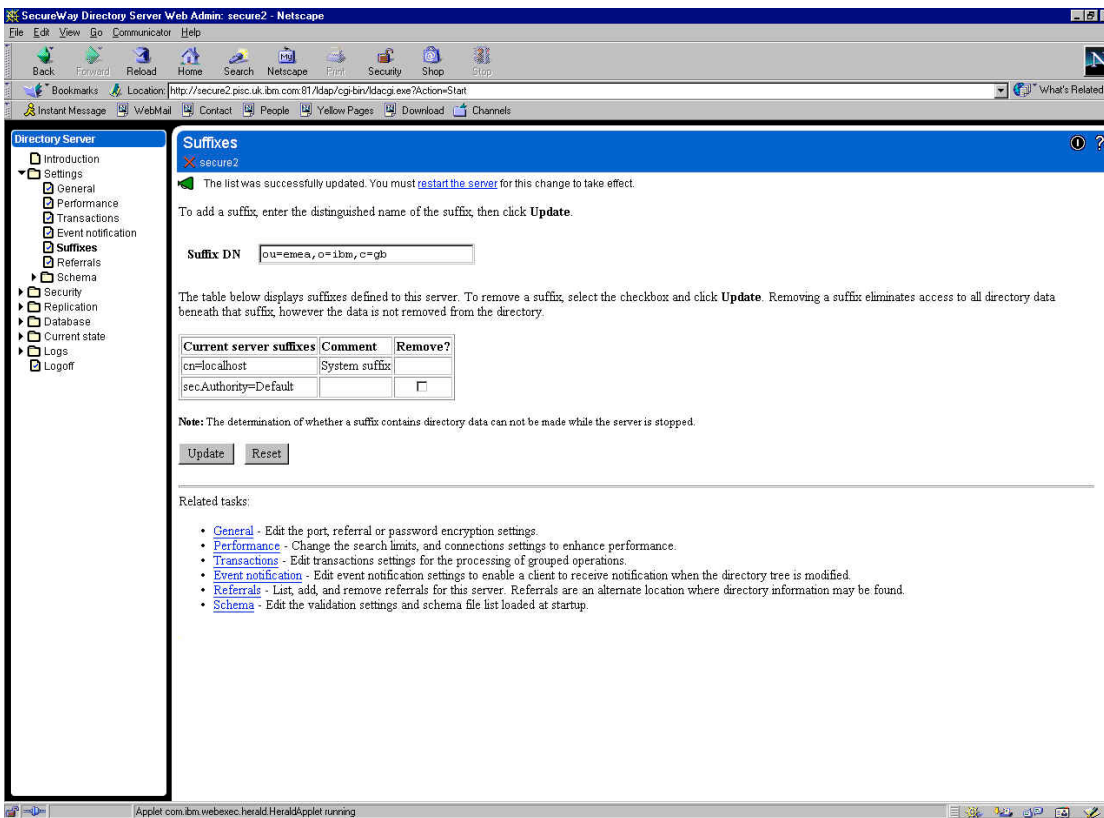
- p. Click on '**Logon**'. The 'IBM SecureWay Directory Server Administration' panel is displayed. It will indicate 'You must add suffixes' at the top of the screen.



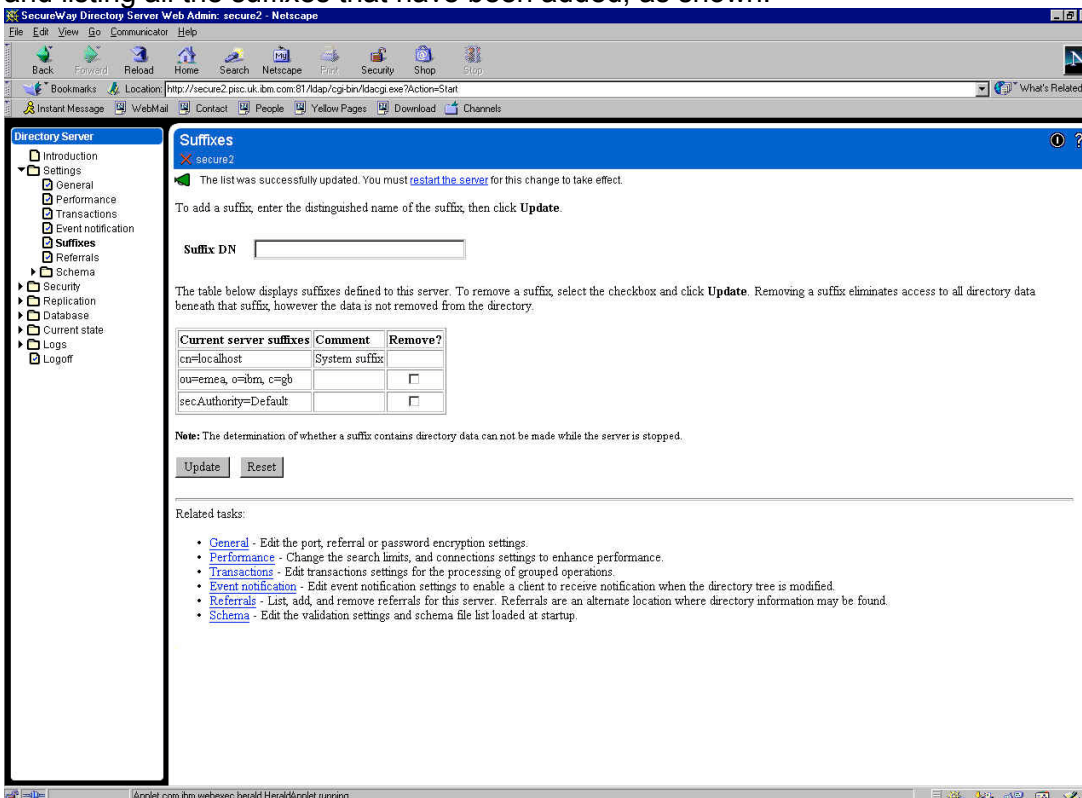
- q. If a message specifies ‘You must configure the database’ it may mean that one of the earlier installation steps failed. Ensure that the `\ldapdb2` directory was deleted before installing the Directory. Alternatively, try issuing `Start → Programs → IBM SecureWay Directory → SecureWay Directory Configuration`, and reconfigure the directory web server. (This appears to happen sometimes when certain files are left over from a previous DB2/LDAP installation.)
- r. Click on ‘Add suffixes’. Enter `secAuthority=Default` in the ‘Suffix DN’ box:



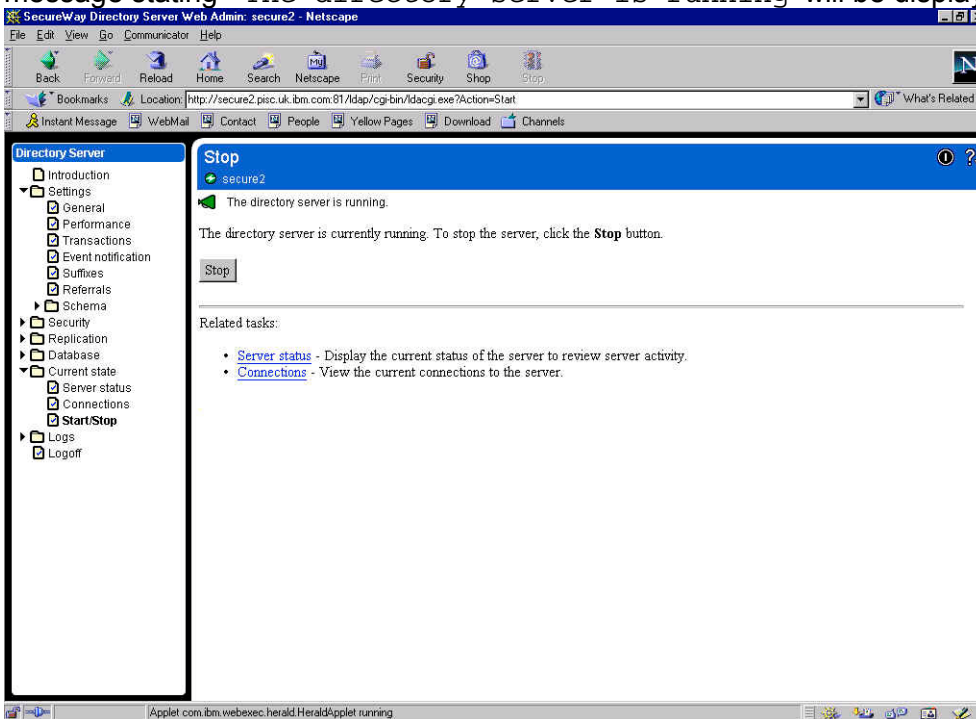
- s. Click on '**Update**'. The suffix should be added to the list of Current server suffixes and a message should be displayed stating 'The suffix was successfully added. You must restart the server for this change to take effect'.
- t. Enter a suffix for the Policy Director users and Global Sign-On (GSO) data (for example **ou=emea,o=ibm,c=gb** as shown below, or just **o=ibm,c=gb** as used elsewhere in this document) All the Policy Director resources subsequently defined must sit below the suffix defined here - thus if the country, organization and organizational unit are specified here, all PD resources will have to be held within that organizational unit, whereas if just the country is specified here, all PD resources will merely have to be held within that country. Alternatively it would be possible to specify just a country and organization. Clearly this decision will depend on the directory strategy of the organization in question.



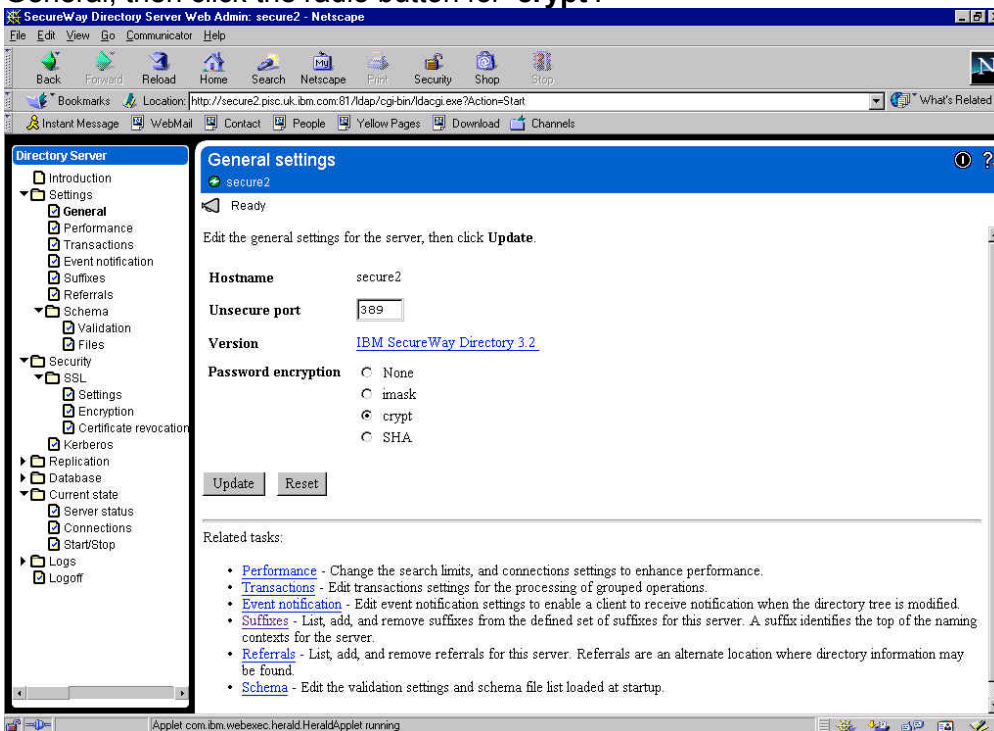
u. Click on 'Update'. A message should be displayed stating 'The list was successfully updated. You must restart the server for this change to take effect', and listing all the suffixes that have been added, as shown:



- v. Click on the [‘restart the server’](#) link at the top of the page. A message stating 'The directory server is starting' is displayed. This restart process can take several minutes. Then a message stating 'The directory server is running' will be displayed as below.



- w. You may wish to specify one-way password encryption. To do this, click on Settings → General, then click the radio button for **‘crypt’**:



- x. Then click on **‘Update’**. It will display a message: 'The changes were successfully updated. You must [restart the server](#) for these changes to take effect'. Click on [‘restart the server’](#) and wait for the server to restart.

y. The web browser is no longer required and may be closed.

### If you are unable to run the LDAP Administrative web server...

There have been installations where (for various reasons) it has not been possible to run a web server to perform the LDAP administrative operations. In that case an alternative approach is to edit the configuration file manually. The file in question is:

C:\Program Files\IBM\LDAP\etc\slapd32.conf

You can add the suffixes we added above by adding the following lines to slapd32.conf  
Beneath the entry `ibm-slapdSuffix: cn=localhost:`

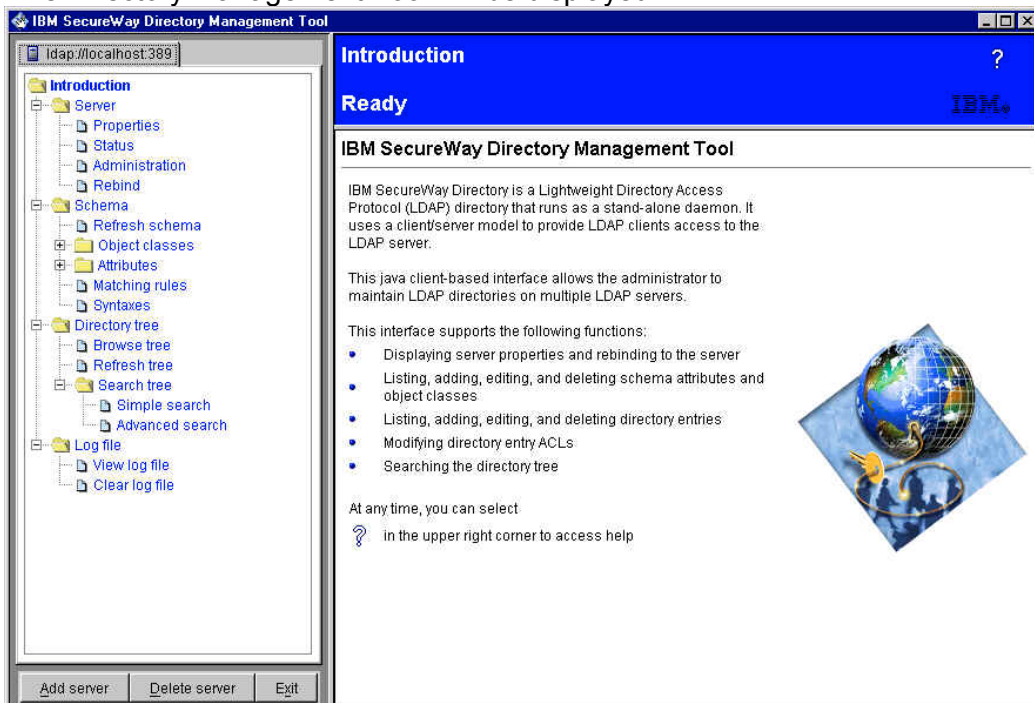
```
ibm-slapdSuffix: secAuthority=Default
ibm-slapdSuffix: o=ibm, c=gb
```

You can specify one-way password encryption by modifying the `ibm-slapdPwEncryption` line to:

```
ibm-slapdPwEncryption: crypt
```

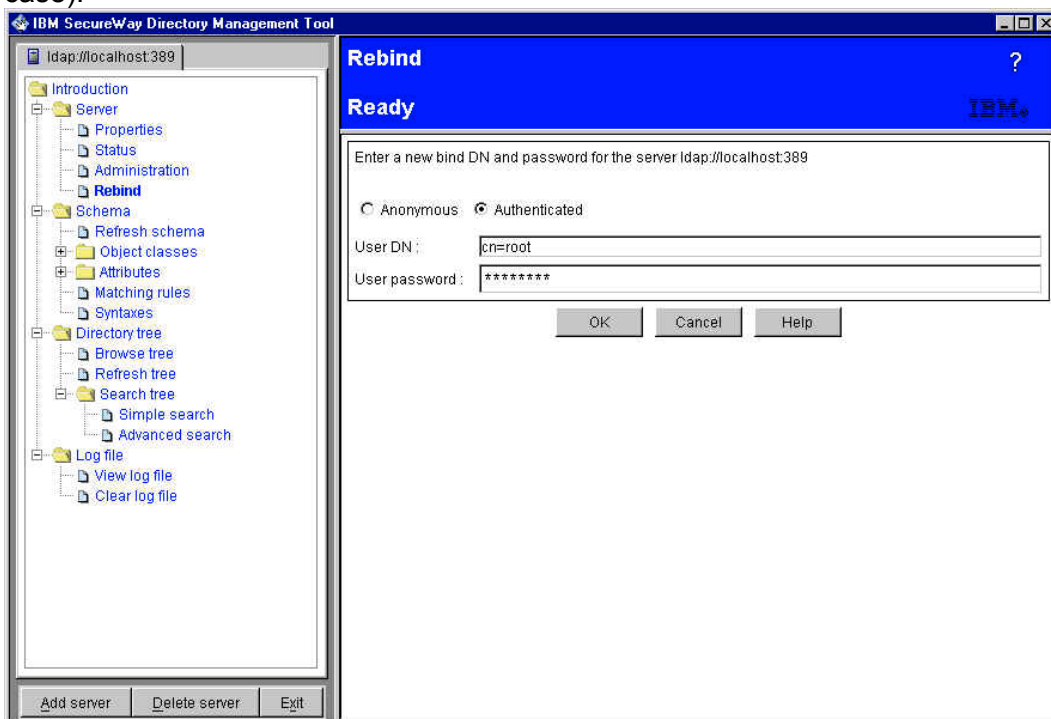
## 6.8 Directory Management Tool steps

- a. Click on Start -> Programs -> IBM SecureWay Directory -> Directory Management Tool
- b. The Directory Management Tool will be displayed:

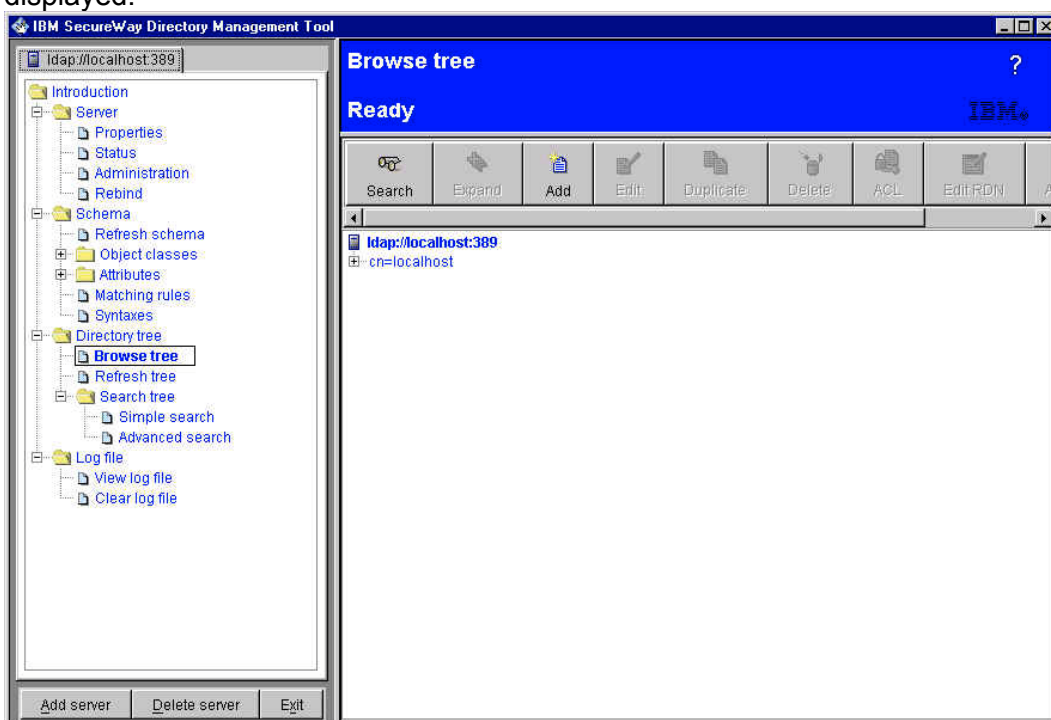




- c. Click on 'Rebind' (listed under 'Server'). A 'Rebind to server' dialogue panel is displayed. Click on 'Authenticated', and enter the administrator DN and password (cn=root, Secure99 in our case):



- d. Click on 'OK'. Message panels indicating that certain entries do not contain any data may be displayed; click on 'OK' to dismiss these dialogues. The 'Browse directory tree' panel will be displayed:



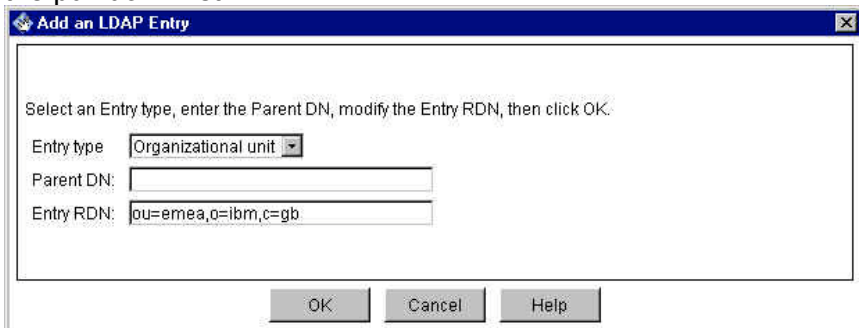
- e. Click on 'Add' in the upper right hand frame. An 'Add an LDAP Entry' dialogue is displayed. Against 'Entry RDN', enter the suffix previously entered for the Policy Director users and Global

Sign-On (GSO) data (`ou=emea,o=ibm,c=gb` in our case).

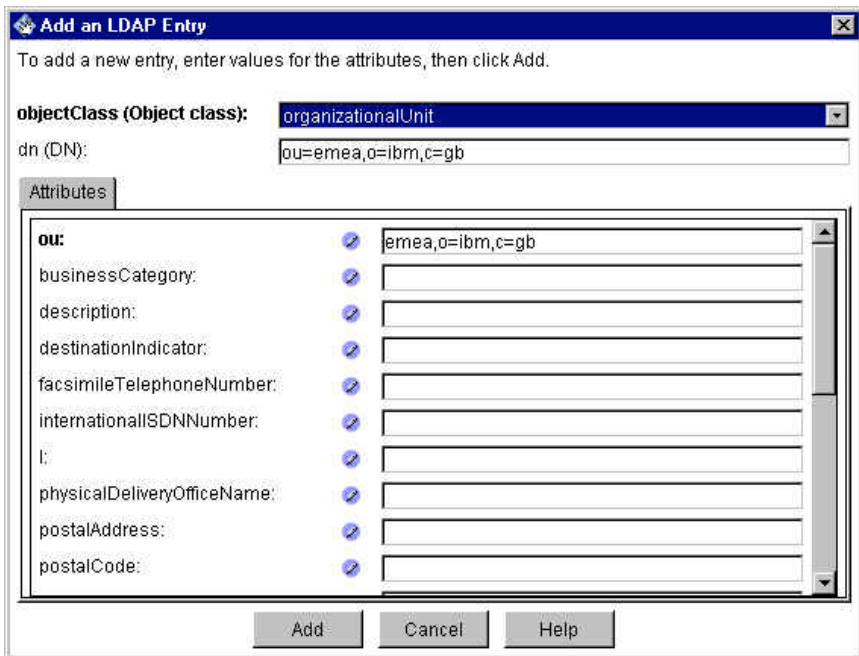
If you have specified an organizational unit (as in our case), select Select 'Organizational unit' as the entry type in the pull down list.

If you have specified an Organization (such as `o=ibm,c=gb`), select Select 'Organization' as the entry type in the pull down list.

If you have specified just a Country (such as `c=gb`), select Select 'Country' as the entry type in the pull down list.



f. Click on 'OK'.



g. Click on 'Add'. A warning will be displayed indicating that "secauthority=default" does not contain any data – click on 'OK' to dismiss this.

h. The entry which has just been added will be displayed:



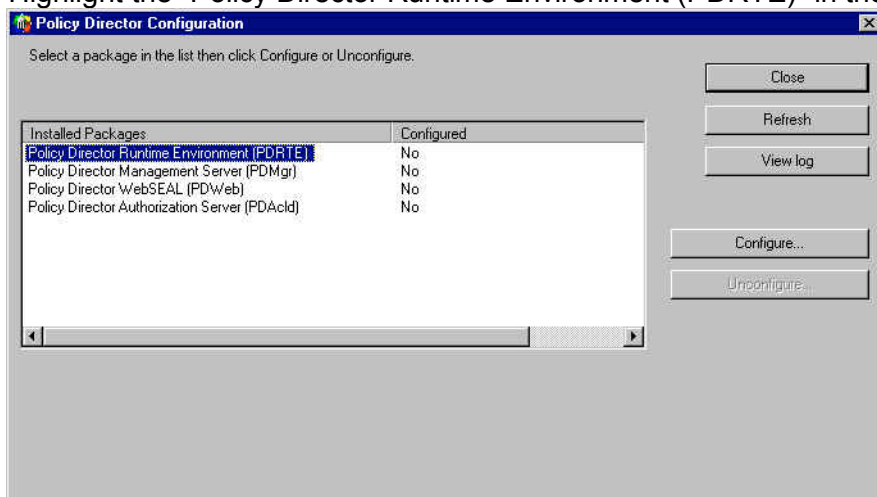
i. The Directory Management Tool is no longer required and can be closed.

j. The LDAP Configuration is now complete.

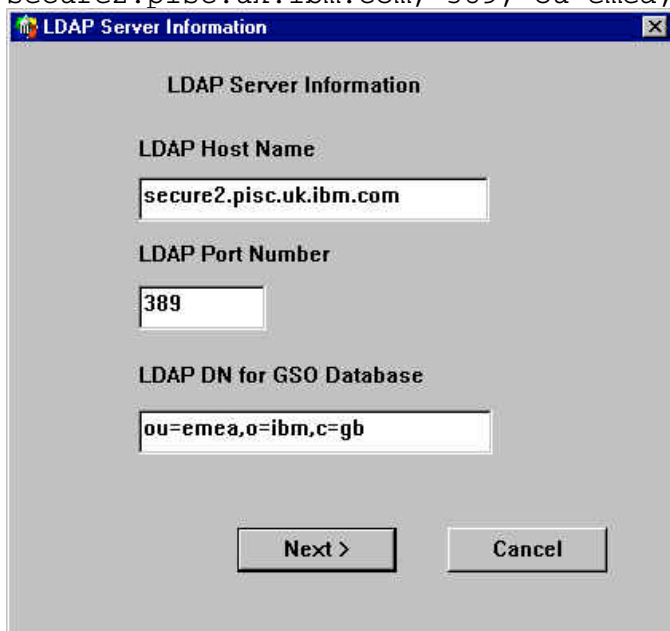
## 6.9 Policy Director Configuration (Windows)

**Note:** this section describes how to configure the policy director components we installed earlier.

- a. Use Start → Programs → Policy Director → Configuration. The 'Policy Director Configuration' panel appears.
- b. The servers need to be configured in the following order: Policy Director Runtime Environment, then Policy Director Management Server; then either Policy Director Authorization Server and/or Policy Director WebSEAL as required.
- c. Highlight the "Policy Director Runtime Environment (PDRTE)" in the installed packages column:

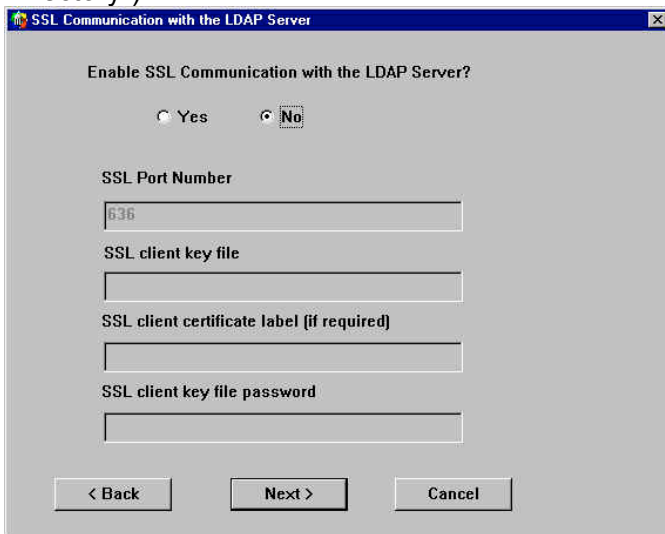


- d. Click on 'Configure'. You are prompted for the LDAP Server information. Enter the fully qualified LDAP Host Name, the port number and the LDAP DN for GSO. In our case the values were: `secure2.pisc.uk.ibm.com`, `389`, `ou=emea,o=ibm,c=gb`.

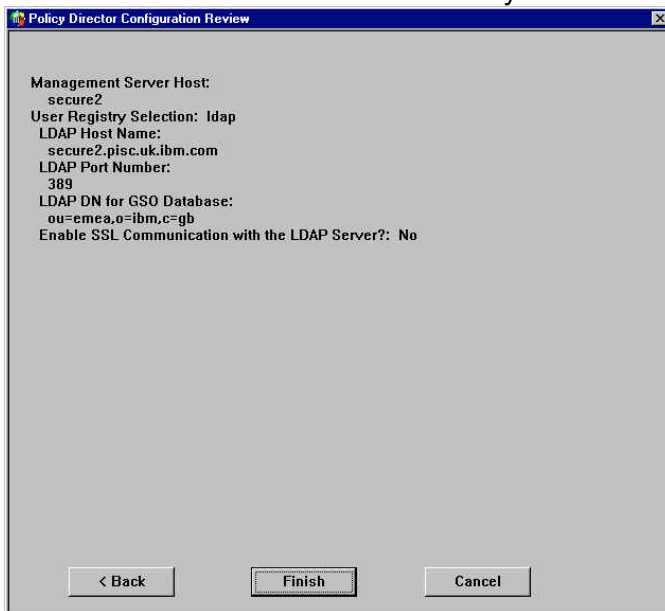


- e. Click on 'Next'. You are prompted whether to Enable SSL Communication with the LDAP

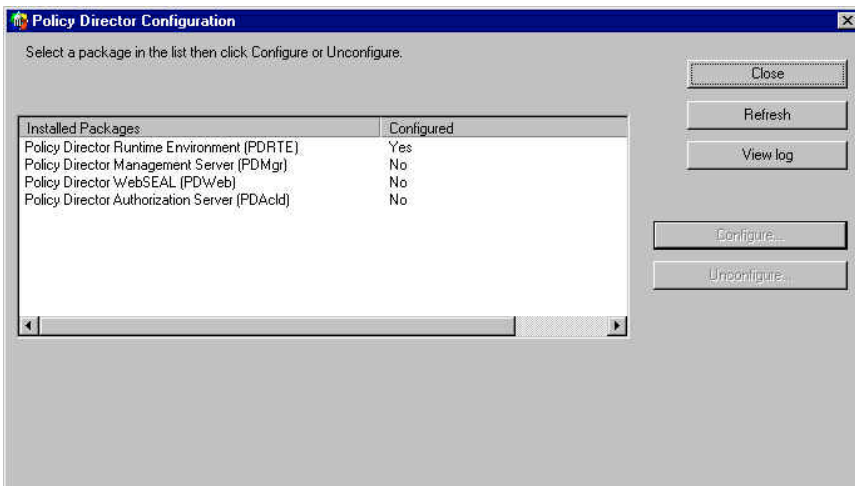
Server. Select **'No'**. (If you want to use SSL communication with the LDAP Server, ensure that you have followed the steps in a later section called “Setting up an SSL connection to the LDAP Directory”)



f. Click on **'Next'**. You are shown a 'Policy Director Configuration Review' panel:



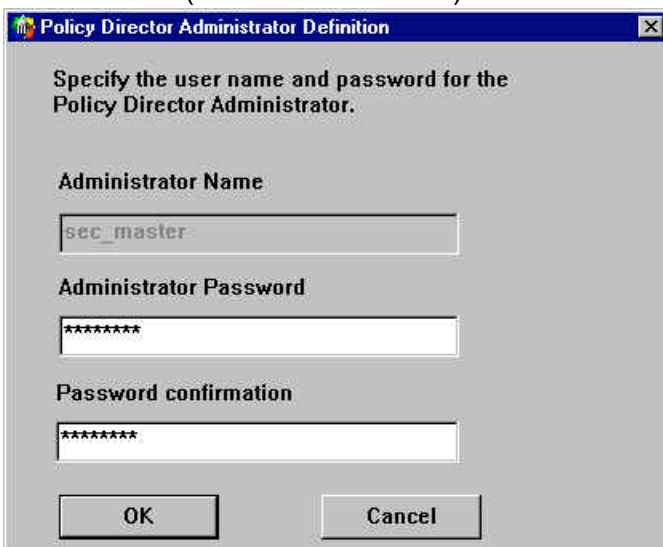
g. After reviewing the values click **'Finish'**. You will see a message 'Configuring Policy Director Runtime'. After a successful configuration, PD Runtime Environment will be marked as configured:



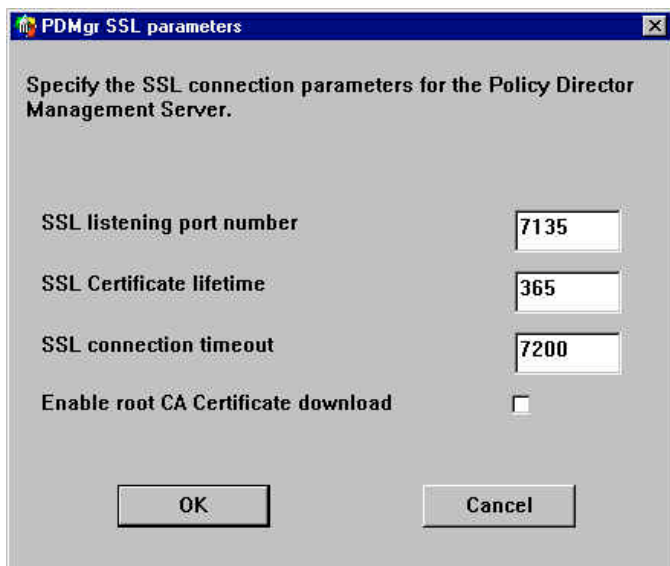
- h. Next highlight “Policy Director Management Server (PDMgr)” and click on ‘Configure’. The ‘LDAP Administrator Login’ panel is displayed. Enter the LDAP administrator name and password (`cn=root` and `Secure99` in our case):



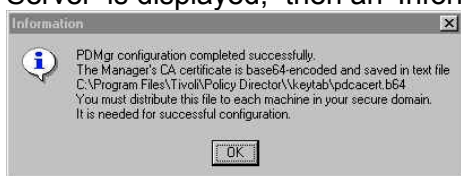
- i. Click ‘OK’. The ‘Policy Director Administrator Definition’ panel is displayed. The Policy Director Administrator Name is fixed as `sec_master`; specify the password for the Policy Director Administrator (we used `Secure99`):



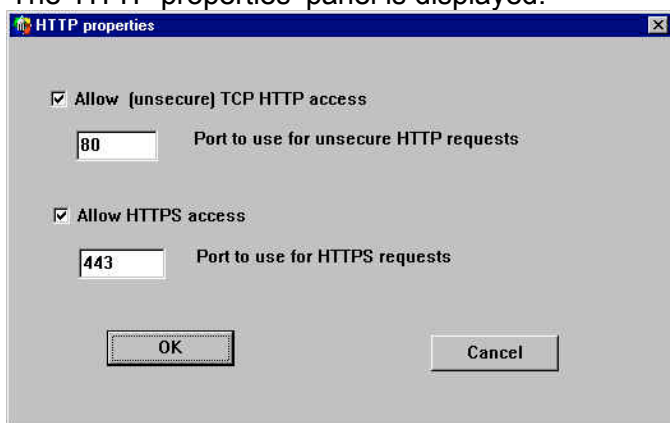
- j. Click on ‘OK’. The ‘PDMgr SSL parameters’ panel is displayed: this screen configures the ports that the Management Server will use for accepting SSL connections from the other PD servers, the pdadmin command line and the Admin Console.



- k. (If desired you can also select 'Enable root CA Certificate download'. This simplifies the distribution of the Root CA Certificate to subsequent Policy Director machines, but may introduce security exposures if the network can be compromised during the configuration step.)
- l. Accept these values and click on 'OK'. A message 'Configuring Policy Director Management Server' is displayed; then an 'Information' panel is displayed:



- m. Take note of this message: this certificate is used to support SSL communications between the Policy Director components and must be present on all PD servers configured into the secure domain. Click on 'OK' to continue.
- n. You are returned to the 'Policy Director Configuration' panel once again. Select the next component you want to configure, in our case WebSEAL. Highlight 'Policy Director WebSEAL (PDWeb)' and click on 'Configure'.
- o. The 'HTTP properties' panel is displayed:



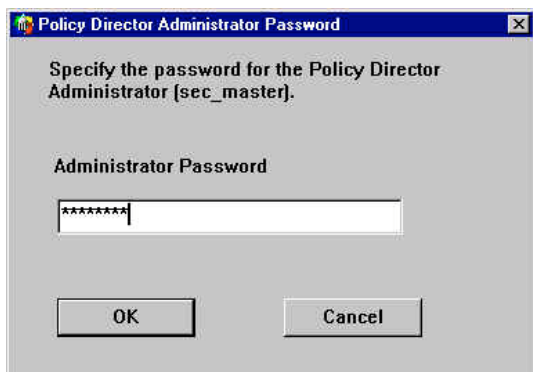
- p. Accept the values and click on 'OK'. The 'Policy Director Administrator Password' panel is displayed; enter the Policy Director Administrator password (secure99 in our case):



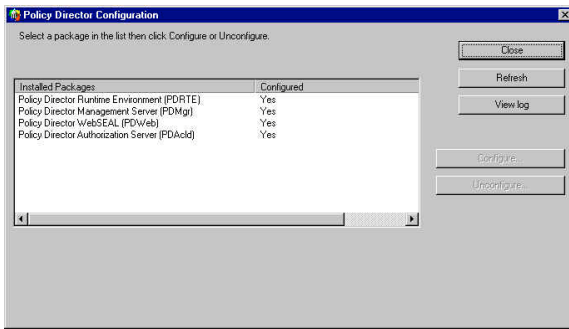
- q. Click on '**OK**'; WebSEAL is then configured.
- r. The 'Policy Director Configuration' panel is displayed once again. Highlight 'Policy Director Authorization Server (PDAcId)' and click on 'Configure'. The 'LDAP Administrator Login' is displayed; enter the Administrator name and password (`cn=root` and `secure99` in our case):



- s. Click on '**OK**'. The 'Policy Director Administrator Password' panel is displayed; enter the Policy Director Administrator password (`secure99` in our case):



- t. Click on '**OK**'. The Policy Director Authorization Server is then configured.
- u. You are then returned to the 'Policy Director Configuration' panel and if you have followed all the steps you should see that all the installed packages are now configured:



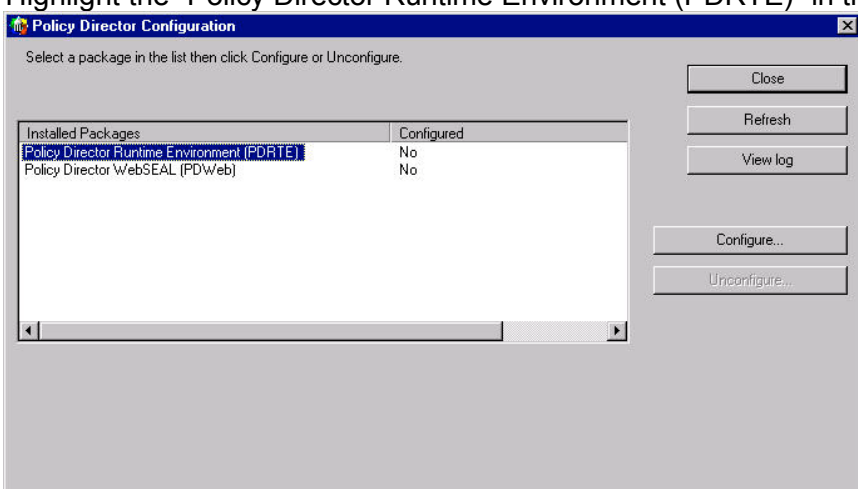
- v. This completes the Policy Director configuration. Click on 'Close' to close the panel. You may want to check that the Policy Director services you have installed are started in NT's services before doing any testing.
- w. You can now check that Policy Director is working by following the steps described in Section 17 - Initial Policy Director Validation on Page 123 below.



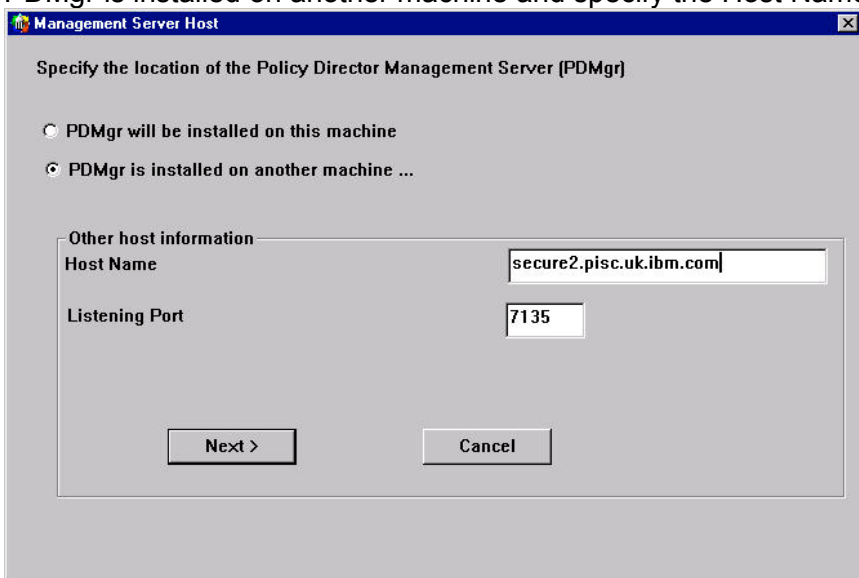
## 6.10 Policy Director RTE + WebSEAL Configuration (Windows)

This is an example of the steps to take when configuring a separate system with just WebSEAL installed.

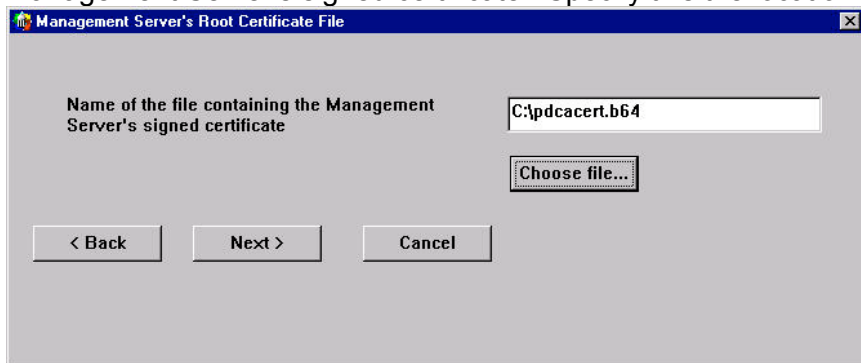
- a. Copy the file containing the pdmgrd CA Cert file from the pdmgrd to the WebSEAL machine C:\Program Files\Tivoli\Policy Director\keytab\pdcacert.b64 by default. Unless you selected “Enable root CA Certificate download” when configuring PDMgr.
- b. Use Start → Programs → Policy Director → Configuration. The ‘Policy Director Configuration’ panel appears.
- c. Highlight the “Policy Director Runtime Environment (PDRTE)” in the installed packages column:



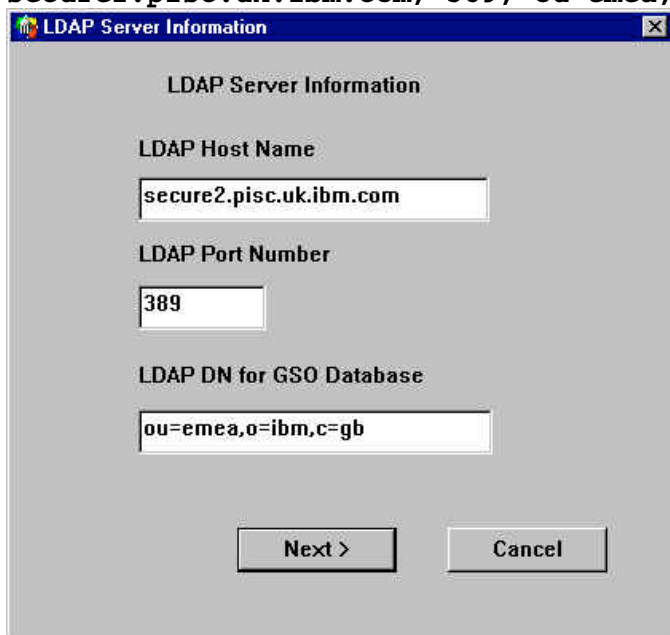
- d. Click on ‘Configure’. The Management Server Host dialogue box will be displayed. Specify that PDMgr is installed on another machine and specify the Host Name of the box running pdmgrd:



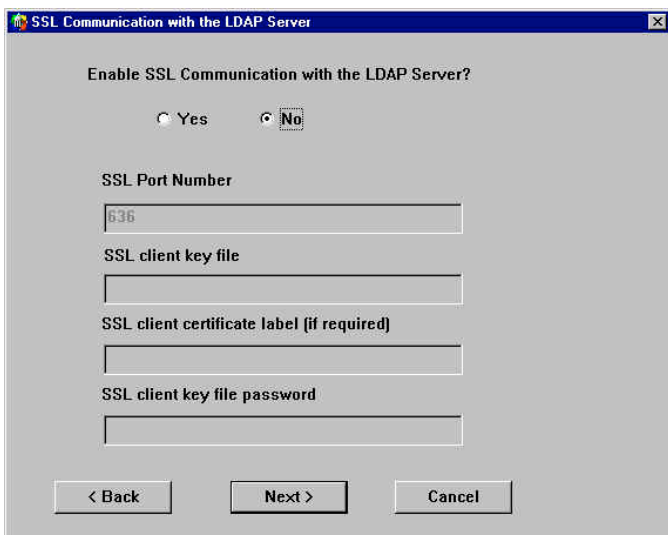
- e. Click on '**Next**'. You are required to specify the location of the file containing the PD Management Server's signed certificate. Specify this the location of this file.



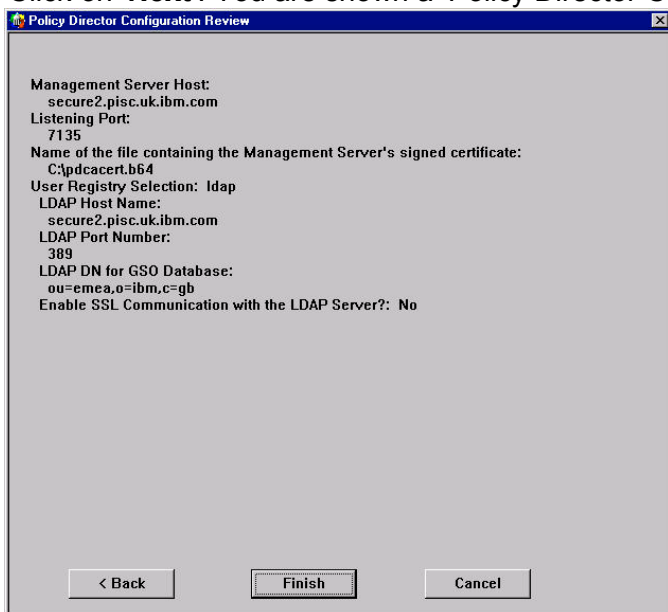
- f. Click on '**Next**'. You are prompted for the LDAP Server information. Enter the fully qualified LDAP Host Name, the port number and the LDAP DN for GSO. (In our case the values were: `secure2.pisc.uk.ibm.com`, `389`, `ou=emea,o=ibm,c=gb`).



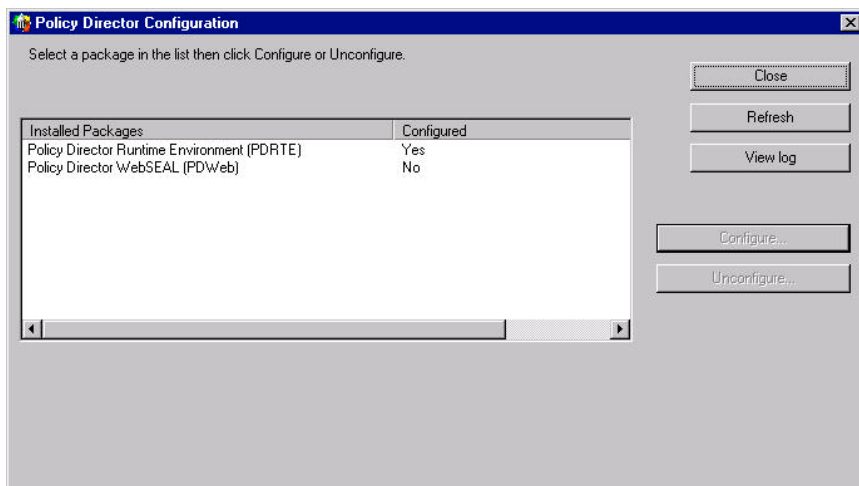
- g. Click on '**Next**'. You are prompted whether to Enable SSL Communication with the LDAP Server. Select '**No**'. (If you want to use SSL communication with the LDAP Server, ensure that you have followed the steps in the later section "Setting up an SSL connection to the LDAP Directory")



h. Click on 'Next'. You are shown a 'Policy Director Configuration Review' panel:

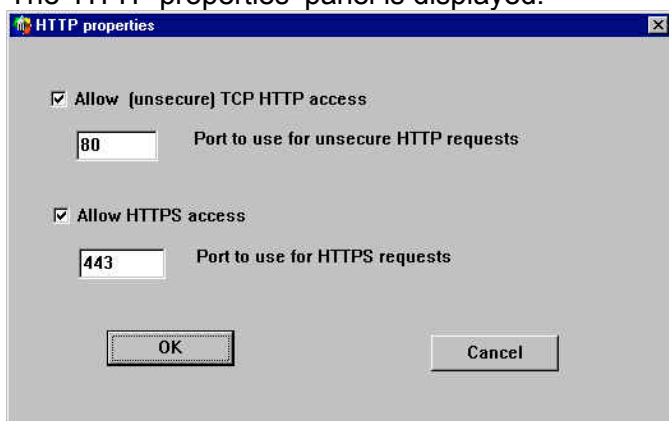


i. After reviewing the values click 'Finish'. You will see a message 'Configuring Policy Director Runtime'. After a successful configuration, PD Runtime Environment will be marked as configured:



j. You are returned to the 'Policy Director Configuration' panel. Highlight 'Policy Director WebSEAL (PDWeb)' and click on 'Configure'.

k. The 'HTTP properties' panel is displayed:



l. Accept the values and click on 'OK'. The 'Policy Director Administrator Password' panel is displayed; enter the Policy Director Administrator password (*secure99* in our case):



m. Click on 'OK'; WebSEAL is then configured.

n. You are then returned to the 'Policy Director Configuration' panel. This completes the Policy Director configuration. Click on 'Close' to close the panel.

o. You can now check that Policy Director is working by following the steps described in Section 17 - Initial Policy Director Validation on Page 123 below.

---

## 6.11 Web Portal Manager Installation & Configuration (Windows)

**Note:** this section describes how to install the Web Portal Manager (WPM) which is the new PD GUI and replaces the previous java based application.

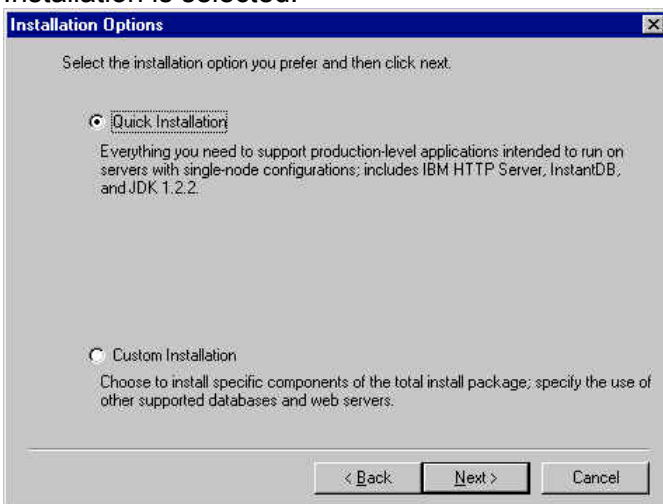
- a. Ensure that GSKit 4.0.3.168 or higher has been installed, and IBM HTTP Server with SSL support. (It is the 'Additional Modules' component in the HTTP Server installation that provides the SSL libraries.
- b. Ensure that you have the necessary prerequisites for WebSphere 3.5 Advanced Edition.
  - 75 MB disk space to install from CD
  - 300 MB disk space for product (footprint)
  - 256 MB of RAM to run IBM WebSphere Application Server (512 MB is recommended)
  - Network interface
- c. Use Start -> Settings -> Control Panel -> Services (NT) or Start -> Programs -> Administrator Tools -> Services (2000) to stop the IBM HTTP Server and IBM HTTP Administration services.
- d. Insert the **Tivoli SecureWay Policy Director Web Portal Manager Version 3.8** CD.
- e. Using 'My Computer' or Windows Explorer find the **lwindows\websphere** directory on the CD, and double click on **setup.exe**. The 'Choose Setup Language' dialog box appears:



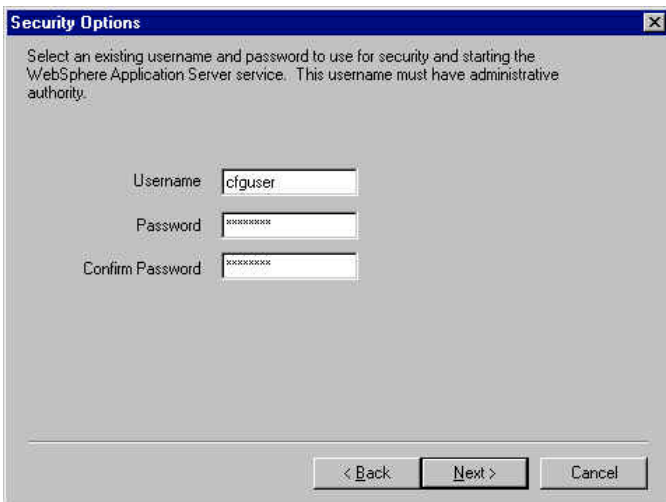
- f. Select a language and click on '**OK**'; The WebSphere Application Server 3.5 welcome screen is displayed:



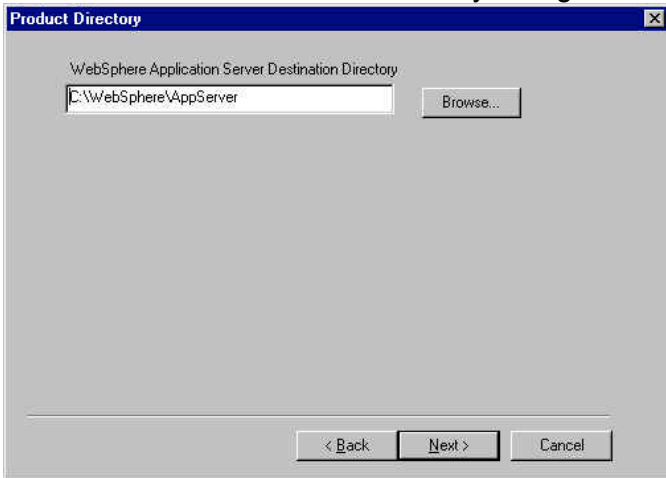
- g. Click on '**Next**'; the Installation Options dialogue box is displayed. Ensure that 'Quick Installation' is selected:



- h. Click on '**Next**'; specify a username and password under which the WebSphere Application Server service is to run; we used a user ID of `cfguser`, password `secure99`:



i. Click on 'Next'; the Product Directory dialogue box is displayed:



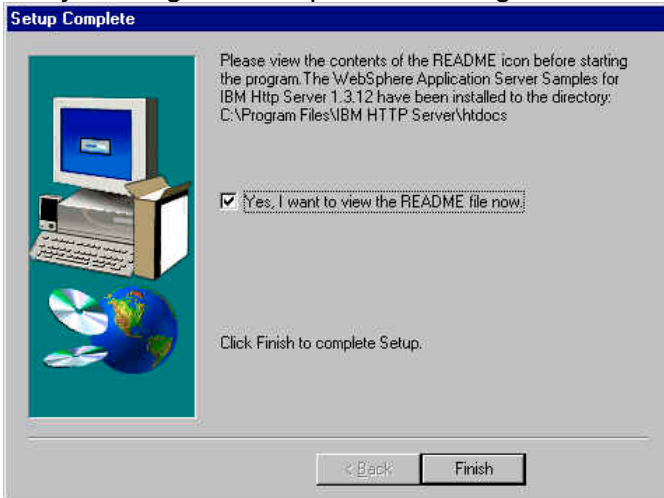
j. Click on 'Next'; the 'Select Program Folder dialog box is displayed:



k. Click on 'Next'; the files are copied across; you are prompted to confirm the directory containing the IBM HTTP Server configuration file:



- l. Click on **'OK'**; the remaining files are copied across and the **'Setup Complete'** panel is displayed, and you are given the option of viewing the README.



- m. Click on **'Finish'**; the **'Restarting Windows'** dialogue box will be displayed. Select **'No, I will restart my computer later'**:



- n. Click on **'OK'**.

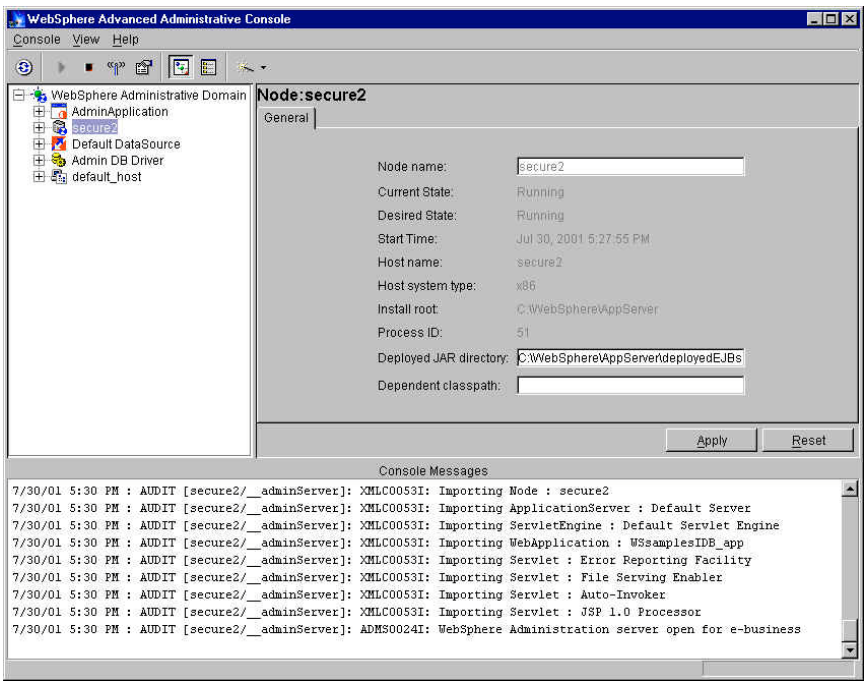


- o. Still using the **Tivoli SecureWay Policy Director Web Portal Manager Version 3.8** CD: copy all the files from the **windows\websphere\PTf4** directory on the CD to a temporary directory on the hard drive.
- p. Run **install.bat** from the temporary directory:

```

C:\temp\websphere-PTF4>install
Enter the directory where the IBM WebSphere Application Server is installed:
c:\websphere\appserver
WASHOME c:\websphere\appserver
JDKHOME c:\websphere\appserver\jdk
      1 file(s) copied.
"Installing the WebSphere Application Server Advanced Edition 3.5 PTF 4"
. . . .
. . . .
. . . .
2001/07/30 17:07:34 Please view the activity log for details.
Do you wish to upgrade the WebSphere Application Server samples?(Yes/No)
Yes
In order to update the WebSphere Application Server Samples
the currently configured WebServer's doc root must be specified
Eg. C:\IBM HTTP Server\htdocs
Please enter your webserver's doc root path:
C:\Program Files\IBM HTTP Server\htdocs
C:\Program Files\IBM HTTP Server\htdocs
Is this correct?(Yes/No)
yes
142 File(s) copied
47 File(s) copied
21 File(s) copied
WARNING: If you install IBM HTTP Server PTF, you may not be able to uninstall it
cleanly. The Gskit
package will not be uninstalled.
Do you wish to upgrade the IBM HTTP Server 1.3.12:(Yes/No)
no
. . . .
. . . .
. . . .
2001/07/30 17:10:59 Installation completed with no errors.
2001/07/30 17:10:59
2001/07/30 17:10:59 Please view the activity log for details.
846 File(s) copied
IBM WebSphere Application Server V3.5.4 Standard Fixpack install complete
    
```

- q. Re-boot the computer by issuing Start -> Shut Down -> 'Restart the computer'.
- r. Use Start -> Settings -> Control Panel -> Services (NT) or Start -> Programs -> Administrator Tools -> Services (2000) to start the IBM WS AdminServer.
- s. Ensure that WebSphere Application Server has started correctly by running the admin console via Start -> Programs -> IBM WebSphere -> Application Server V3.5 -> Administrator's Console:

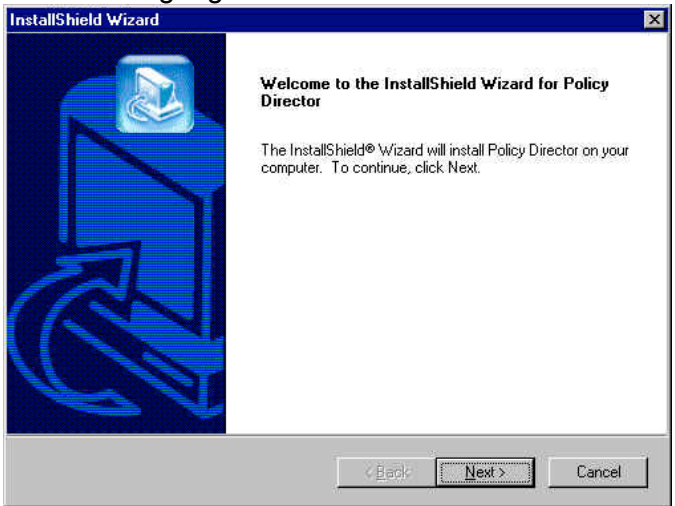


t. Still using the **Tivoli SecureWay Policy Director Web Portal Manager Version 3.8** CD:

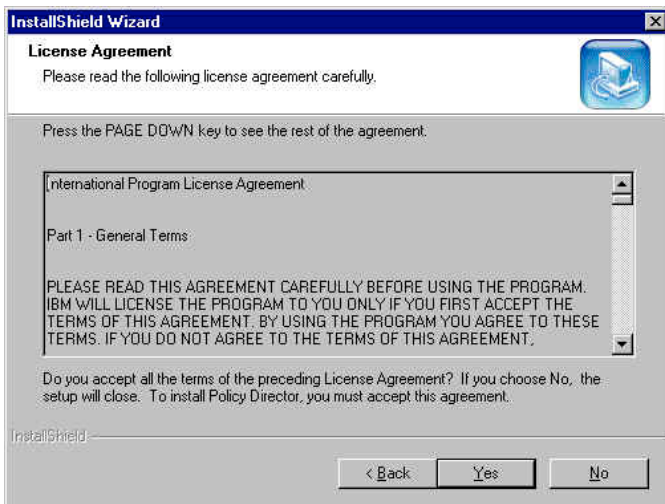
u. Using 'My Computer' find the **\Policy Director\Server** directory on the CD, and double click on **setup.exe**. The 'Choose Setup Language' dialogue box is displayed:



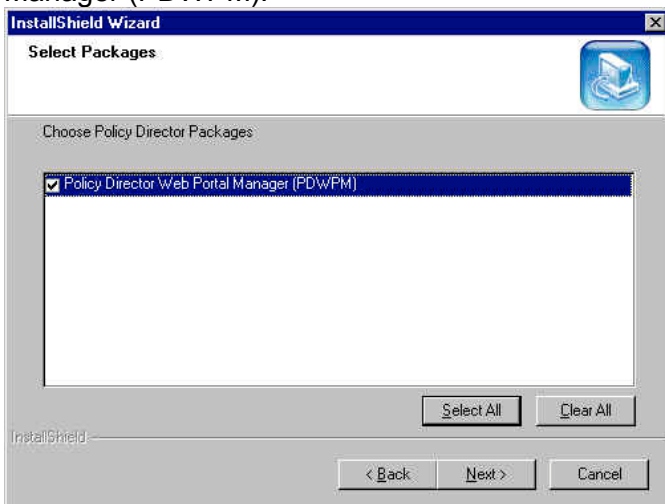
v. Select a language and click on '**OK**'. The InstallShield Wizard panel will be displayed:



w. Click on '**Next**'. The License Agreement panel is displayed:



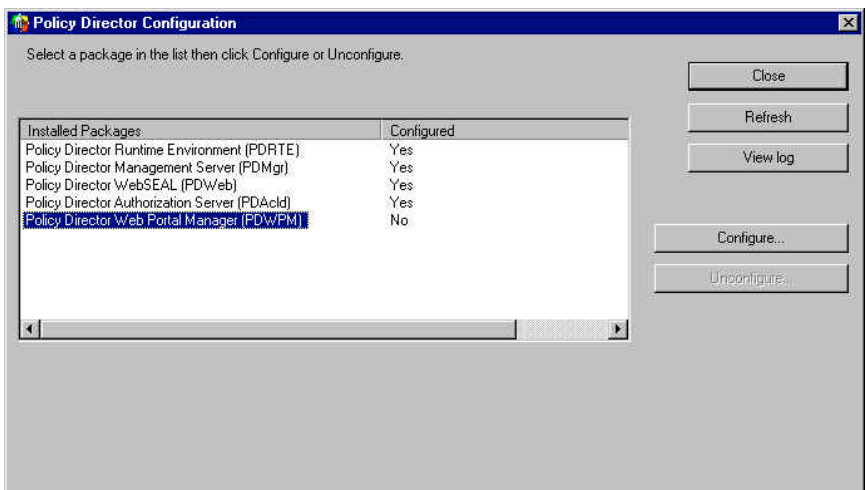
- x. Click on **'Yes'**. The **'Select Packages'** panel will be displayed. Select **Policy Director Web Portal Manager (PDWPM)**:



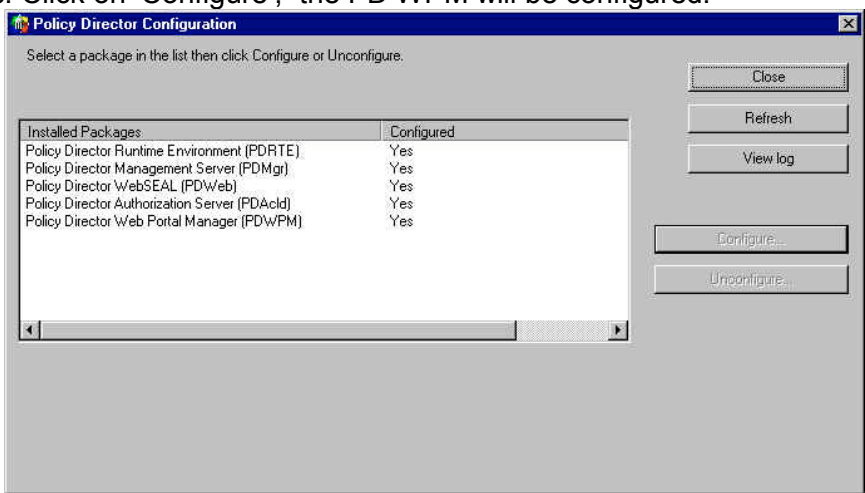
- y. Click on **'Next'**. The product will be installed, and then an Information message displayed:



- z. Click on **'OK'** to dismiss the dialogue.
- aa. Use Start → Programs → Policy Director → Configuration. The **'Policy Director Configuration'** panel appears.
- bb. Highlight the **"Policy Director Web Portal Manager (PDWPM)"** entry in the installed packages column:



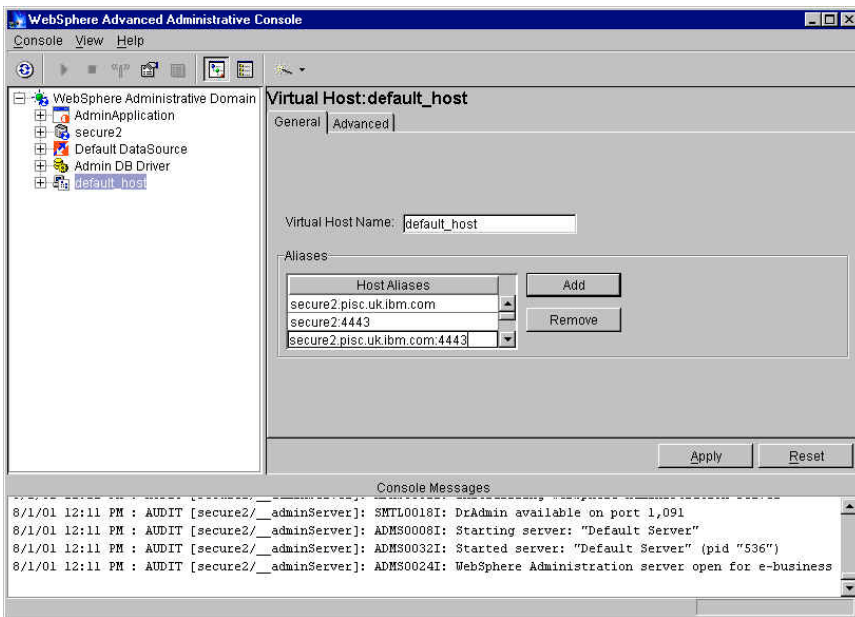
cc. Click on 'Configure'; the PD WPM will be configured:



dd. If you are running WebSEAL on the same machine that you are using to run WPM and want WebSEAL to own port 443 for SSL communication then edit the HTTP configuration file, `httpd.conf`, by default found in the `C:\Program Files\IBM HTTP Server\conf` directory. Locate the references to 443 value in the `httpd.conf` file and change the entries `Listen 443` and `<VirtualHost :443>` to a different port number – we used `4443`.

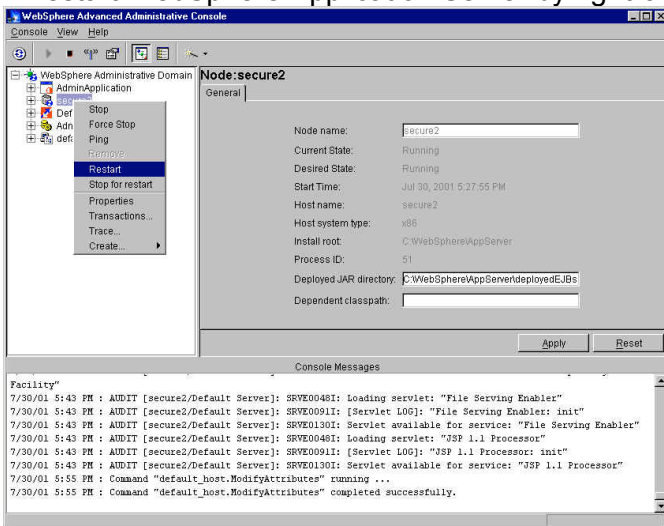
ee. Use Start → Settings → Control Panel → Services to stop and re-start IBM HTTP Server for the changes to take effect.

ff. Use Start → Programs → IBM WebSphere → Application Server V3.5 → Administrator's Console to start the WebSphere Administrative Console; Click on the '+' sign behind WebSphere Administrative Domain and click on default\_host (in the left hand panel), then add entries which include the revised SSL port numbers to the hostnames listed under HostAliases. In our case the new entries were `secure2:4443` and `secure2.pisc.uk.ibm.com:4443`:

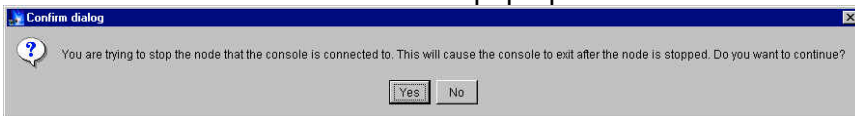


gg. Click on **'Apply'**.


hh. Restart WebSphere Application Server by right-clicking on your machine's hostname:



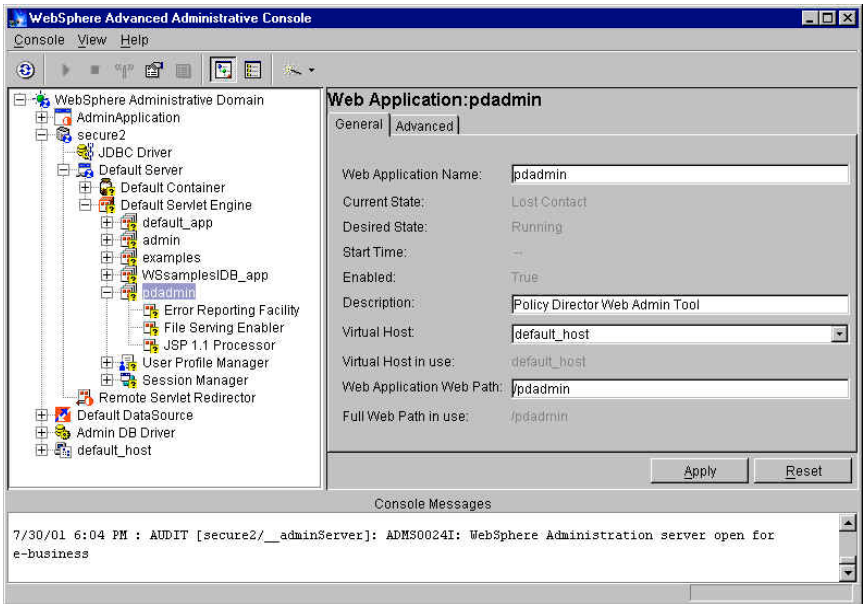
ii. And then click on **'Restart'** from the pop-up menu. A confirm dialogue box is displayed:



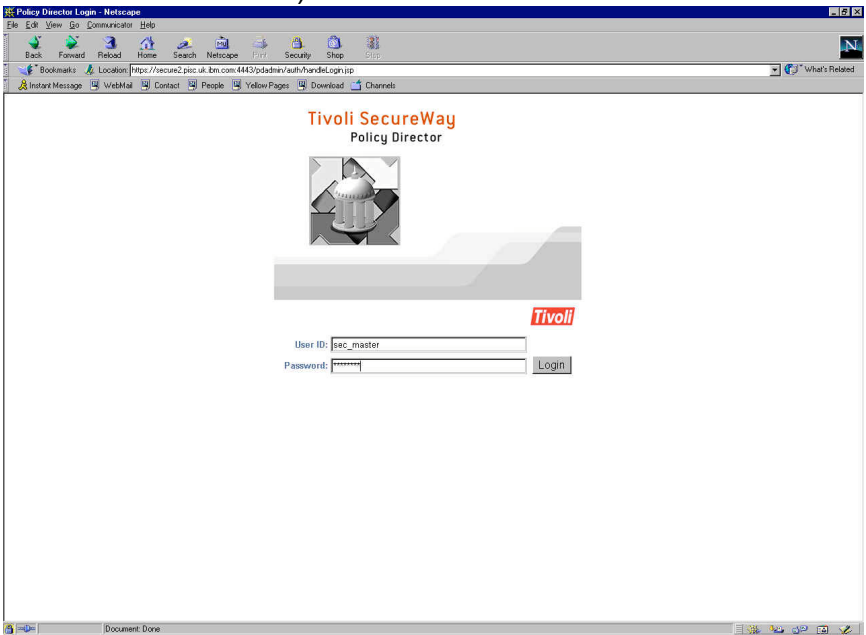
jj. Click on **'Yes'**. As part of restarting WebSphere Application Server the WebSphere console is closed.

kk. Use Start → Programs → IBM WebSphere → Application Server V3.5 → Administrator's Console; the presence of the  symbol to the right of the machine name indicates that the Default Server is running:

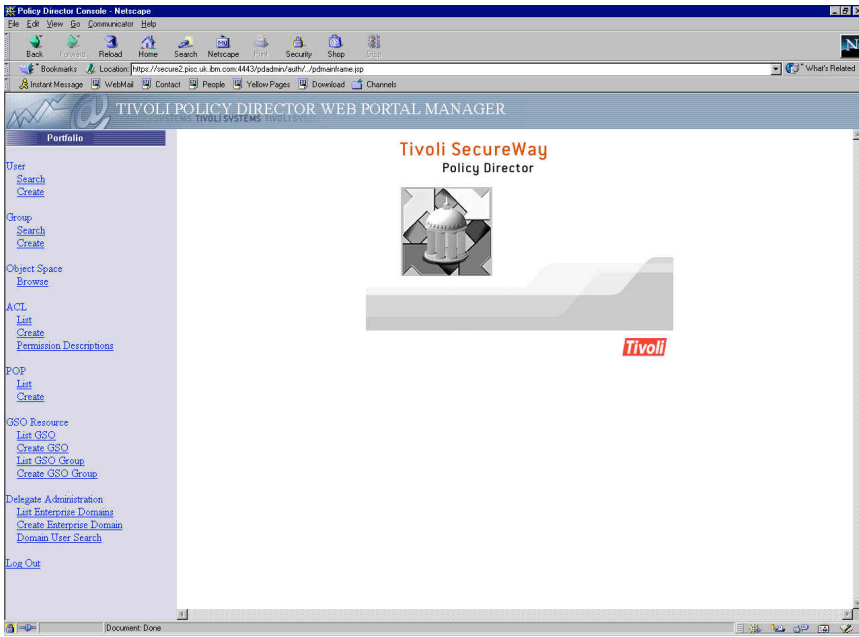
ll. You can use the console to verify that WPM is running:



mm. Point a web browser at `https://hostname:port number/pdadmin` (the port number was 4443 in our case). Enter a PD administrator userid and password (`sec_master` and `Secure99` in our case):



nn. Click on 'Login':



oo. From here you can use the Web Portal Manager to administer PD.

---

## Part III - AIX Environment

**Note:** PD 3.8 now provides a quick installation path using shell scripts for UNIX systems such as AIX and Solaris - these scripts make it easy to install Policy Director by automatically installing required software and prerequisites. We have not yet documented their use in an AIX environment. The following sections describe just the native install processes for AIX.

---

### 7. AIX System Preparation and general AIX Notes

- A Policy Director AIX 4.3.3 system requires the following software patch for the operating system: `bos.rte.libpthreads`. This patch must be at level 4.3.3.51 or greater. You can download this patch from the following support site:  
<http://www-1.ibm.com/support/rs6000.html>
- We try to assume a minimum level of AIX knowledge in these chapters: we have therefore tried to document most steps, but we may not have mentioned every **F4**, 'Enter' etc.
- Ensure that the date and time are set correctly across the environment you are using - this may avoid problems later on.
- Ensure that you have IP connectivity (for example, attempt to 'ping' another machine).
- Our experiences here are based on AIX 4.3.3, although we have successfully followed the same procedures on other versions of AIX.
- Throughout these chapters we make use of an AIX system management tool called **SMIT**. You launch this by typing '**smitty**' at a command line - this will start the menu driven tool.
- During the installation Policy Director and its pre-requisites it will be necessary to use a number of CDs. At some points you may need to mount them explicitly using with the `mount` command.

Depending on how your AIX system has been set up you may need to create a file system on which to mount the CD:

Using **smitty**, select:

System Storage Management (Physical & Logical Storage)

File Systems

Add / Change / Show / Delete File Systems

CDROM File Systems

Add a CDROM File System (or you can use the `Change / Show` option if you think that this may already have been set).

In the '**DEVICE Name**' field, press **F4** then select the CD-ROM device (in our case `cd0`) and press **Enter**

In the `MOUNT POINT` field, enter a new directory name where you want to mount the CD (in



our case `/cdrom`) and press **Enter**

When you see `OK` next to `Command:`, press **F10** to exit smitty.

If you do not specify that this should be mounted automatically at system restart, you will need to type `mount /cdrom` when you are going to use this mount point.

- Please be aware that the graphical screens shown in these chapters may vary slightly depending on your AIX environment.
- Note also that file and directory names in AIX are case sensitive.
- **Disk space: ensure that there is sufficient space in the various filesystems.** Whereas smitty will automatically increase the allocation if necessary, other steps will just fail frequently without any helpful error messages. The increases in disk space during the Policy Director installation described here are as detailed below. Clearly this does not take into account the storage required for a large user registry, etc., but is provided for information.

Increases in filesystem usage during install and configure steps			
Filesystem	512-blocks used	MB used	Inodes used
<code>/</code>	3,300	1.6	214
<code>/usr</code>	741,000	370	4374
<code>/var</code>	4,600	2.3	197
<code>/tmp</code>	1,300	0.6	11
<code>/home</code>	54,400	27	486

---

## 8. LDAP Server installation/configuration (AIX)

---

### 8.1 Operating system pre-requisites

The IBM SecureWay Directory requires these levels of the following filesets:

```
X11.Dt.lib 4.3.3.2
X11.Dt.rte 4.3.3.3
X11.adt.motif 4.3.3.1
X11.base.lib 4.3.3.2
X11.base.rte 4.3.3.2
X11.compat.lib.X11R5 4.3.3.2
X11.motif.lib 4.3.3.2
X11.motif.mwm 4.3.3.1
bos.adt.include 4.3.3.1
bos.adt.prof 4.3.3.3
bos.net.tcp.client 4.3.3.3
bos.rte.libpthreads 4.3.3.3
bos.sysmgt.serv_aid 4.3.3.2
```

The 4.3.3.0 levels of these filesets are not sufficient, and if they are not already installed on your system you will need to upgrade. (You can type, for example, `lslpp -l |grep X11.Dt.lib` to determine the level of `X11.Dt.lib` installed on your machine. If the system is for demonstration use you can upgrade using CD 23 from AIX DEMOpkg 2000.) This upgrade process is not described here any further.

---

### 8.2 Install the IBM HTTP Server

- a. Log in as `root`.
- b. Insert the **Tivoli SecureWay Policy Director Base for AIX and Linux Version 3.8 CD**.
- c. Using **smitty**, select:  
Software Installation and Maintenance ->  
Install and Update Software ->  
Install and Update from LATEST Available Software
- d. Against Input device / directory for software press **F4** and select the CD-ROM – typically `/dev/cd0`.
- e. Against SOFTWARE to install press **F4**. A list of SOFTWARE to install will be displayed.

- f. Move the cursor to **1.3.12.0 HTTP Server Base Run-Time** and press **F7** to select it. Then press **Enter**:

```

Install and Update from LATEST Available Software

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                [Entry Fields]
* INPUT device / directory for software      /dev/cd0                >
* SOFTWARE to install                        [+ 1.3.12.0 HTTP Serve> +
PREVIEW only? (install operation will NOT occur)  no                    +
COMMIT software updates?                      yes                   +
SAVE replaced files?                          no                    +
AUTOMATICALLY install requisite software?      yes                   +
EXTEND file systems if space needed?          yes                   +
OVERWRITE same or newer versions?            no                    +
VERIFY install and check file sizes?          no                    +
Include corresponding LANGUAGE filesets?      yes                   +
DETAILED output?                             no                    +
Process multiple volumes?                    yes                   +

F1=Help          F2=Refresh          F3=Cancel          F4=List
F5=Reset         F6=Command         F7=Edit           F8=Image
F9=Shell        F10=Exit           Enter=Do

```

- g. Press **Enter**. You will be asked if you are sure. Press **Enter** again. The software will be installed. Exit smitty.

- h. By default the IBM HTTP Server listens to port 80, the same as WebSEAL. To avoid port conflicts edit the HTTP configuration file `/usr/HTTPServer/conf/httpd.conf`. Locate the Port value and change it from Port 80 to a different port number – we used Port 81.

- i. Change directory to `/usr/HTTPServer/bin`

- j. Start the server by entering the following command:

```
./apachectl start
```

(If the server is already running first issue `./apachectl stop`, or else issue `ps -ef|grep httpd` to determine the PID and then issue `kill process id` to stop it; then re-attempt to start it.)

- k. If you want the web server to start automatically upon system boot, carry out the following steps:

- change directory to `/etc`
- create a file `rc.http` as follows

```
#!/usr/bin/sh
BINPATH=/usr/HTTPServer/bin
echo 'Starting IBM HTTP Server....'
$BINPATH/apachectl start
```
- Give the system root access to the server file and make it executable:

```
chown root:system rc.http
chmod 0774 rc.http
```

- l. You can verify that the web server is working by pointing a web browser at

`http://hostname:port number` (`http://charon.emea.tivoli.com:81` in our case) – this should result in Index of / being displayed.

## 8.3 Install GSKit

- a. Still using the **Tivoli SecureWay Policy Director Base for AIX and Linux Version 3.8** CD:
- b. Using **smitty**, select:  
Software Installation and Maintenance ->  
Install and Update Software ->  
Install and Update from LATEST Available Software
- c. Against Input device / directory for software press **F4** and select the CD-ROM – typically /dev/cd0.
- d. Against SOFTWARE to install press **F4**. A list of SOFTWARE to install will be displayed.
- e. Move the cursor to **gskit ALL** and press **F7** to select it. Then press **Enter**:

```

Install and Update from LATEST Available Software

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                [Entry Fields]
* INPUT device / directory for software      /dev/cd0
* SOFTWARE to install                        [gskit          > +
PREVIEW only? (install operation will NOT occur)  no          +
COMMIT software updates?                      yes         +
SAVE replaced files?                          no          +
AUTOMATICALLY install requisite software?      yes         +
EXTEND file systems if space needed?           yes         +
OVERWRITE same or newer versions?             no          +
VERIFY install and check file sizes?          no          +
Include corresponding LANGUAGE filesets?      yes         +
DETAILED output?                              no          +
Process multiple volumes?                     yes         +

F1=Help          F2=Refresh          F3=Cancel          F4=List
F5=Reset         F6=Command          F7=Edit            F8=Image
F9=Shell         F10=Exit            Enter=Do

```

- f. Press **Enter**. You will be asked if you are sure. Press **Enter** again. The software will be installed. Exit smitty.

## 8.4 Install IBM Universal Database (DB2)

- a. Still using the **Tivoli SecureWay Policy Director Base for AIX and Linux Version 3.8** CD:
- b. Using **smitty**, select:  
Software Installation and Maintenance ->  
Install and Update Software ->  
Install and Update from LATEST Available Software
- c. Against Input device / directory for software press **F4** and select the CD-ROM – typically /dev/cd0.
- d. Against SOFTWARE to install press **F4**. A list of SOFTWARE to install will be displayed.

e. Move the cursor to each of the following entries and press **F7** to select it:

- **db2\_06\_01.cnvucs**           **ALL**
- **db2\_06\_01.conv**           **ALL**
- **6.1.0.13 DB2 Engine**
- **6.1.0.13 DB2 Run-time Environment**
- **6.1.0.13 License Support for DB2 UDB Enterprise Edition**

f. Then press **Enter**:

```

Install and Update from LATEST Available Software

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                     [Entry Fields]
* INPUT device / directory for software      /dev/cd0          >
* SOFTWARE to install                        [db2_06_01.cnvucs] > +
PREVIEW only? (install operation will NOT occur)  no              +
COMMIT software updates?                     yes             +
SAVE replaced files?                         no              +
AUTOMATICALLY install requisite software?      yes             +
EXTEND file systems if space needed?          yes             +
OVERWRITE same or newer versions?            no              +
VERIFY install and check file sizes?          no              +
Include corresponding LANGUAGE filesets?      yes             +
DETAILED output?                             no              +
Process multiple volumes?                    yes             +

F1=Help          F2=Refresh      F3=Cancel      F4=List
F5=Reset         F6=Command     F7=Edit        F8=Image
F9=Shell         F10=Exit       Enter=Do
    
```

g. Press **Enter**. You will be asked if you are sure. Press **Enter** again. The software will be installed. Exit smitty.

---

## 8.5 Install IBM SecureWay Directory

a. Still using the **Tivoli SecureWay Policy Director Base for AIX and Linux Version 3.8 CD**:

b. Using **smitty**, select:

```

Software Installation and Maintenance ->
Install and Update Software ->
Install and Update from LATEST Available Software
    
```

c. Against Input device / directory for software press **F4** and select the CD-ROM – typically /dev/cd0.

d. Against SOFTWARE to install press **F4**. A list of SOFTWARE to install will be displayed.

e. Move the cursor to each of the following entries and press **F7** to select it:

- **ldap.client**           **ALL**
- **ldap.server**         **ALL**

f. Then press **Enter**:

```

Install and Update from LATEST Available Software

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                     [Entry Fields]
* INPUT device / directory for software      /dev/cd0          >
* SOFTWARE to install                       [ldap.client    > +
PREVIEW only? (install operation will NOT occur)  no              +
COMMIT software updates?                     yes             +
SAVE replaced files?                         no              +
AUTOMATICALLY install requisite software?     yes             +
EXTEND file systems if space needed?         yes             +
OVERWRITE same or newer versions?           no              +
VERIFY install and check file sizes?        no              +
Include corresponding LANGUAGE filesets?     yes             +
DETAILED output?                            no              +
Process multiple volumes?                   yes             +

F1=Help          F2=Refresh      F3=Cancel      F4=List
F5=Reset         F6=Command     F7=Edit       F8=Image
F9=Shell         F10=Exit       Enter=Do

```

g. Press **Enter**. You will be asked if you are sure. Press **Enter** again. The software will be installed. Exit smitty.

h. Also supplied on the CD is eFix 3.2.1-SWD-002 for SecureWay Directory 3.2.1, in directory `/cdrom/usr/sys/inst.images/patches/ldap_efix` (assuming that your CD-ROM device is mounted as `/cdrom`). The file `Readme` in this directory details the problems fixed and the installation procedure. (You may need to define a mount point and type `mount /cdrom` before you can view these files.)

---

## 8.6 Configure LDAP

a. At this point it is strongly suggested that you run `df` to ensure that you have sufficient space in your `/home` directory. The suggested *minimum* is 32 MB (or 65536 512-blocks). If you have insufficient space, you will get a series of failure messages when you attempt to run `ldapcfg`, with very little indication as to the cause of the problem.

b. Issue the following commands to create an appropriate directory for the LDAP instance:

If the `/home` directory does not already exist, create it by issuing `mkdir /home`

```
mkdir /home/ldapdb2
```

```
chmod a+rwx /home/ldapdb2
```

(In a production environment you will want to make permissions less permissive.)

c. Issue the following commands to configure LDAP:

```
ldapcfg -u "cn=root" -p password
```

(where `password` is the LDAP Administrator password – we used `Secure99`)

```
ldapcfg -l /home/ldapdb2
```

```
ldapcfg -s ibmhttp -f /usr/HTTPServer/conf/httpd.conf
```

**d. Restart the IBM HTTP Server:**

```
/usr/HTTPServer/bin/apachectl stop
/usr/HTTPServer/bin/apachectl start
```

**e. The output should look similar to the following:**

```
# mkdir /home/ldapdb2
# chmod a+rwX /home/ldapdb2
# ldapcfg -u "cn=root" -p Secure99
Password for administrator DN cn=root has been set.

IBM SecureWay Directory Configuration complete.
# ldapcfg -l /home/ldapdb2
Creating the directory DB2 default database.
This operation may take a few minutes.

Configuring the database.
Creating database instance: ldapdb2.
Created database instance: ldapdb2.
Starting database manager for instance: ldapdb2.
Started database manager for instance: ldapdb2.
Creating database: ldapdb2.
Created database: ldapdb2.
Updating configuration for database: ldapdb2.
Updated configuration for database: ldapdb2.
Completed configuration of the database.

IBM SecureWay Directory Configuration complete.
# ldapcfg -s ibmhttp -f /usr/HTTPServer/conf/httpd.conf

IBM SecureWay Directory Configuration complete.
The web server must be restarted for changes to take effect.
# /usr/HTTPServer/bin/apachectl stop
/usr/HTTPServer/bin/apachectl stop: httpd stopped
# /usr/HTTPServer/bin/apachectl start
/usr/HTTPServer/bin/apachectl start: httpd started
#
```

**f. Before starting the IBM SecureWay Directory server as root, verify that the user root is in the dbsysadm group. Verify that the file /etc/group contains an entry similar to the following:**

```
dbsysadm:!:400:ldapdb2,root
```

**g. Start the IBM SecureWay Directory Server:**

```
/usr/bin/slapd
```

**h. The output should look similar to the following:**

```
# /usr/bin/slapd
Configuration read securePort 636.
Plugin of type EXTENDEDOP is successfully loaded from libevent.a.
Plugin of type EXTENDEDOP is successfully loaded from libtranext.a.
Plugin of type PREOPERATION is successfully loaded from libDSP.a.
Plugin of type EXTENDEDOP is successfully loaded from libevent.a.
Plugin of type AUDIT is successfully loaded from /lib/libldapaudit.a.
Plugin of type EXTENDEDOP is successfully loaded from libevent.a.
Plugin of type DATABASE is successfully loaded from /lib/libback-rdbm.a.
Non-SSL port initialized to 389.
Local UNIX socket name initialized to /tmp/s.slapd.
#
```

(This step is likely to take several minutes to run.)

**i. To configure the IBM SecureWay Directory server to start automatically upon system boot, add**

the following line to /etc/inittab:

```
ldapd:2:once/usr/bin/slapd >/dev/console 2>&1 #Autostart LDAP/DB2 Services
```

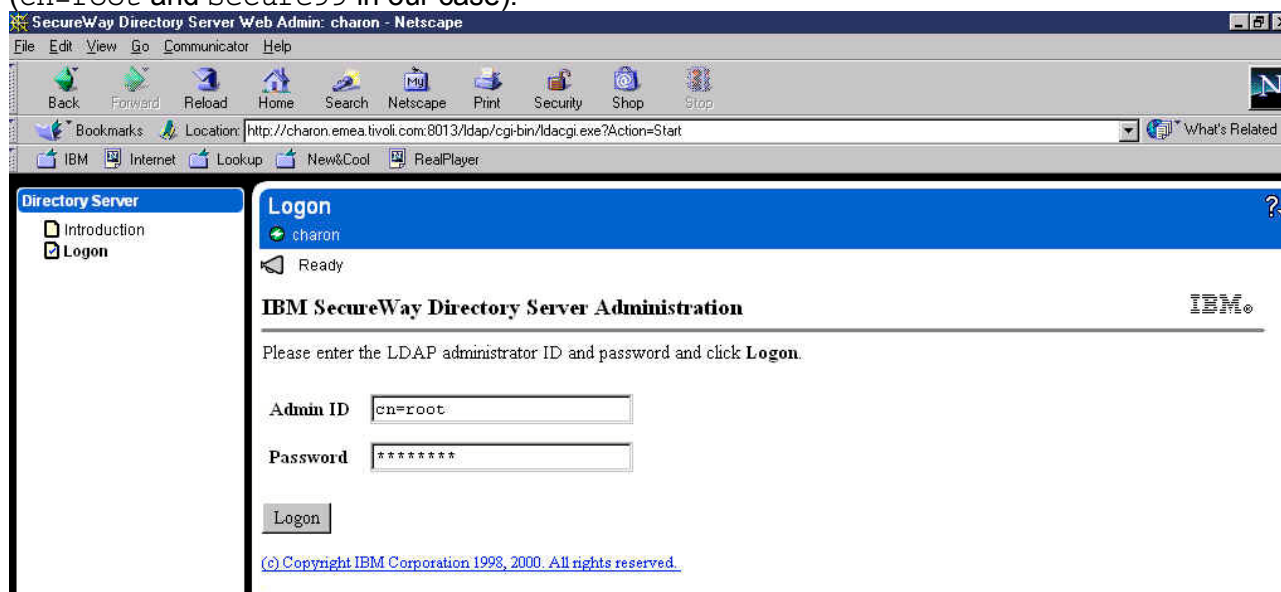
j. To determine whether slapd has started, issue:

```
ps -ef|grep slapd
```

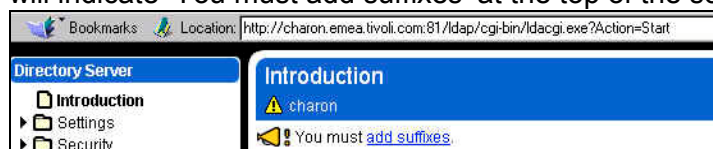
(If slapd is not running, /tmp/slapd.errors might give some further information.)

## 8.7 Add Policy Director Suffixes

a. Point a web browser at `http://hostname:port number/ldap/index.html` (the port number was 81 in our case). The SecureWay Directory Server Logon panel is displayed. Set the User ID to the LDAP Administrator ID and the password to that which was entered previously (cn=root and Secure99 in our case):

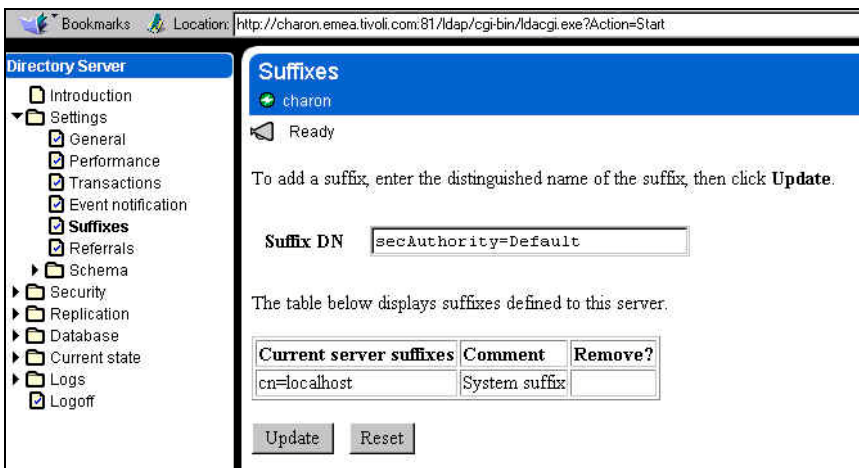


b. Click on 'Logon'. The 'IBM SecureWay Directory Server Administration' panel is displayed. It will indicate 'You must add suffixes' at the top of the screen:



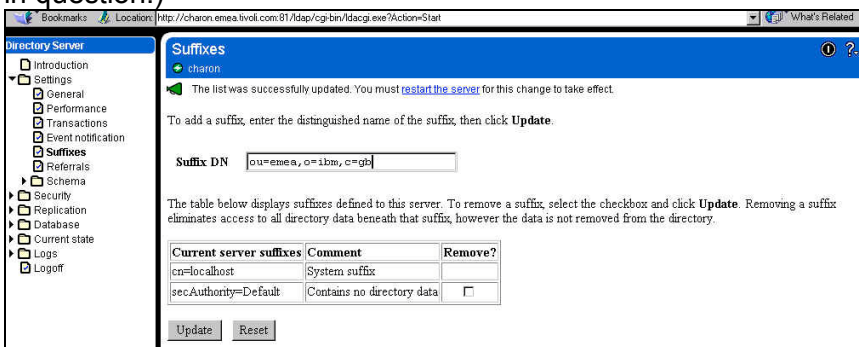
c. Click on 'add suffixes'. Enter `secAuthority=Default` in the 'Suffix DN' box:



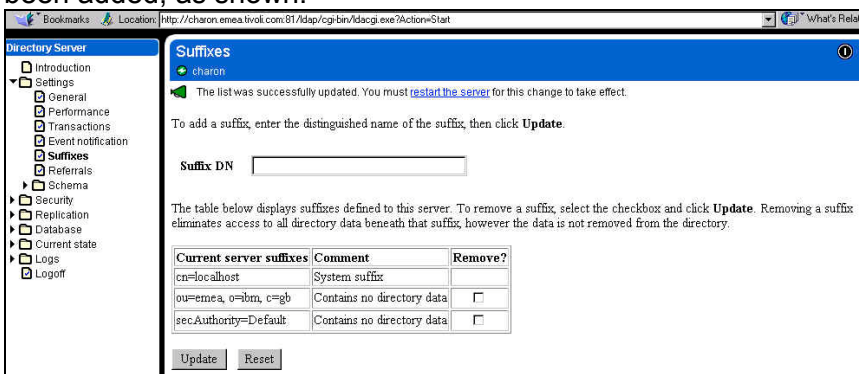


d. Click on 'Update'. The suffix should be added to the list of current server suffixes and a message should be displayed stating 'The suffix was successfully added. You must restart the server for this change to take effect'.

e. Enter a suffix for the Policy Director users and Global Sign-On (GSO) data. For example ou=emea, o=ibm, c=gb as shown below. All the Policy Director resources subsequently defined must sit below the suffix defined here - thus if the country, organization and organizational unit are specified here, all PD resources will have to be held within that organizational unit, whereas if just the country is specified here, all PD resources will merely have to be held within that country. Alternatively it would be possible to specify just a country and organization. Clearly this decision will depend on the directory strategy of the organization in question.)

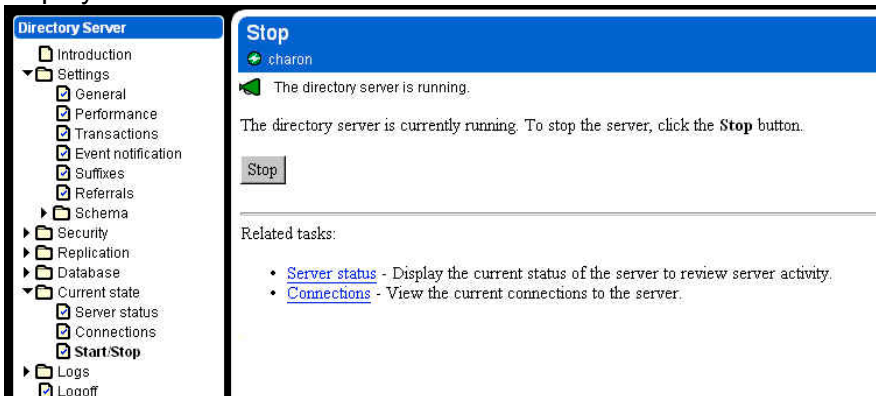


f. Click on 'Update'. A message should be displayed stating 'The list was successfully updated. You must restart the server for this change to take effect', and listing all the suffixes that have been added, as shown:

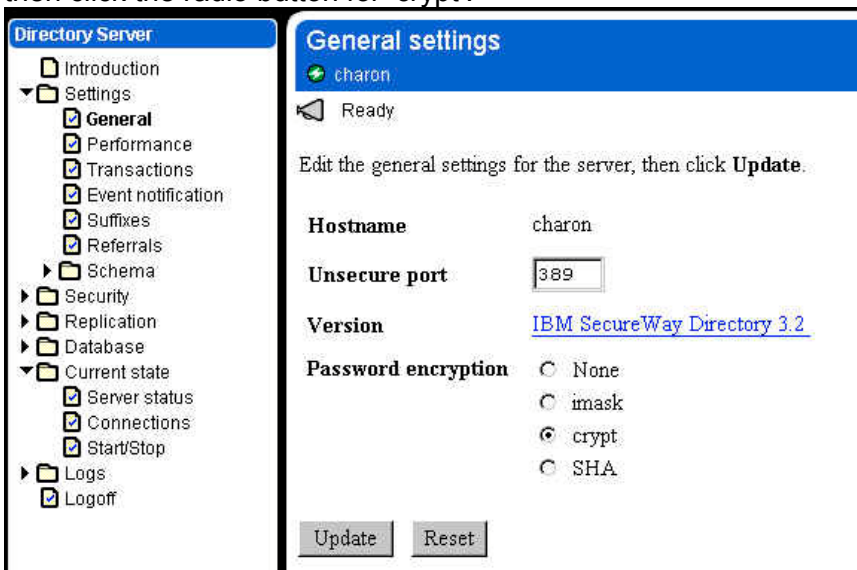


g. Click on the 'restart the server' link at the top of the page. A message stating 'The

directory server is starting' is displayed. This restart process can take several minutes. Once complete a message stating 'The directory server is running' will be displayed:



h. You may wish to specify one-way password encryption. To do this, click on Settings → General, then click the radio button for 'crypt':



i. Then click on 'Update'. It will display a message: 'The changes were successfully updated. You must restart the server for these changes to take effect'. Click on 'restart the server' and wait for the server to restart.

j. The web browser is no longer required and may be closed.

**If you are unable to run the LDAP Administrative web server...**

There have been installations where (for various reasons) it has not been possible to run a web server to perform the LDAP administrative operations. In that case an alternative approach is to edit the configuration file manually. The file in question is:

```
/usr/ldap/etc/slapd32.conf
```

You can add the suffixes we added above by adding the following lines to `slapd32.conf` Beneath the entry `ibm-slapdSuffix: cn=localhost:`

```
Ibm-slapdSuffix: secAuthority=Default
ibm-slapdSuffix: o=ibm, c=gb
```

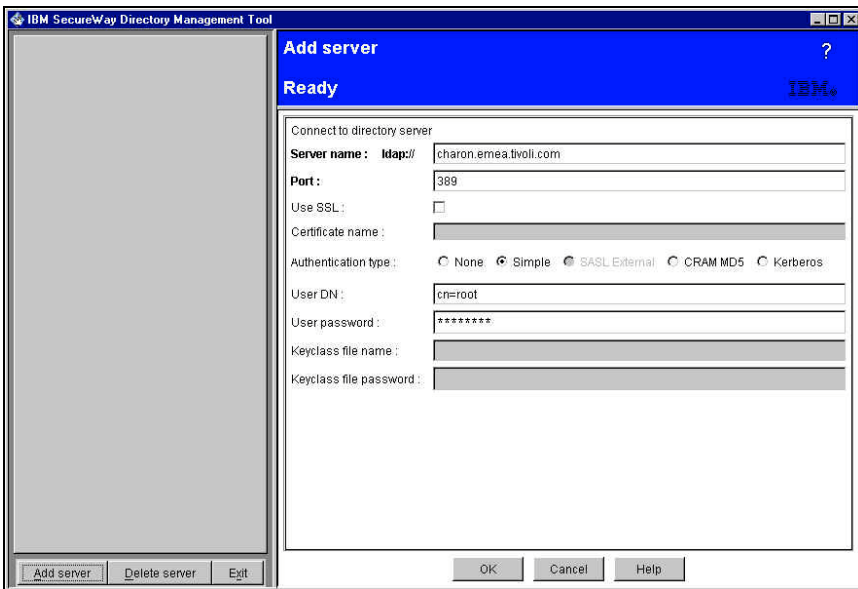
You can specify one-way password encryption by modifying the `ibm-slapdPwEncryption` line to:

```
Ibm-slapdPwEncryption: crypt
```

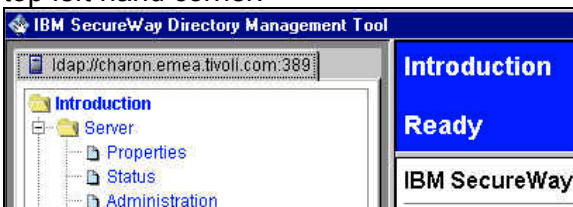
---

## 8.8 Directory Management Tool steps

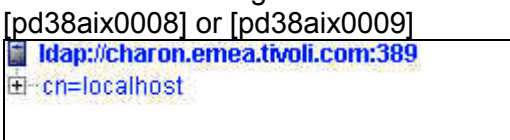
- a. Start the Directory Management Tool. You can do one of the following:
  - run the Directory Management Tool on the same AIX box as that on which the directory is located;
  - run the Directory Management Tool on a remote system and point it at the AIX box on which the directory is located.
- b. To start the Directory Management Tool on an AIX XWindows system, type `dmt` on the AIX command line. To start the Directory Management Tool on a PC, use Start -> Programs -> IBM SecureWay Directory -> Directory Management Tool.
- c. **If you are accessing the directory from a remote system**, as the Directory Management Tool is starting an error message may be displayed indicating ‘An error occurred connecting to server “ldap://localhost:389” – if so, click on ‘OK’ to dismiss the error message.
- d. Click on ‘Add server’ (listed on the bottom left hand corner). An ‘Add Server’ frame is displayed. Enter the Server name, LDAP administrator DN and password (`charon.emea.tivoli.com`, `cn=root` and `Secure99` in our case):



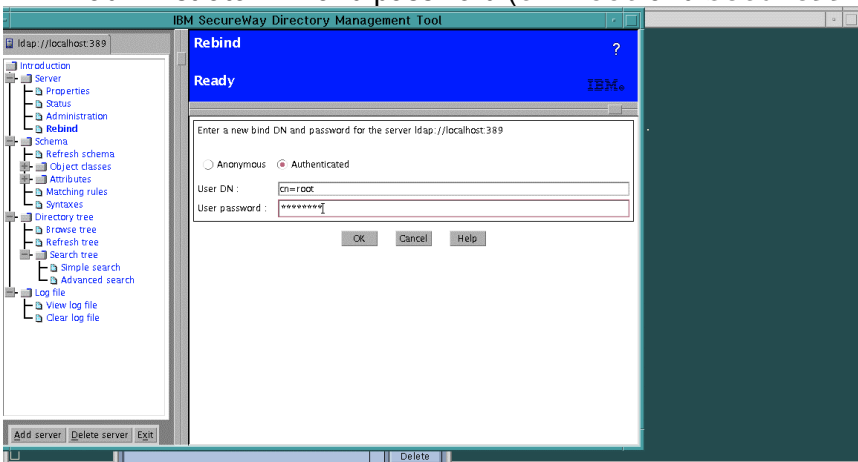
- e. Click on 'OK'. A message panel indicating 'Retrieving server schema. Please wait.' may be displayed. The Directory Management Tool will be re-displayed, showing the hostname in the top left hand corner:



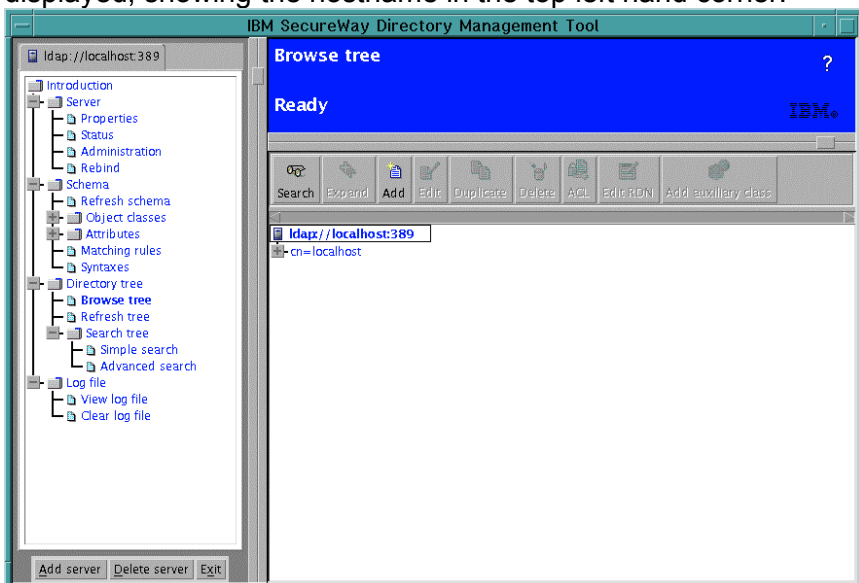
- f. Click on the 'Browse tree' entry, on the left hand panel under the 'Directory tree' node. Message panels indicating that certain entries do not contain any data may be displayed; click on 'OK' to dismiss these dialogues. The 'Browse directory tree' panel will be displayed:



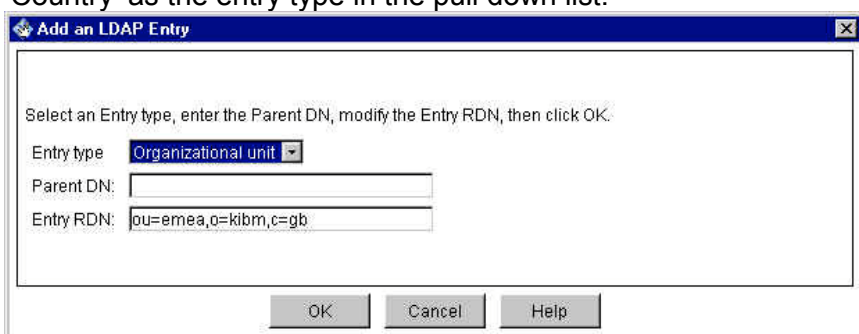
- g. **If you running the Directory Management Tool on the same AIX box as the directory**, click on 'Rebind' (listed under 'Server' in the left hand panel). Click on 'Authenticated' and enter the LDAP administrator DN and password (cn=root and Secure99 in our case):



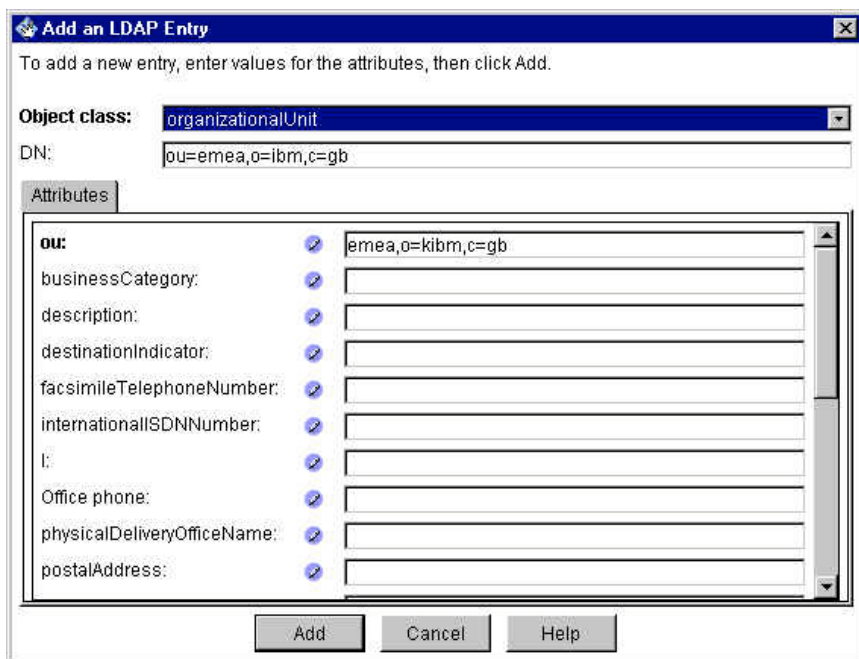
- h. Click on 'OK'. Message panels indicating that certain entries do not contain any data may be displayed; click on 'OK' to dismiss these dialogues. The Directory Management Tool will be re-displayed, showing the hostname in the top left hand corner:



- i. **Click on 'Add' in the upper right hand frame.** An 'Add an LDAP Entry' dialogue is displayed. Against 'Entry RDN', enter the suffix previously entered for the Policy Director users and Global Sign-On (GSO) data (ou=emea, o=ibm, c=gb in our case). If you have specified an organizational unit (as in our case), select 'Organizational unit' as the entry type in the pull down list. If you have specified an organization (such as o=ibm, c=gb), select 'Organization' as the entry type in the pull down list. If you have specified just a country (such as c=gb), select 'Country' as the entry type in the pull down list.



- j. Click on 'OK'. An 'Add an LDAP Entry' panel will be displayed:



k. If desired you can enter a description, etc, then click on 'Add'. Again, a warning indicating 'Entry "secauthority=default" does not contain any data' may be displayed – click on 'OK' to dismiss this. The entry which has just been added will be displayed:



l. The Directory Management Tool is no longer required and can be closed – click on 'Exit' to close it. The LDAP Configuration is now complete.

## 9. Policy Director Server installation (AIX)

- a. Log in as `root`.
- a. Insert the **Tivoli SecureWay Policy Director Base for AIX and Linux Version 3.8** CD.
- b. Using **smitty**, select:
  - Software Installation and Maintenance ->
  - Install and Update Software ->
  - Install and Update from LATEST Available Software
- c. Against Input device / directory for software press **F4** and select the CD-ROM – typically `/dev/cd0`.
- d. Against SOFTWARE to install press **F4**. A list of SOFTWARE to install will be displayed. Move the cursor to **PD ALL** and press **F7** to select it. Then press Enter:

```

Install and Update from LATEST Available Software

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                [Entry Fields]
* INPUT device / directory for software      /dev/cd0
* SOFTWARE to install                        [PD          > +
PREVIEW only? (install operation will NOT occur)  no          +
COMMIT software updates?                      yes         +
SAVE replaced files?                          no          +
AUTOMATICALLY install requisite software?       yes         +
EXTEND file systems if space needed?            yes         +
OVERWRITE same or newer versions?              no          +
VERIFY install and check file sizes?           no          +
Include corresponding LANGUAGE filesets?       yes         +
DETAILED output?                              no          +
Process multiple volumes?                     yes         +

F1=Help          F2=Refresh        F3=Cancel        F4=List
F5=Reset         F6=Command         F7=Edit          F8=Image
F9=Shell         F10=Exit           Enter=Do
  
```

- e. Press **Enter**. You will be asked if you are sure. Press **Enter** again. The software will be installed. Exit **smitty**.

## 10. WebSEAL Installation (AIX)

**Note:** this will install WebSEAL together with any necessary pre-requisite components (namely Policy Director Runtime, GSKit and LDAP Client) if they are not already installed.

- b. Log in as `root`.
- a. Insert the **Tivoli SecureWay Policy Director WebSEAL Version 3.8 CD**.
- b. Using **smitty**, select:
  - Software Installation and Maintenance ->
  - Install and Update Software ->
  - Install and Update from LATEST Available Software
- c. Against Input device / directory for software press **F4** and select the CD-ROM – typically `/dev/cd0`.
- d. Against SOFTWARE to install take the default value `_all_latest`:

```

Install and Update from LATEST Available Software

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

                                [Entry Fields]
* INPUT device / directory for software      /dev/cd0
* SOFTWARE to install                        [_all_latest]
PREVIEW only? (install operation will NOT occur)  no
COMMIT software updates?                      yes
SAVE replaced files?                          no
AUTOMATICALLY install requisite software?       yes
EXTEND file systems if space needed?           yes
OVERWRITE same or newer versions?             no
VERIFY install and check file sizes?          no
Include corresponding LANGUAGE filesets?       yes
DETAILED output?                              no
Process multiple volumes?                     yes

F1=Help      F2=Refresh      F3=Cancel      F4=List
F5=Reset     F6=Command     F7=Edit       F8=Image
F9=Shell     F10=Exit       Enter=Do
    
```

- e. Press **Enter**. You will be asked if you are sure. Press **Enter** again. The software will be installed. Exit `smitty`.



## 11. Policy Director Configuration (AIX)

**Note:** This section describes how to configure all the Policy Director servers together with WebSEAL. The appropriate selection of servers needs to be configured. \*\*\*\*\*

- a. Ensure that the Directory (and any intervening network) is working correctly.
- b. Using smitty, select:  
Communications Applications and Services ->  
Policy Director
- c. You will be presented with the Policy Director Setup Menu. Type 1 (corresponding to Configure Package):

```
Policy Director Setup Menu

    1. Configure Package
    2. Unconfigure Package
    3. Display Configuration Status
    x. Exit

Please select the menu item [x]: 1
```

- d. Press Enter. You will be presented with the Policy Director Configuration Menu. Type 1 (corresponding to Policy Director Runtime (PDRTE) Configuration):

```
Policy Director Configuration Menu

    1. Policy Director Runtime (PDRTE) Configuration
    2. Policy Director Management Server (PDMgr) Configuration
    3. Policy Director Authorization Server (PDAclD) Configuration
    4. Policy Director WebSEAL (PDWeb) Configuration
    x. Return to Policy Director Setup Menu

Please select the menu item [x]: 1
```

- e. Press Enter. When prompted enter the LDAP Server hostname. The output should look similar to the following:

```
Policy Director Configuration Menu

    1. Policy Director Runtime (PDRTE) Configuration
    2. Policy Director Management Server (PDMgr) Configuration
    3. Policy Director Authorization Server (PDAclD) Configuration
    4. Policy Director WebSEAL (PDWeb) Configuration
    x. Return to Policy Director Setup Menu

Please select the menu item [x]: 1

Enter the LDAP server hostname: charon.emea.tivoli.com

Enter the LDAP server port number [389]:
This package has been successfully configured.

Press <enter> to continue ...
```

- f. Press Enter. You will again be presented with the Policy Director Configuration Menu. Type 1 (this time corresponding to Policy Director Management Server (PDMgr) Configuration) and press Enter. When prompted enter the LDAP administrator password (we used `Secure99`), the LDAP DN for the GSO database (we used `ou=emea,o=ibm,c=gb`), and a password for the Policy Director Administrator `sec_master` (we again used `Secure99`). Unless you have configured the LDAP directory for SSL communication answer `n` when asked whether SSL communication is to be enabled between the Policy Director server and the LDAP server. The configuration process can take several minutes. (If desired you can also select 'Enable root CA Certificate download'. This simplifies the distribution of the Root CA Certificate to subsequent Policy Director machines, but may introduce security exposures if the network can be compromised during the configuration step.) The output should look similar to the following:

```
Policy Director Configuration Menu

    1. Policy Director Management Server (PDMgr) Configuration
    2. Policy Director Authorization Server (PDAclD) Configuration
    3. Policy Director WebSEAL (PDWeb) Configuration
    x. Return to Policy Director Setup Menu

Please select the menu item [x]: 1
Enter the LDAP administrative user DN [cn=root]:
Enter the LDAP administrative user password: Secure99
Do you want to enable SSL communication between the
Policy Director server and the LDAP server (y/n) [Yes]? n
Enter the LDAP DN for GSO database: ou=emea,o=ibm,c=gb

You are required to provide a password for the
Policy Director Administrator account.
The administrator login name is sec_master and cannot be changed.

Enter the password for the Policy Director Administrator: Secure99
Re-enter the password for confirmation: Secure99

Enter the SSL server port for PDMgr [7135]:
Enter the PDMgr SSL certificate lifetime [365]:
```

```
Selecting the Enable root CA Certificate download option simplifies the
configuration of the PD Runtime on subsequent machines. Enabling this option
may introduce a security exposure if a non-trusted host can impersonate the
PD Management server in the network.
```

```
Enable root CA Certificate download (y/n) [No]? n
```

```
* Configuring server
```

```
Generating Server Certificates, please wait.
```

```
Creating the SSL certificate. This may take several minutes...
```

```
The Policy Director Manager's SSL configuration has completed successfully.
The Manager's signed SSL certificate is base-64 encoded and saved in text file
/var/PolicyDirector/keytab/pdcacert.b64
```

```
This file is required by the configuration program on each machine in your
secure domain.
```

```
SSL Configuration completed successfully
```

```
* Starting server
```

```
Policy Director Management Server v3.8.0 (Build 010907a)
```

```
Copyright (C) Tivoli Systems 2001
```

```
Copyright (C) IBM Corporation 2001
```

```
Copyright (C) 1994-1999 DASCOS, Inc. All Rights Reserved.
```

```
2001-09-25-10:22:34.244-01:00I----- 0x1354A0A0 pdmgrd NOTICE ivc general ivmgrd.
cpp 638 0x00000001
```

```
Server startup
```

```
2001-09-25-10:22:34.332-01:00I----- 0x1354A0A0 pdmgrd NOTICE ivc general ivmgrd.
cpp 643 0x00000001
```

```
Loading configuration
```

```
This package has been successfully configured.
```

```
Press <enter> to continue ...
```

- g. Press Enter. You will again be presented with the Policy Director Configuration Menu. Type 1 (this time corresponding to Policy Director Authorization Server (PDAcl) Configuration) and press Enter. When prompted enter the LDAP administrator password (we used `Secure99`), and the password for the Policy Director Administrator `sec_master` (we again used `Secure99`). Unless you have configured the LDAP directory for SSL communication answer `n` when asked whether SSL communication is to be enabled between the Policy Director server and the LDAP server. The configuration process can take several minutes. The output should look similar to the following:

```
Policy Director Configuration Menu

    1. Policy Director Authorization Server (PDAcl) Configuration
    2. Policy Director WebSEAL (PDWeb) Configuration
    x. Return to Policy Director Setup Menu

Please select the menu item [x]: 1
Enter the LDAP administrative user DN [cn=root]:
Enter the LDAP administrative user password: Secure99
Do you want to enable SSL communication between the
Policy Director server and the LDAP server (y/n) [Yes]? n
Enter the password for the Policy Director Administrator: Secure99

* Configuring server

Configuration of server ivacl is in progress. This may take several minutes...
SSL configuration has completed successfully for the server.

* Starting server

Policy Director Authorization Server v3.8.0 (Build 010907a)

Copyright (C) Tivoli Systems 2001
Copyright (C) IBM Corporation 2001
Copyright (C) 1994-1999 DASCOS, Inc. All Rights Reserved.

2001-09-25-10:39:54.939-01:00I----- 0x1354A0A0 pdacl NOTICE ivc general ivacl.
cpp 410 0x00000001
Server startup
2001-09-25-10:39:54.978-01:00I----- 0x1354A0A0 pdacl NOTICE ivc general ivacl.
cpp 415 0x00000001
Loading configuration
This package has been successfully configured.

Press <enter> to continue ...
```

- h. Press Enter. You will again be presented with the Policy Director Configuration Menu. Type 1 (this time corresponding to Policy Director WebSEAL (PDWEB) Configuration). Press Enter. When prompted enter the password for the Policy Director Administrator `sec_master` (we used `Secure99`). Unless you have configured the LDAP directory for SSL communication answer 'n' when asked whether SSL communication is to be enabled between the Policy Director server and the LDAP server. The configuration process can take several minutes. The output should look similar to the following:

```
Policy Director Configuration Menu

      1. Policy Director WebSEAL (PDWeb) Configuration
      x. Return to Policy Director Setup Menu

Please select the menu item [x]: 1
Enter the password for the Policy Director Administrator: Secure99
Do you want to enable SSL communication between the
Policy Director server and the LDAP server (y/n) [Yes]? n
Please check Web Server configuration:

1. Enable TCP HTTP?                Yes
2. HTTP Port                       80
3. Enable HTTPS?                   Yes
4. HTTPS Port                      443
5. Web document root directory     /opt/pdweb/www/docs

a. Accept configuration and continue with installation
x. Exit installation

Select item to change: a

* Configuring the Web Server

Configuration of server webseald is in progress.  This may take several minutes.
..

SSL configuration has completed successfully for the server.

* Starting server

Policy Director WebSEAL Version 3.8.0 (Build 010831)

Copyright (C) Tivoli Systems 2001
Copyright (C) IBM Corporation 2000-2001
Copyright (C) 1994-1999 DASC0M, Inc.  All Rights Reserved.

Press <enter> to continue ...
```

- i. Press Enter. You can now check that Policy Director is working by following the steps described in Section Part V - 17 - Initial Policy Director Validation on Page 123 below.

---

## 12. Useful commands for Policy Director in the AIX environment

### LDAP

- a. LDAP can be started from the command line by issuing the command 'slapd'. This should start the associated DB2 processes as well so don't worry about how to start DB2.
- b. You can check if LDAP has started by looking for the slapd process (e.g. `ps -ef | grep "slapd"`)

### PD

- `/etc/iv/iv start` Starts pdmgrd and ivaclld
- `/etc/iv/iv stop` Stops pdmgrd and ivaclld
- `/etc/iv/iv status` Displays status of pdmgrd and ivaclld
- `/etc/iv/pdweb start` Starts webseald
- `/etc/iv/pdweb stop` Stops webseald
- `/etc/iv/pdweb status` Displays status of webseald

### Policy Director Processes

If you type `ps -ef |grep PolicyDirector`, the following processes should be listed: pdmgrd, pdaclld and if you type `ps -ef |grep pdweb` the following process should be listed: webseald.

### AIX

- a. Shutdown `-Fr &` will shutdown and restart AIX immediately as a background task.
- b. `oslevel` will show the version of AIX
- c. `df -k` is useful for showing the state of the file system in 1024 blocks.

## Part IV - Solaris Environment

---

### 13. Solaris System Preparation and general Solaris Notes

- We try to assume a minimum level of Solaris knowledge in these chapters: we have therefore tried to document most steps, but we may not have mentioned every 'Enter' etc.
- Ensure that the date and time are set correctly across the environment you are using - this may avoid problems later on.
- Ensure that you have IP connectivity (for example, attempt to 'ping' another machine).
- The steps described here were documented based on Solaris 8, although we have successfully followed the same procedures on other versions of Solaris.
- Please be aware that the graphical screens shown in these chapters may vary slightly depending on your Solaris environment.
- Note also that file and directory names in Solaris are case sensitive.

---

### 14. Easy Installation Process for Solaris

PD 3.8 now provides a quick installation path using shell scripts for UNIX systems such as Solaris. These scripts make it easy to install Policy Director by automatically installing required software and prerequisites. They let you see what components are currently installed and prompt you for configuration information. Below we will run through a basic install using these scripts.

---

#### 14.1 IBM SecureWay Directory and Prerequisite Installation and Configuration

First we will use the **ezinstall\_idap\_server** script. This sets up a workstation with the following packages; IBM DB2 v6.1 + FP3, GSKit, IBM HTTP Server, IBM SecureWay Directory client and server v3.2.1 together with efix4

- a. Insert the **Tivoli SecureWay Policy Director Base for Solaris and HP-UX Version 3.8** CD.
- b. At the command prompt type the following:

```
# cd /cdrom/cdrom0
# ./ezinstall_ldap_server
```

c. This will check for installed components and show the following list:

```
IBM SecureWay Directory Server 3.2
Installation and Configuration
-----

Product                                Status
IBM DB2 6.1 ..... Not Installed
IBM Global Security Toolkit 4 ..... Not Installed
IBM HTTPD Server ..... Not Installed
IBM SecureWay Directory Client ..... Not Installed
IBM SecureWay Directory Client Languages ... Not Installed
IBM SecureWay Directory Server 3.2 ..... Not Installed

Press ENTER to continue...
```

d. The details show will vary depending on the state of your system. Above you can see the results for a newly installed system.

e. Press **'Enter'**, you will be shown the **'IBM HTTP Server Configuration Options'**

```
IBM HTTP Server Configuration Options
-----

Option                                Value
1. Administration ID ..... root
2. Administration Password ..... *****
3. HTTP Port ..... 80

Enter the Administration Password:
```

f. Enter a password for the Administartor (we used **Secure99**) and press **'Enter'**. You will be shown a summary of the configuration options and be asked if you want to modify them or begin configuration, as shown below:

```
IBM HTTP Server Configuration Options
-----

Option                                Value
1. Administration ID ..... root
2. Administration Password ..... *****
3. HTTP Port ..... 80

Enter the number to modify, or y to begin configuration:
```

g. At this point I selected (3) to change the HTTP listening port from 80 to 81 in our case. In order to avoid port conflicts with WebSEAL later on, which by default listens on port 80. The results of this change are shown below.



```

IBM HTTP Server Configuration Options
-----

Option                               Value
1. Administration ID ..... root
2. Administration Password ..... *****
3. HTTP Port ..... 81

Enter the number to modify, or y to begin configuration:
    
```

h. Type **'y'** and **'Enter'** to begin configuration. Next you are prompted to select the language files that you need for the IBM SecureWay Directory

```

===IBM SecureWay Directory Language Files===

1. [Not Installed] IBMldmde  IBM SecureWay Directory Messages (de_DE)
2. [Not Installed] IBMldmes  IBM SecureWay Directory Messages (es_ES)
3. [Not Installed] IBMldmfr  IBM SecureWay Directory Messages (fr_FR)
4. [Not Installed] IBMldmit  IBM SecureWay Directory Messages (it_IT)
5. [Not Installed] IBMldmja  IBM SecureWay Directory Messages (ja)
6. [Not Installed] IBMldmko  IBM SecureWay Directory Messages (ko)
7. [Not Installed] IBMldmptB IBM SecureWay Directory Messages (pt_BR)
8. [Not Installed] IBMldmzh  IBM SecureWay Directory Messages (zh)
9. [Not Installed] IBMldmzhT IBM SecureWay Directory Messages (zh_TW)

Choose the number of the language files to install.
Then press Y to begin their installation.
Press X to undo the selections and start over.  Y
    
```

i. Select any languages that you need and press **'y'** and **'Enter'** to begin installation. The IBM SecureWay Directory Configuration Options will be displayed:

```

IBM SecureWay Directory Server Configuration Options
-----

IBM SecureWay Directory Server Configuration Options
-----

Option                               Value
1. LDAP Administrator ID (DN) ..... cn=root
2. LDAP Administrator Password ..... *****
3. LDAP Host Name ..... secureway2
4. Suffix ..... Not Specified
5. LDAP Server Port ..... 389
6. LDAP SSL Keyfile ..... /cdrom/pd_hp_solaris_/common/pd_ldapkey.kdb
7. LDAP SSL Key File Password ..... *****
8. SSL Client Certificate Label ..... PDLdap

Enter the LDAP Administrator Password:
    
```

j. Enter the LDAP Administrator password as prompted (we used **Secure99**), then re-enter it for confirmation. You are the prompted to enter the suffix, enter the suffix you need for your LDAP entries, for example we entered **'o=ibm,c-gb'**. You will be shown a summary of the configuration values as below. **Note:** the installation script will add **secAuthority=Default** automatically for you.

```

IBM SecureWay Directory Server Configuration Options
-----
Option                                     Value
1. LDAP Administrator ID (DN) ..... cn=root
2. LDAP Administrator Password ..... *****
3. LDAP Host Name ..... secureway2
4. Suffix ..... o=ibm,c=gb
5. LDAP Server Port ..... 389
6. LDAP SSL Keyfile ..... /cdrom/pd_hp_solaris_/common/pd_ldapkey.kdb
7. LDAP SSL Key File Password ..... *****
8. SSL Client Certificate Label ..... PDLLDAP

Enter the number to modify, or y to begin configuration:
    
```

k. Type 'y' and 'Enter' to begin configuration, you will be informed that the SSL Client Keyfile has been copied. Press 'Enter' to continue, a summary is shown and the install continues with DB2. Eventually after about 10-15 minutes this phase will complete and you should see the screen below saying that the installation and configuration is complete.

```

IBM SecureWay Directory Server 3.2
Installation and Configuration
-----

Product                                     Status
IBM DB2 6.1 ..... Configured [6.1.0.13]
IBM Global Security Toolkit 4 ..... Configured [4.0.3.168]
IBM HTTPD Server ..... Configured [1.3.12.0]
IBM SecureWay Directory Client ..... Configured [3.2.1.0]
IBM SecureWay Directory Client Languages ... Not Installed
IBM SecureWay Directory Server 3.2 ..... Configured [3.2.1.0]

IBM SecureWay Directory Server 3.2
Installation and Configuration is complete.
    
```

l. This completes the Directory and requisite installation.

## 14.2 Policy Director RTE and Mgr Installation and Configuration

Use the **ezinstall\_pdmgr** script to install the PDRTE and PDMgr components. This sets up a workstation with the following packages; GSKit, IBM SecureWay Directory client v3.2.1, PDRTE and PDMgr.

- a. Insert the **Tivoli SecureWay Policy Director Base for Solaris and HP-UX Version 3.8 CD**.
- b. At the command prompt type the following:

```

# cd /cdrom/cdrom0
# ./ezinstall_pdmgr
    
```

- c. This will check for installed components and show the following list:

```

Tivoli SecureWay Policy Director Management Server
    
```

Installation and Configuration

```
-----
Product                               Status
IBM Global Security Toolkit 4 ..... Configured [4.0.3.168]
IBM SecureWay Directory Client ..... Configured [3.2.1.0]
IBM SecureWay Directory Client Languages .... Not Installed
Tivoli SecureWay Policy Director Runtime..... Not Installed
Tivoli SecureWay PD Management Server ..... Not Installed

Press ENTER to continue...
```

- d. The script will check to see the status of the components it is designed to install and configure. As you can see above in our case GSKit and the Directory client were already installed by the previous script (ezinstall\_ldap\_server).
- e. Press **'Enter'** to continue. The list of SecureWay Directory client language files are presented. Select any that you need and type **'y'** and **'Enter'** to continue.
- f. The Policy Director Runtime Configuration options are displayed as shown below

Tivoli SecureWay Policy Director Runtime Configuration Options

```
-----
Option                               Value
1. Configure Using This Registry Type ..... ldap
2. LDAP Server Hostname ..... Not Specified
3. LDAP Server Port ..... 389
```

Enter the LDAP Server Hostname:

- g. Enter the fully qualified LDAP Server hostname as prompted (in our case secureway2.pisc.uk.ibm.com) and press **'Enter'**

Tivoli SecureWay Policy Director Runtime Configuration Options

```
-----
Option                               Value
1. Configure Using This Registry Type ..... ldap
2. LDAP Server Hostname ..... secureway2.pisc.uk.ibm.com
3. LDAP Server Port ..... 389
```

Enter the number to modify, or y to begin configuration:

- h. The options are updated with the name you entered. Press **'y'** and **'Enter'** to begin the configuration.

Tivoli SecureWay Policy Director Management Server Configuration Options

```
-----
Option                               Value
1. LDAP Server Hostname ..... secureway2.pisc.uk.ibm.com
2. LDAP Administrator ID (DN) ..... cn=root
```

```

3. LDAP Administrator Password ..... *****
4. Security Master Password ..... *****
5. Enable SSL between PD and LDAP ..... Not Specified
6. LDAP SSL Client Key File ..... Not Specified
7. SSL Client Certificate Label .....
8. SSL Keyfile Password ..... *****
9. LDAP Server SSL Port ..... 636
10. LDAP DN for GSO Database ..... Not Specified
11. SSL Server Port for PD Management Server.. 7135
12. PDMGR SSL Certificate Lifetime ..... 365
13. Enable Download of Certificates ..... Not Specified
    
```

Enable SSL with LDAP Server? [Y|N]:

- i. The screen above is displayed showing a number of options and you are prompted for configuration information. Each time the screen above is updated with the values
- j. First decide if you want to enable SSL with the LDAP server. We choose no and typed 'n' and 'Enter'.
- k. You are then prompted for the LDAP Administrator Password (**Secure99** in our case)
- l. You are then prompted for the Security Master Password (**Secure99** in our case) and asked to reconfirm it.
- m. You are prompted to enter the LDAP DN for the GSO database (o=ibm,c=gb in our case)
- n. You are asked if you want other PD Client machines to download the certificate file (a new feature in 3.8) we answered 'n'. The summary below is now displayed.

Tivoli SecureWay Policy Director Management Server Configuration Options  
 -----

Option	Value
1. LDAP Server Hostname .....	secureway2.pisc.uk.ibm.com
2. LDAP Administrator ID (DN) .....	cn=root
3. LDAP Administrator Password .....	*****
4. Security Master Password .....	*****
5. Enable SSL between PD and LDAP .....	N
6. LDAP SSL Client Key File .....	Not Specified
7. SSL Client Certificate Label .....	
8. SSL Keyfile Password .....	*****
9. LDAP Server SSL Port .....	636
10. LDAP DN for GSO Database .....	o=ibm,c=gb
11. SSL Server Port for PD Management Server..	7135
12. PDMGR SSL Certificate Lifetime .....	365
13. Enable Download of Certificates .....	N

Enter the number to modify, or y to begin configuration:

- o. This completes the mandatory information, you now have the chance to make further changes and the begin the configuration.
- p. Press 'y' and 'Enter' to start the configuration. Files will be installed and configured and after a few minutes you will see that the installation and configuration is complete as shown below.

```

Tivoli SecureWay Policy Director Management Server
Installation and Configuration
-----

Product                                Status
IBM Global Security Toolkit 4 ..... Configured [4.0.3.168]
IBM SecureWay Directory Client ..... Configured [3.2.1.0]
IBM SecureWay Directory Client Languages .... Not Installed
Tivoli SecureWay Policy Director Runtime..... Configured [Version 3 , Revision 8]
Tivoli SecureWay PD Management Server ..... Configured [Version 3 , Revision 8]

Tivoli SecureWay Policy Director Management Server
Installation and Configuration is complete.
    
```

q. This completes the **ezinstall\_pdmgr** script. The Policy Director management server should now be installed and working. You can test this out by making use of the 'pdadmin' interface to administer PD.

## 14.3 WebSEAL Install and Configuration

Use the **ezinstall\_pdweb** script to install WebSEAL. This sets up a workstation with the following packages; GSKit, IBM SecureWay Directory client v3.2.1, PDRTE and WebSEAL.

- a. Insert the **Tivoli SecureWay Policy Director WebSEAL Version 3.8 CD**.
- b. At the command prompt type the following:

```

# cd /cdrom/cdrom0
# ./ezinstall_pdweb
    
```

c. This will check for installed components and show the following list:

```

Policy Director WebSEAL Server
Installation and Configuration
-----

Product                                Status
IBM Global Security Toolkit 4 ..... Configured [4.0.3.168]
IBM SecureWay Directory Client ..... Configured [3.2.1.0]
IBM SecureWay Directory Client Languages .... Not Available
Tivoli SecureWay Policy Director Runtime..... Configured [Version 3 , Revision 8]
Policy Director WebSEAL Server ..... Not Installed

Press ENTER to continue...
    
```

d. Press **'Enter'** to continue and you will see the configuration screen below.

```

IBM HTTP Server Configuration Options
-----

Option                                Value
1. Security Master Password ..... *****
2. Enable SSL between PD and LDAP ..... Not Specified
3. LDAP SSL Client Key File ..... Not Specified
4. LDAP SSL Key File Password ..... *****
5. SSL Client Certificate Label .....
6. SSL Server Port ..... 636
    
```

Enable SSL between PD and LDAP on Domino? (Y|N) :

- e. You are asked if you want to enable SSL between PD and LDAP (we choose 'n')
- f. You are asked for the Security Master password (**Secure99** in our case)
- g. You are then shown a summary of the configuration information and asked if you want to begin configuration. Press 'y' the 'Enter' and the components are installed and configured.

```
Policy Director WebSEAL Server
Installation and Configuration
-----
Product                               Status
IBM Global Security Toolkit 4 ..... Configured [4.0.3.168]
IBM SecureWay Directory Client ..... Configured [3.2.1.0]
IBM SecureWay Directory Client Languages .... Not Available
Tivoli SecureWay Policy Director Runtime..... Configured [Version 3 , Revision 8]
Policy Director WebSEAL Server ..... Configured [3.8.0]

Policy Director WebSEAL Server
Installation and Configuration is complete.
```

- h. WebSEAL should now be installed and configured.
- i. You can test that WebSEAL is running by pointing a browser at <https://hostname>, you should be prompted to authenticate with a username and password. At this stage you should be able to authenticate with the sec\_master account and password.

---

## 15. Policy Director Component Configuration & Unconfiguration (Solaris)

If you need to manually configure or unconfigure any of the PD components (ie, PDRTE, PDMgr, WebSEAL) then you can use the pdconfig tool.

- a. Change to the /opt/PolicyDirector/bin directory and run 'pdconfig', i.e.

```
# cd /opt/PolicyDirector/bin
# pdconfig
```

- b. You will be presented with the Policy Director Setup Menu as shown below. Follow the menu options you require.

```
Policy Director Setup Menu

    1. Configure Package
    2. Unconfigure Package
    3. Display Configuration Status
    x. Exit

Please select the menu item [x]:
```

---

## 16. Useful commands for Policy Director in the Solaris environment

### LDAP

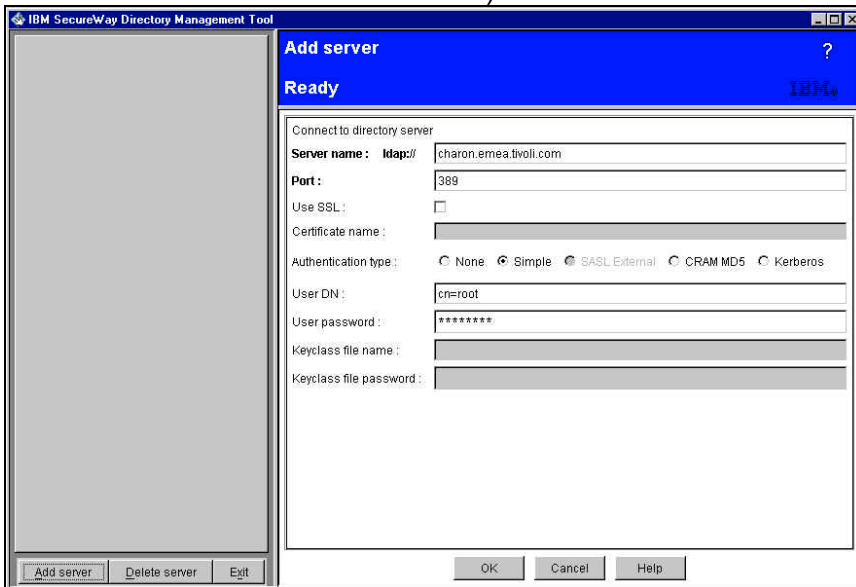
- a. LDAP can be started from the command line by issuing the command 'slapd'. This should start the associated DB2 processes as well so don't worry about how to start DB2.
- b. You can check if LDAP has started by looking for the slapd process (e.g. ps -ef | grep "slapd")

### Directory Management Tool steps

- a. Start the Directory Management Tool. You can do one of the following:
- run the Directory Management Tool on the same AIX box as that on which the directory is located;
  - run the Directory Management Tool on a remote system and point it at the AIX box on which the directory is located.
- b. To start the Directory Management Tool on a Solaris XWindows system, type `dmt&` at the command line.
- c. **If you are accessing the directory from a remote system**, as the Directory Management Tool

is starting an error message may be displayed indicating ‘An error occurred connecting to server “ldap://localhost:389” – if so, click on ‘OK’ to dismiss the error message.

- d. Click on ‘Add server’ (listed on the bottom left hand corner). An ‘Add Server’ frame is displayed. Enter the Server name, LDAP administrator DN and password (charon.emea.tivoli.com, **cn=root** and **Secure99** in our case):



## PD

- `/etc/iv start` Starts the PD Servers
- `/etc/iv stop` Stops the PD Servers
- `/etc/iv status` Displays status of PD Servers
- `/etc/pdweb start` Starts WebSEAL
- `/etc/pdweb stop` Stops WebSEAL
- `/etc/pdweb status` Displays status of WebSEAL

## Solaris

- **reboot** will shutdown and restart Solaris immediately as a background task.
- **eject** will eject the CD



---

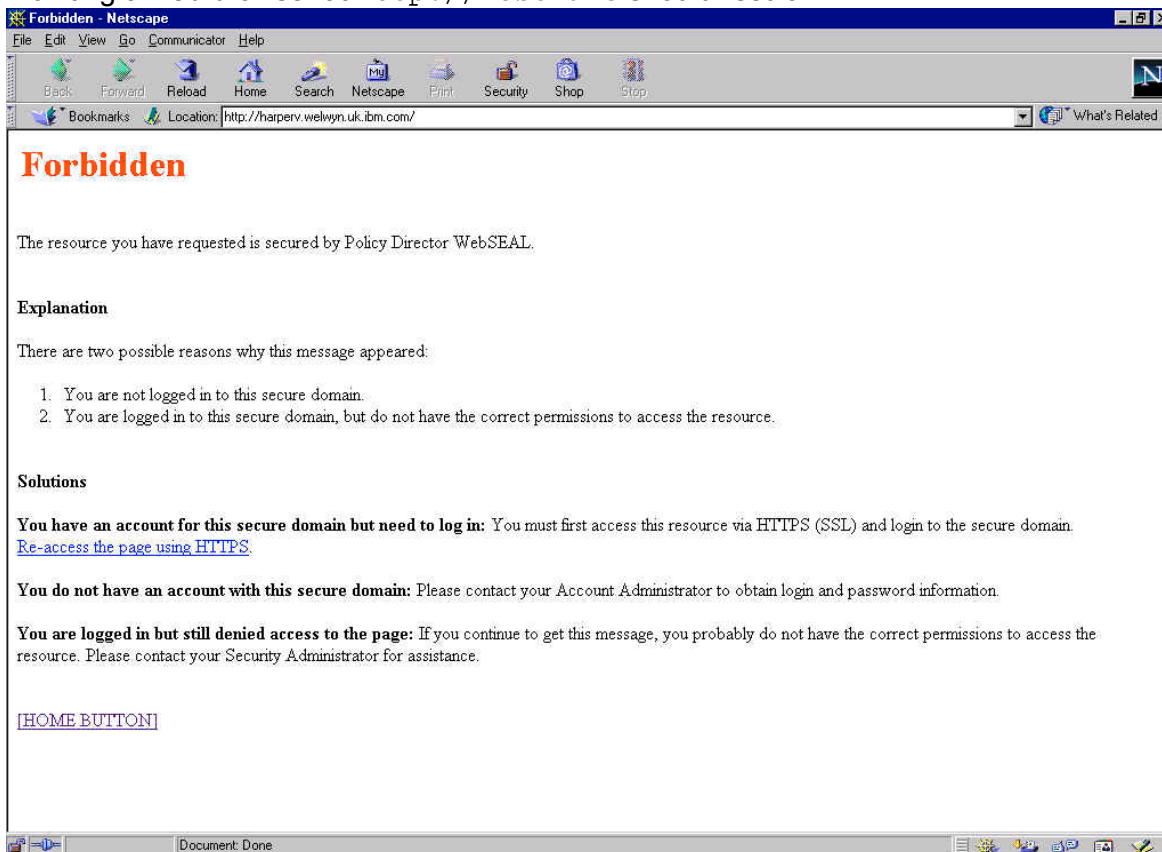
## Part V - Generic Product Configuration

---

### 17. Initial Policy Director Validation

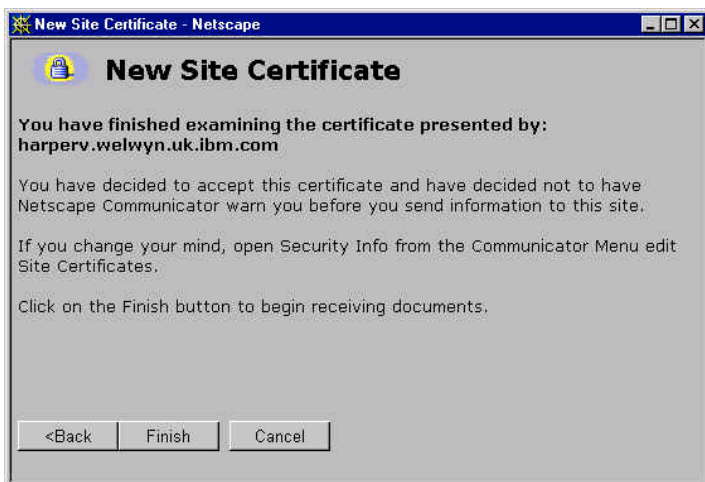
---

a. Pointing a web browser at `http://hostname` should result in:



b. Click on the link Re-access the page using HTTPS, or else point a web browser at `https://hostname`. You can then ignore the web browser error messages (because the WebSEAL Server Certificate has not been signed by a recognized Certification Authority and the name in it does not match the WebSEAL domain name):





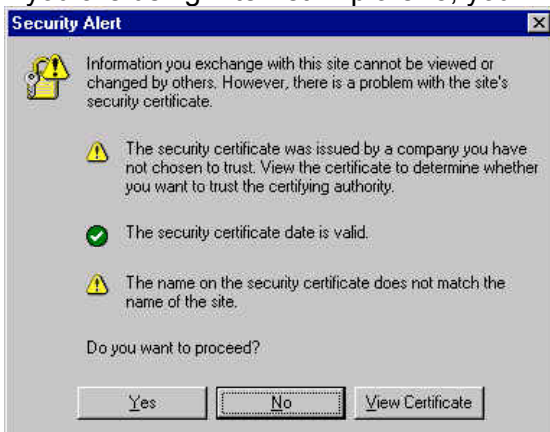
c. You can then log in to the browser Basic Authentication prompt with User Name `sec_master` and the Policy Director Administrator password (`secure99` in our case):



- d. (Note that the User Name is not case sensitive, but the Password *is* case sensitive.)
- e. Click on 'OK' – you should then be presented with the Policy Director splash screen. (The padlock in the bottom left hand corner of the screen in the locked position indicates that SSL is established.)



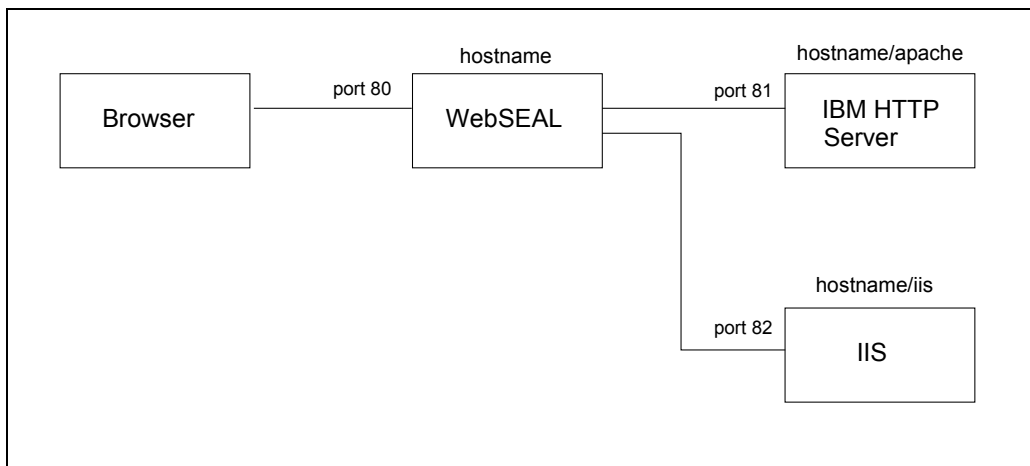
- f. If you are using Internet Explorer 5, you will get panels similar to the following:





## 18. Further Policy Director Configuration

In order to set up a demonstration configuration similar to this, perform the following steps. (The examples featured here use Netscape Communicator, IBM HTTP Server and IIS; using other browsers and web servers should give similar results.)



- a. Set up a web server to listen on port 81 - for example, during the LDAP installation IBM HTTP Server was installed and we edited `\Program Files\IBM HTTP Server\conf\httpd.conf` to change the `Port` directive from 80 to 81 (or some other value).

If you are using Microsoft Internet Information Server (IIS), the only way we have found of changing its port number is to do the following:

- a) Use Start -> Settings -> Control Panel -> Services to stop Policy Director WebSEAL (as this is listening on port 80).
  - b) Use Start -> Programs -> Microsoft Internet Server (Common) -> Internet Service Manager to start Microsoft Internet Service Manager.
  - c) Click on Properties -> Start Service in Internet Service Manager to start IIS (which by default will listen on port 80).
  - d) Double-click on the computer name (on the same line as the reference to 'WWW'). This displays the 'WWW Service Properties' dialogue, including a 'TCP Port' field which you can change (to, say, 82). Click on 'OK'.
  - e) In Internet Service Manager, click on Properties -> Stop Service to stop IIS.
  - f) Click on Properties -> Start Service to re-start IIS.
- b. Verify that pointing the browser at `http://hostname:80/` results in the WebSEAL responding with a Policy Director banner as before.
  - c. Verify that pointing the browser at `http://hostname:81/` and/or `http://hostname:82/` results in the other web server(s) responding.
  - d. Ensure that the LDAP Server is started.
  - e. You can use the `pdadmin` command line interface to create a user as follows:

```
# pdadmin -a sec_master -p Secure99
pdadmin> user create usera cn=usera,ou=emea,o=ibm,c=gb usera usera passw0rd
pdadmin> user modify usera account-valid yes
pdadmin> user show usera
Login ID: usera
LDAP DN: cn=usera,ou=emea,o=ibm,c=gb
LDAP CN: usera
LDAP SN: usera
Description:
Is SecUser: yes
Is GSO user: no
Account valid: yes
Password valid: yes
Authorization mechanism: Default:LDAP
pdadmin>
```

- f. Note that the relevant elements of the DN (ou=emea, o=ibm, c=gb in our case) must be consistent with the suffixes previously specified.

The password must be consistent with the password rules - passw0rd and password1 are consistent with the default password rules, which require at least one numeric character.

- g. You can show the characteristics of the WebSEAL server(s) as follows:

```
pdadmin> server list
webseald-harperv
ivaclld-harperv.welwyn.uk.ibm.com
pdadmin> server show webseald-harperv
webseald-harperv
Description: webseald/harperv
Hostname: harperv.welwyn.uk.ibm.com
Principal: webseald/harperv
Port: 7237
Listening for authorization database update notifications: yes
AZN Administration Services:
webseal-admin-svc
azn_admin_svc_trace
pdadmin>
```

- h. You can set up a smart junction as follows:

```
pdadmin> server task webseald-harperv create -t tcp -h harperv.welwyn.uk.ibm.com
-p 81 -i -w /apache
Created junction at /apache
pdadmin>
```

- i. **Note:** as we are junctioning a windows-based web server, we specify the -i and -w switches to treat URLs as case-insensitive and handle 8.3 format file names correctly.

- j. Note also that an error message will be displayed if the junctioned web server is not operating.

- k. The junctions and the characteristics of the junctions can be listed as follows: [pd38nt2.op]

```
pdadmin> server task webseald-harperv list
/
/apache
pdadmin> server task webseald-harperv show /apache
Junction point: /apache
Type: TCP
```

```

Junction hard limit: 0 - using global value
Junction soft limit: 0 - using global value
Active worker threads: 0
Basic authentication mode: filter
Authentication HTTP header: do not insert
Stateful junction: no
Scripting support: no
Delegation support: no
Mutually authenticated: no
    Insert WebSphere LTPA cookies: no
Insert WebSEAL session cookies: no
Server 1:
    ID: bfb75898-a845-11d5-adc6-204c4f4f5020
    Server State: running
    Hostname: harperv.welwyn.uk.ibm.com
    Port: 81
    Virtual hostname: harperv.welwyn.uk.ibm.com:81
    Server DN:
    Query_contents URL: /cgi-bin/query_contents
    Query-contents: unknown
    Case insensitive URLs: yes
    Allow Windows-style URLs: no
    Total requests : 1
pdadmin>

```

I. A second junction can be added and verified as follows:

```

pdadmin> server task webseald-harperv create -t tcp -h harperv.welwyn.uk.ibm.com
-p 82 -i -w -q /cgi-bin/query_contents.exe /iis
Created junction at /iis
pdadmin> server task webseald-harperv list
/
/apache
/iis
pdadmin> server task webseald-harperv show /iis
Junction point: /iis
Type: TCP
Junction hard limit: 0 - using global value
Junction soft limit: 0 - using global value
Active worker threads: 0
Basic authentication mode: filter
Authentication HTTP header: do not insert
Stateful junction: no
Scripting support: no
Delegation support: no
Mutually authenticated: no
    Insert WebSphere LTPA cookies: no
Insert WebSEAL session cookies: no
Server 1:
    ID: d1728480-a84b-11d5-adc6-204c4f4f5020
    Server State: running
    Hostname: harperv.welwyn.uk.ibm.com
    Port: 82
    Virtual hostname: harperv.welwyn.uk.ibm.com:82
    Server DN:
    Query_contents URL: /cgi-bin/query_contents.exe
    Query-contents: unknown
    Case insensitive URLs: yes
    Allow Windows-style URLs: no
    Total requests : 1
pdadmin>

```

m. **Note:** when using query\_contents with IIS, you need to specify -q /cgi-



bin/query\_contents.exe when creating the junction.

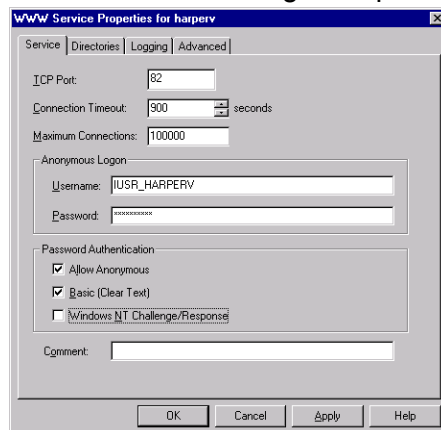
- n. Verify that pointing the web browser to the junctioned url works - for example pointing the browser at https://harperv.welwyn.uk.ibm.com/apache should result in the same web page being displayed as pointing the browser at http://harperv.welwyn.uk.ibm.com:81.
- o. Set up query\_contents on the junctioned web server - this is to enable the Policy Director Web Portal Manager to be used for managing web server contents.

For IBM HTTP Server, do the following:

- a) In httpd.conf, uncomment the line ScriptAlias /cgi-bin/ "C:/Program Files/IBM HTTP Server/cgi-bin/".
- b) Copy query\_contents.exe from C:\Program Files\Tivoli\PDWeb\www\lib\query\_contents to C:\Program Files\IBM HTTP Server\cgi-bin (or whatever other directory ScriptAlias /cgi-bin/ points to).
- c) Copy query\_contents.cfg from C:\Program Files\Tivoli\PDWeb\www\lib\query\_contents to C:\Winnt.
- d) Edit C:\Winnt\query\_contents.cfg, so that the docroot line points to whatever subdirectory the DocumentRoot line in httpd.conf points to.
- e) Stop and re-start IBM HTTP Server.

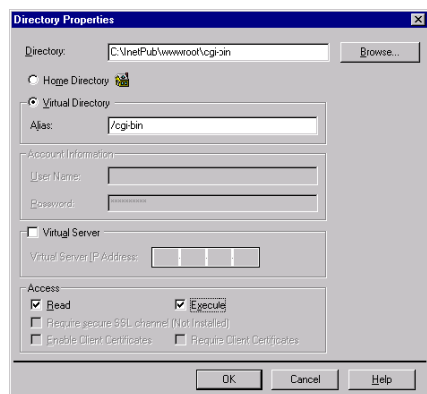
p. For IIS do the following:

- a) Create a cgi-bin directory: md c:\inetpub\wwwroot\cgi-bin
- b) Use Start -> Programs -> Microsoft Internet Server (Common) -> Internet Service Manager to start Microsoft Internet Service Manager.
- c) Double-click on the computer name (on the same line as the reference to 'WWW'). This displays the 'WWW Service Properties' dialogue, including a 'TCP Port' field which you can change (to, say, 82).
- d) Select the 'Allow Anonymous' and 'Basic (Clear Text)' boxes and deselect the 'Windows NT Challenge/Response' box.

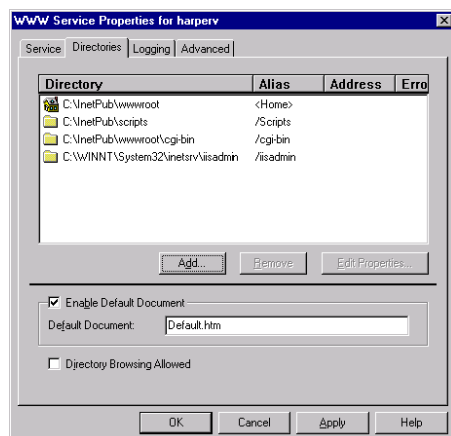


- e) Click on the 'Directories' tab.
- f) Pull the Alias column to the right so that you can see the full path name.
- g) Click on 'Add'.
- h) Set 'Directory' to C:\inetpub\wwwroot\cgi-bin
- i) Set Virtual Directory Alias to /cgi-bin

j) Select the Access - 'Read' and 'Execute' boxes :



k) Click on 'OK':



l) Click on 'OK'.

m) Click on Properties -> Stop Service in Internet Service Manager to stop IIS.

n) Click on Properties -> Start Service to re-start IIS.

o) Ideally obtain a copy of query\_contents.exe written specifically to cope with the virtual directories which IIS and Netscape support.

copy query\_contents.exe to c:\inetpub\wwwroot\cgi-bin\.

copy query\_contents.cfg to c:\winnt\.;

edit query\_contents.cfg to contain the following:

```
[server]
docroot=C:\inetpub\wwwroot

[directories]
/iisadmin=c:\winnt\system32\inetrv\iisadmin
```

p) Failing that, copy the WebSEAL query\_contents.\* files from the Policy Director directory to the appropriate directories:

copy c:\Program Files\Tivoli\PDWeb\www\lib\query\_contents\query\_contents.exe  
to c:\inetpub\wwwroot\cgi-bin\.

copy c:\Program Files\Tivoli\PDWeb\www\lib\query\_contents\query\_contents.cfg  
to c:\winnt\.;

edit c:\winnt\query\_contents.cfg to specify  
docroot=c:\inetpub\wwwroot

q. Test `query_contents.exe` from a DOS window:

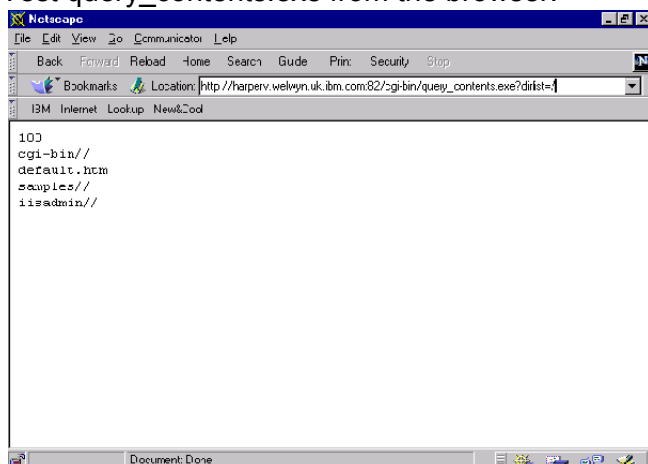
```
C:\>c:\inetpub\wwwroot\cgi-bin\query_contents.exe dirlist=/
Content-type: text/plain

100
cgi-bin//
default.htm
samples//
iisadmin//

C:\>
```

(The line containing `iisadmin` will not be present when using the default `query_contents.exe`.)

r. Test `query_contents.exe` from the browser:



(Again, the line containing `iisadmin` will not be present when using the default `query_contents.exe`.)

s. **Note:** when using `query_contents` with IIS, you need to specify `-q /cgi-bin/query_contents.exe` on the `junctioncp create` command.

## Directory Management Tool

You can verify the existence of the user account created in the previous section by following the following steps:

- Type `dmt` on the command line to start the Directory Management Tool.
- Either click on `Add Server`, then enter the server name, the LDAP Administrator User DN and password, or else click on `Rebind`, click on `Authenticated`, and enter the LDAP Administrator User DN and password (`cn=root`, `Secure99` in our case).
- Click on `Directory tree` -> `Browse tree`.
- Click on the '+' sign beside your organization entry (`ou=emea,o=ibm,c=gb` in our case).
- The user should be listed (`cn=testuser` in our case).

---

## 19. Query\_contents – additional notes

### *Query\_contents with Lotus Domino Go Webserver*

As the book says, copy `/usr/lpp/IV/www/lib/query_contents.sh` to the `cgi-bin` directory of the web server. For Lotus Domino Go this is `/usr/lpp/internet/server_root/cgi-bin`. Remove the `.sh` extension. You can test the script is working correctly by issuing `http://server/cgi-bin/query_contents?dirlist=/`. You should get 100 followed by a listing of the webserver's document-root directory.

For Lotus Domino Go you need to add the lines in bold to `query_contents`:

```
CERN*)
  DOCROOTDIR=/home/www/Web
  ADD_TO_ROOT="cgi-bin/"
  ;;
Domino-Go-Webserver*)
  DOCROOTDIR=`pwd`/..pub
  ADD_TO_ROOT="cgi-bin/"
  ;;
```

### *Query\_contents with Netscape Enterprise Server under AIX*

Set the default `DOCROOTDIR` definition to `/opt/netscape/suitespot/docs` or `/pkg/netscape/suitespot/docs`.

Note: if you want to test `query_contents` from the command line under AIX, you cannot supply a parameter to it directly. Instead, you need to set the environment variable `QUERY_STRING`. For example, type the following at a command prompt:

```
export QUERY_STRING="dirlist=/"
./query_contents
```

---

## 20. Setting up a WebSEAL server certificate

If you use the default WebSEAL server certificate, when you set up an SSL session to WebSEAL you will get browser warnings indicating that (a) the browser does not recognize the authority who signed the site's certificate, and (b) the certificate that the site has presented does not contain the correct site name ("Certificate Name Check"). (The exact messages displayed will depend on the web browser which you are using.)

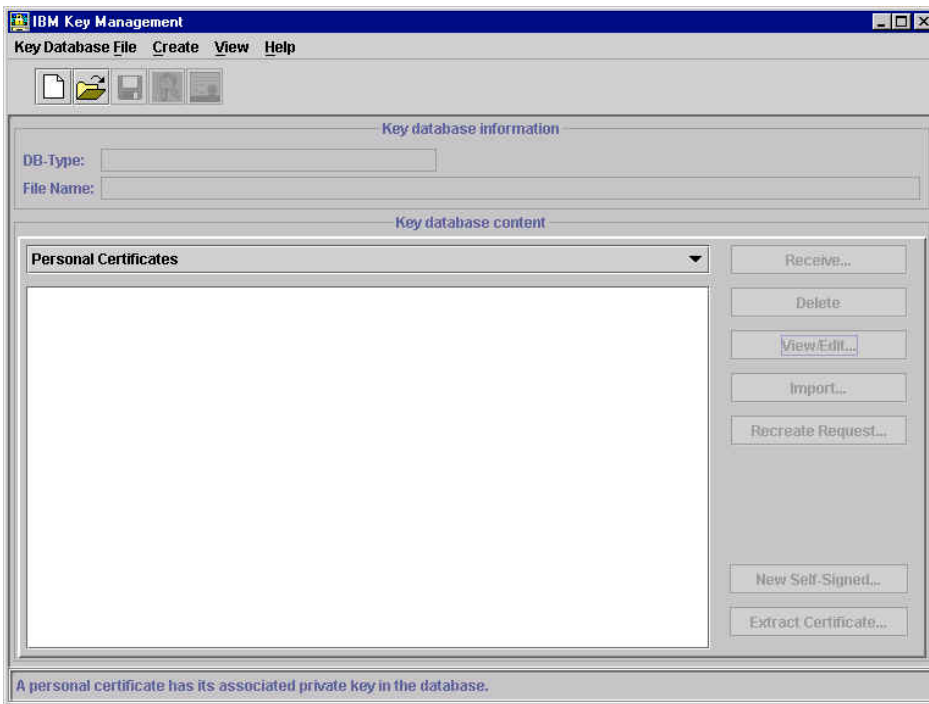
You can prevent these error messages by setting up a WebSEAL server certificate. We have documented three approaches for achieving this:

- generating a self-signed certificate;
- sending a Certificate Signing Request to a Tivoli PKI system;
- sending a Certificate Signing Request to the demonstration Entrust public Certification Authority.

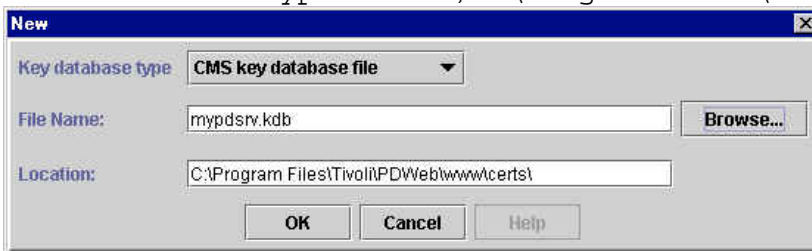
Using a self-signed certificate is adequate for a test system where it is feasible to install the Certificate Authority certificate in the users' browsers; for a production system you would need to send off a Certificate Signing Request (together with appropriate documentation and payment) to a well known Certificate Authority whose certificate is installed by default in the users' browsers.

### Approach (a) - Generating a self-signed certificate

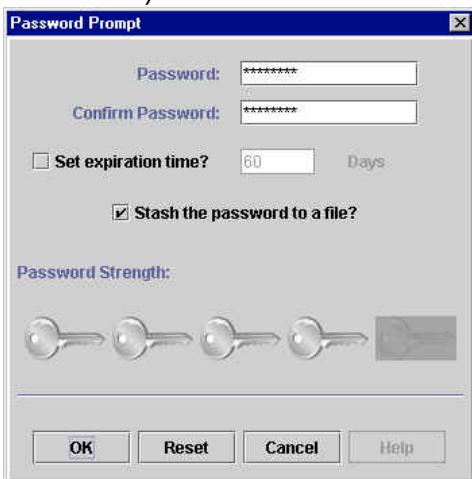
- a. First you may like to back up all the files in `C:\Program Files\Tivoli\PDWeb\www\certs` on Windows or `/var/pdweb/www/certs` on UNIX. The default key database and stash file is contained in this directory; we also used this directory to store the key database and stash file which we created.
- b. If WebSEAL is currently running, stop it. (In Windows, select Services and stop Policy Director WebSEAL. In UNIX issue `/etc/iv/pdweb stop`.)
- c. Start the iKeyman utility:  
In Windows use 'My Computer' or 'Windows Explorer' find the `C:\Program Files\IBM\gsk4\bin` directory and double click on **gsk4ikm.exe**.  
On UNIX type `/usr/bin/gsk4ikm`  
The IBM Key Management window appears:



d. Create a new Key Database: click on Key Database File -> New, and specify a File Name and Location. We used mypdsrv.kdb, C:\Program Files\Tivoli\PDWeb\www\certs\:



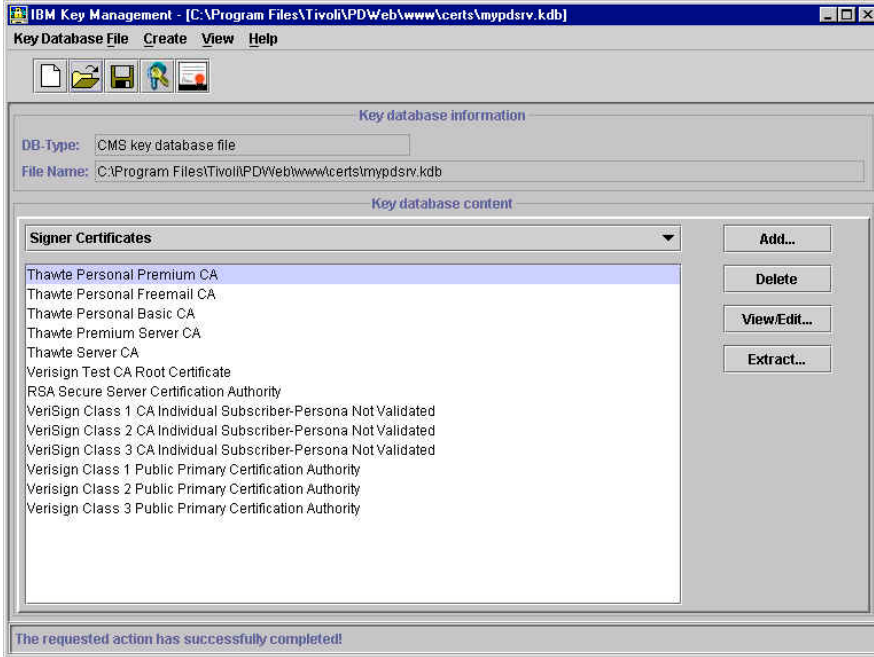
e. Click on 'OK'. A Password Prompt panel will be displayed. Enter a password (twice) (we used Secure99) and check the 'Stash the password to a file?' box:



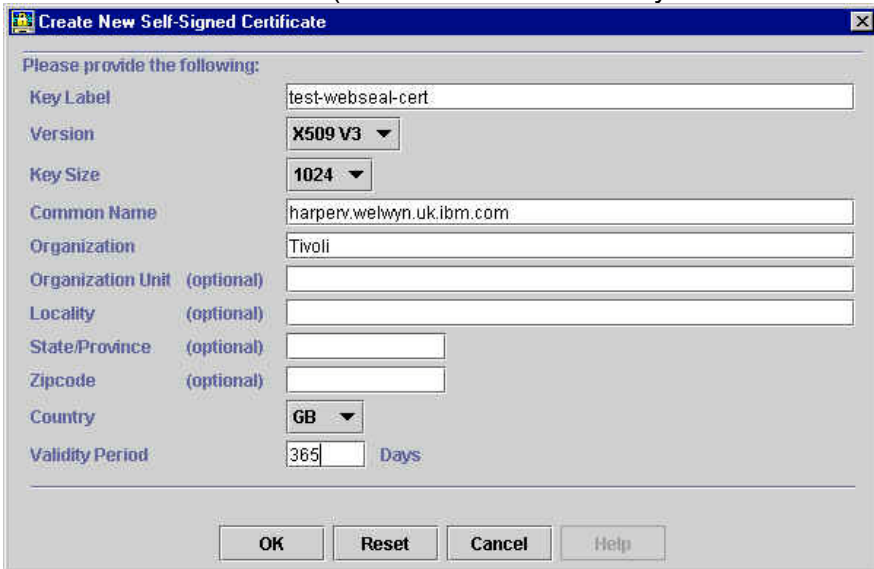
f. Click on 'OK'; an information message will inform you where the password has been saved:



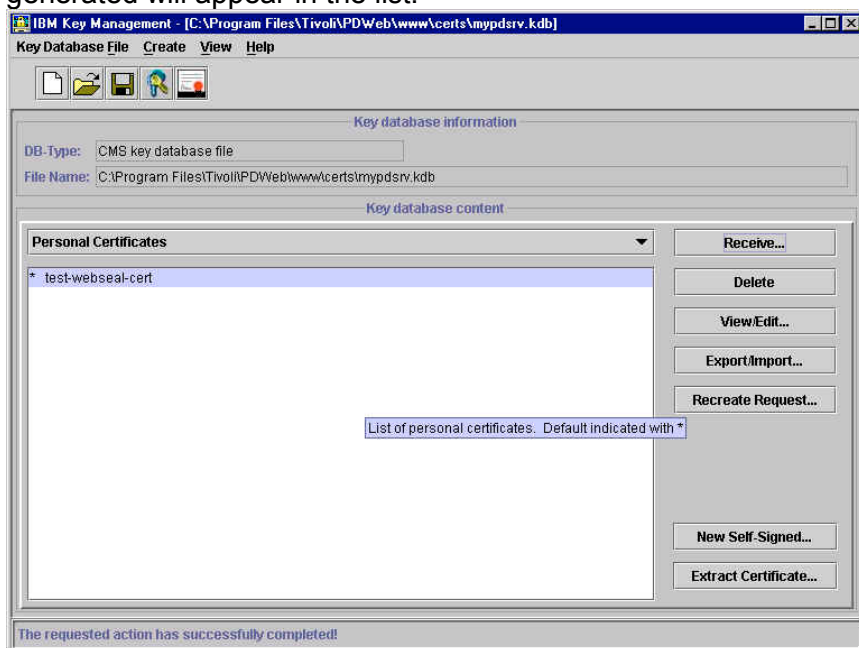
g. Click on 'OK'; information about the key database just created will be displayed:



h. Click on Create -> New Self-Signed Certificate; the 'Create New Self-Signed Certificate' panel will be displayed. Enter a Key Label (we used `test-webseal-cert`), Organization and Country. Ensure that the Common Name is specified which matches the DNS Domain Name of the WebSEAL machine. (The Common Name may be automatically filled in for you.)



- i. Click on 'OK'; a public/private key pair and certificate are generated. The certificate just generated will appear in the list:



- j. The IBM Key Management utility is no longer required and may be closed.
- k. Back up webseald.conf (Windows: in C:\Program Files\Tivoli\PDWeb\etc; UNIX: in /opt/pdweb/etc).
- l. Edit webseald.conf:  
 modify the webseal-cert-keyfile line to point to the key database file (mypdsrv.kdb in our case);  
 modify the webseal-cert-keyfile-stash line to point to the key database password stash file (mypdsrv.sth in our case);  
 specify the key label by introducing a line in the [ssl] stanza of the following form:  
 webseal-cert-keyfile-label = test-webseal-cert
- m. On UNIX, after creating the key database file, change the file ownership of the key database file and stash file to **ivmgr**. Use the appropriate operating system command for changing file ownership:  

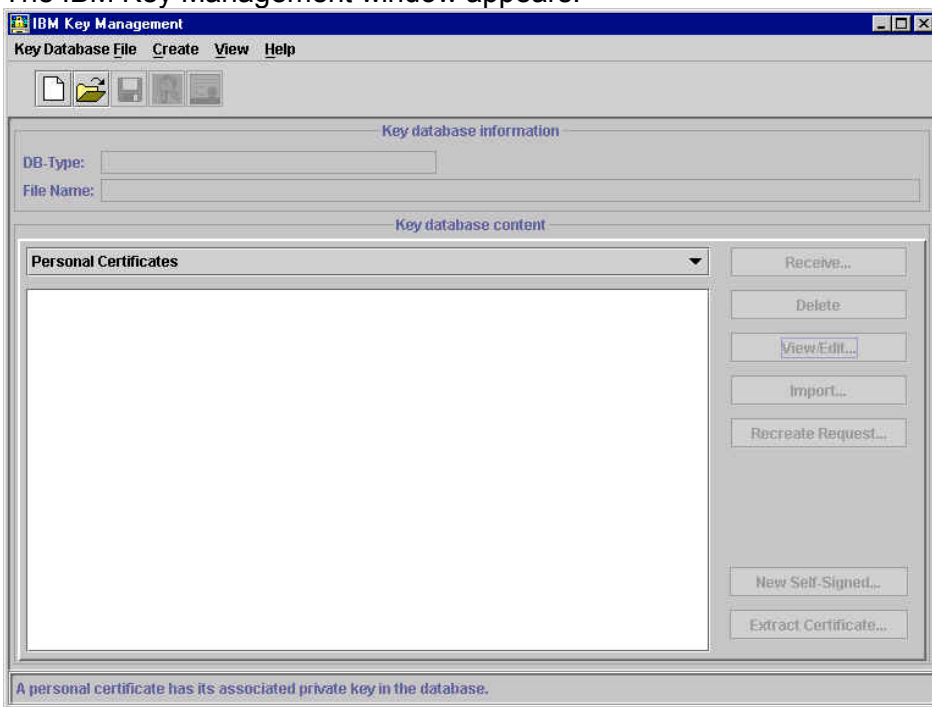
```
# chown ivmgr <keyfile>
# chown ivmgr <stashfile>
```

 (Need to check whether this is necessary with PD 3.8. \*\*)
- n. Start WebSEAL. (In Windows, start Policy Director WebSEAL. In UNIX issue /etc/iv/pdweb start)
- o. Ensure that all the Policy Director services/process have started. If they do not all start, look in the log for the corresponding service/process.
- p. Verify that Policy Director is behaving as is now expected by pointing a web browser at WebSEAL using SSL. Note that a message indicating 'New Site Certificate' or 'The security certificate was issued by a company you have not chosen to trust' (or equivalent), as we have merely installed a self-signed certificate, but you can choose accept the certificate (either for this session or until it expires) using the browser panels. You should no longer see the Certificate Name Check message.

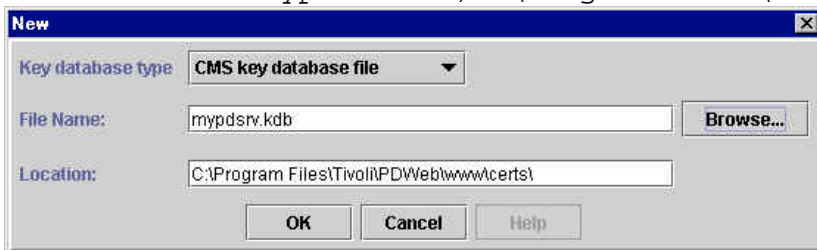


## Approach (b) - Certificate Signing Request sent to Tivoli PKI

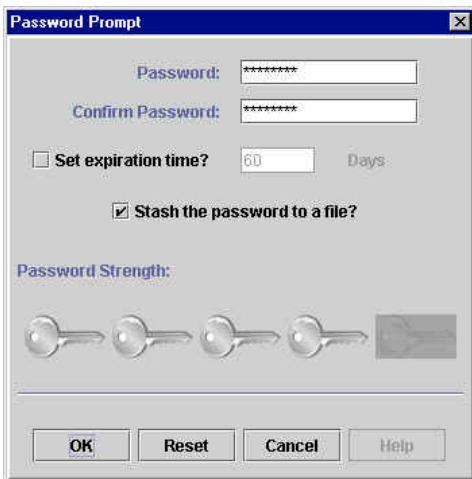
- a. First you may like to back up all the files in `C:\Program Files\Tivoli\PDWeb\www\certs` on Windows or `/var/pdweb/www/certs` on UNIX. The default key database and stash file is contained in this directory; we also used this directory to store the key database and stash file which we created.
- b. If WebSEAL is currently running, stop it. (In Windows, select Services and stop Policy Director WebSEAL. In UNIX issue `/etc/iv/pdweb stop`.)
- c. Start the iKeyman utility:  
 In Windows use 'My Computer' or 'Windows Explorer' find the `C:\Program Files\IBM\gsk4\bin` directory and double click on `gsk4ikm.exe`.  
 On UNIX type `/usr/bin/gsk4ikm`  
 The IBM Key Management window appears:



- d. Create a new Key Database: click on Key Database File -> New, and specify a File Name and Location. We used `mypdsrv.kdb`, `C:\Program Files\Tivoli\PDWeb\www\certs\`:



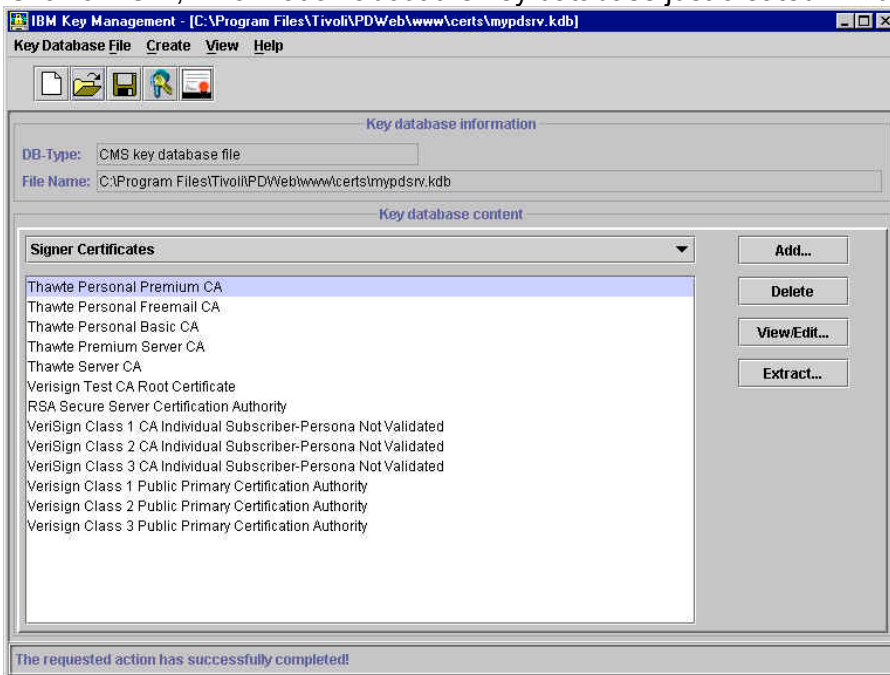
- e. Click on 'OK'. A Password Prompt panel will be displayed. Enter a password (twice) (we used `Secure99`) and check the 'Stash the password to a file?' box:



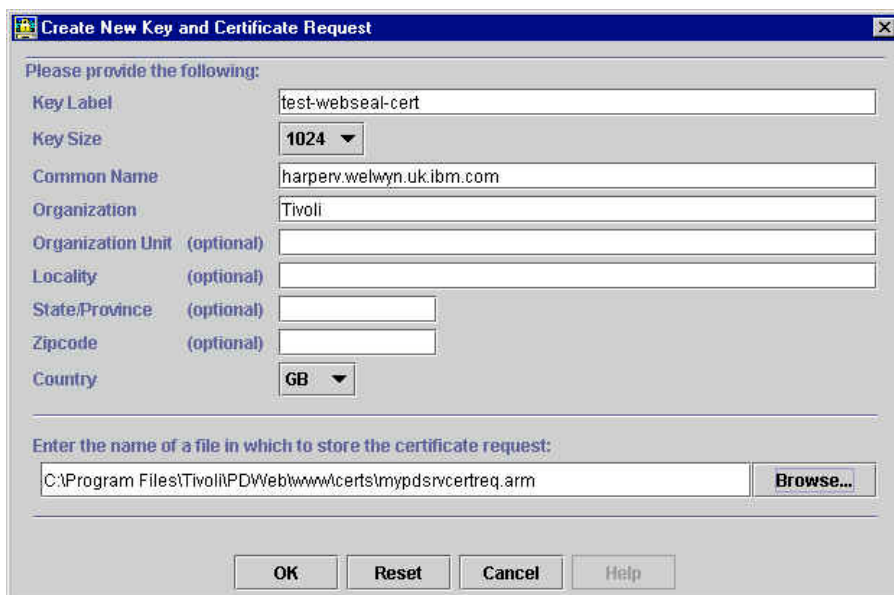
f. Click on 'OK'; an information message will inform you where the password has been saved:



g. Click on 'OK'; information about the key database just created will be displayed:



h. Click on Create -> New Certificate Request; the 'Create New Key and Certificate Request' panel will be displayed. Enter a Key Label (we used test-webseal-cert), Organization and Country, and specify the name of a file in which to store the certificate request. Ensure that the Common Name is specified which matches the DNS Domain Name of the WebSEAL machine. (The Common Name may be automatically filled in for you.)



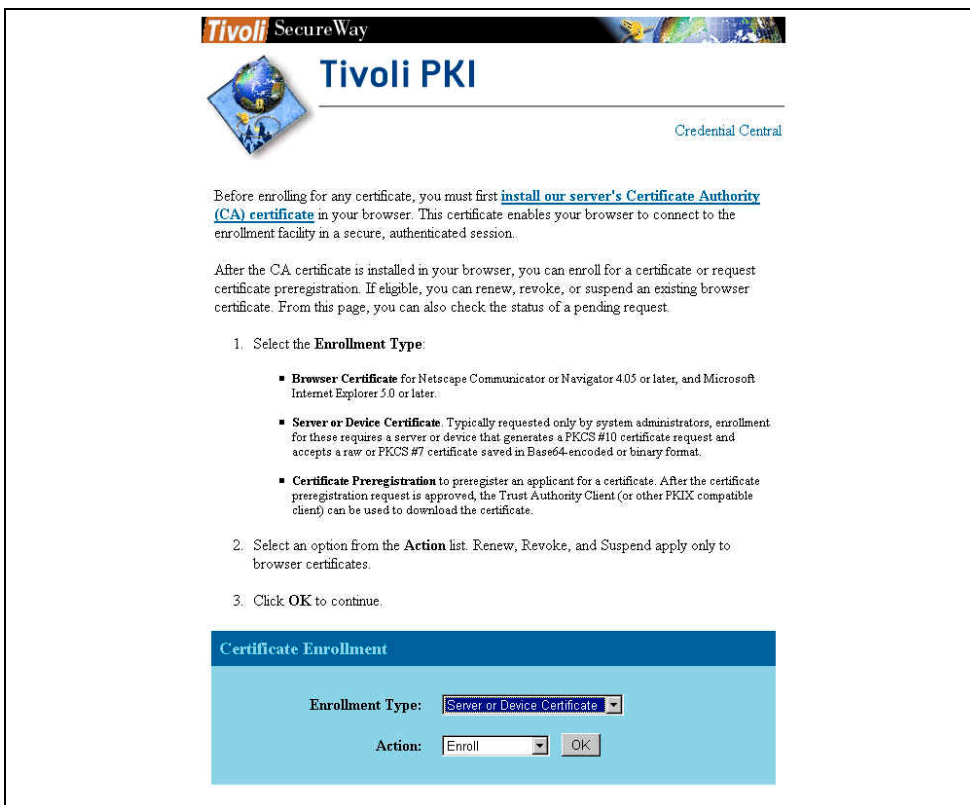
i. Click on 'OK'; an information message will inform you where the certificate request has been stored:



j. Click on 'OK' to dismiss the information message.

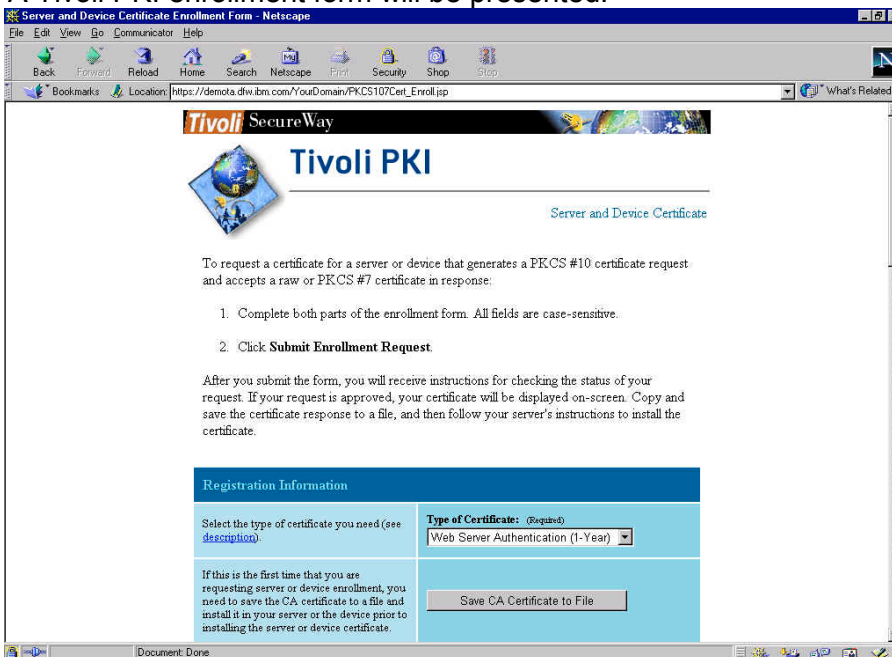
k. Point a web browser at Credential Central on a Tivoli PKI system (such as the demo system at <http://demota.dfw.ibm.com/YourDomain/index.jsp> - this site is accessible over the Internet.)

l. Select Enrolment Type as `Server` or `Device Certificate` and Action as `Enrol`:



m. Click on 'OK'. You may receive warning messages indicating that the server certificate has been issued by a CA which is not trusted by your browser; accept the Site Certificate (at least for this session) so that SSL can be established.

n. A Tivoli PKI enrollment form will be presented:



o. Click on 'Save CA Certificate to File'. The browser will display a 'Save As...' panel: specify a directory and filename as to where to save the CA Certificate. (We used C:\Program Files\Tivoli\PDWeb\www\certs\CACertRaw.b64.)

- p. Fill in First Name, Last Name and the Domain Name (which should match the DNS name of the WebSEAL machine).
- q. Use Notepad (or equivalent) to open the file containing the certificate signing request (mypdsrvcertreq.arm in our case). Copy to the clipboard all the text from `BEGIN NEW CERTIFICATE REQUEST` to `END NEW CERTIFICATE REQUEST`, then copy this to the 'PKCS #10 Certificate Request' area on the browser input form:



Server and Device Certificate

To request a certificate for a server or device that generates a PKCS #10 certificate request and accepts a raw or PKCS #7 certificate in response:

1. Complete both parts of the enrollment form. All fields are case-sensitive.
2. Click **Submit Enrollment Request**.

After you submit the form, you will receive instructions for checking the status of your request. If your request is approved, your certificate will be displayed on-screen. Copy and save the certificate response to a file, and then follow your server's instructions to install the certificate.

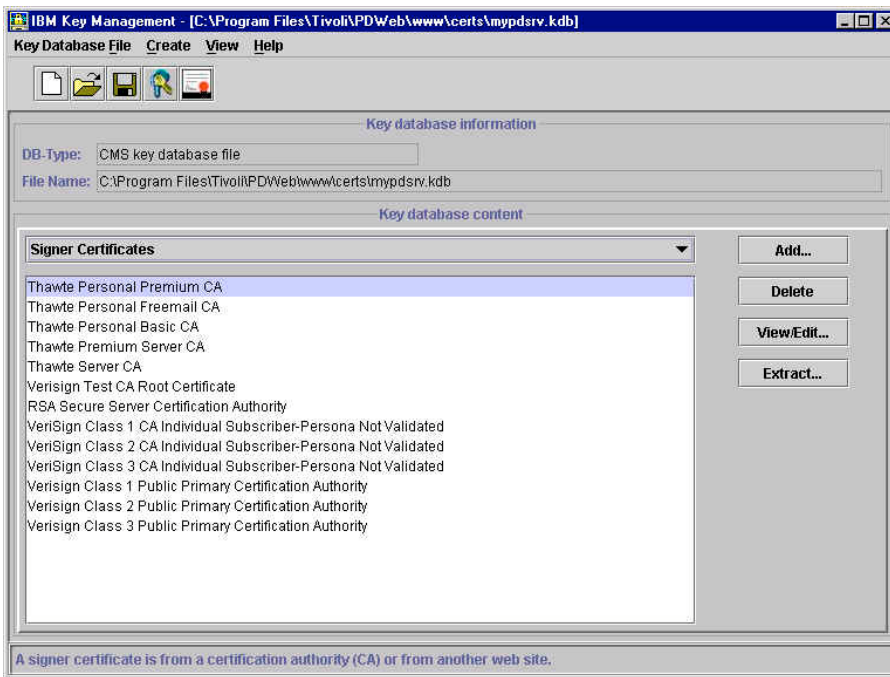
Registration Information	
Select the type of certificate you need (see <a href="#">description</a> ).	<b>Type of Certificate:</b> (Required) Web Server Authentication (1-Year)
If this is the first time that you are requesting server or device enrollment, you need to save the CA certificate to a file and install it in your server or the device prior to installing the server or device certificate.	<input type="button" value="Save CA Certificate to File"/>
Type your first name or given name and, optionally, your middle name or initial.	<b>First Name:</b> (Required) Vaughan
Type your last name, family name, or surname.	<b>Last Name:</b> (Required) Harper
Type your e-mail address, including the at sign (@) and any periods (.). This e-mail address is required by some certificate types, such as those used for secure e-mail.	<b>E-mail Address:</b> (Optional)
Select this option to receive an e-mail notification when your request has been finalized.	<input type="checkbox"/> <b>E-mail Notification:</b> (Optional)
Type a Challenge Question and a Response that are special to you and easy to remember. If you are asked the same Challenge Question when you check your enrollment status, you must respond with the same Challenge Response.	<b>Challenge Question:</b> (Optional) _____ <b>Challenge Response:</b> (Optional) _____

Certificate Request Information	
Copy and paste here the content of the PKCS #10 certificate request (see sample) that was generated by the server or device for which you are requesting a certificate. If you saved the certificate request to a file, open the file in a text editor such as Notepad, and then copy and paste the certificate request here.	<b>PKCS #10 Certificate Request:</b> (Required) -----BEGIN NEW CERTIFICATE REQUEST----- MIIDgTCB6wIBADBQCSwCQYDWOQGEWJH0jEPMAOG VQQDExloYKJwZXJ2Lnd1bHd5b+51ay5pYm0uY29t A4GNADCB1QEBGQCEIge21vMbChwNgPH77fQdS9Rj CSzKrdgTeWAQs12P1we0t4DcCsez1MqSEH2ot/t KcVIUR+Jxr18e1fx8voNqbm2KrcCV68nL6kxRMcB oAAwYj0Ko21hvcNAQEEBQADgTEABkoVpP0C/dD SMTC0cEwzibR0Qvew0Mk0c7ynL701ESGfANyvw i5Xmf05uhrdWqmE+latw+ekiwem54xXI+k9B4CAN NZJ1Op4= -----END NEW CERTIFICATE REQUEST-----
The data you enter below will override the data contained in the PKCS #10 for the same field. Leave the field blank if you already entered the data in your PKCS #10 request and do not wish to override it.	
Type a name to identify this certificate. Typically this is the hostname of your server or device. This field is required if the PKCS #10 certificate request does not contain the Common Name.	<b>Common Name:</b> (Optional)
Type the legally registered name of your organization.	<b>Organization Name:</b> (Optional)
Type the name of your division or department, such as Human Resources or Software Development.	<b>Organizational Unit:</b> (Optional)
Type the street address of your organization.	<b>Street Address:</b> (Optional)
Type the city or municipality where your organization is located, such as Chicago or Paris.	<b>Locality:</b> (Optional)
Type the state or province where your organization is located. Do not abbreviate. For example, use New York instead of NY.	<b>State or Province:</b> (Optional)
Select the country where your organization is located.	<b>Country:</b> (Optional) Use the one set in PKCS #10
Type the domain name if you were instructed to do so. For example, mypc.mydiv.mycorp.com.	<b>Domain Name:</b> (Optional) harperv.welwyn.uk.ibm.com

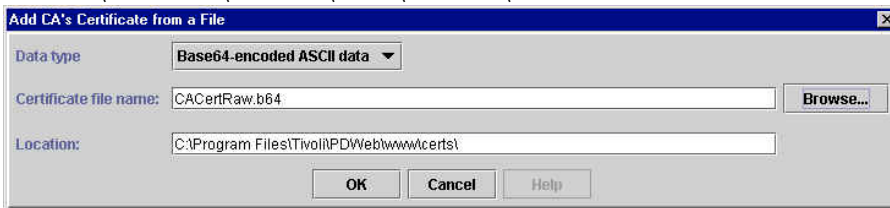
- r. Click on 'Submit Enrolment Request'. Tivoli PKI will display an enrollment status page which it suggests that you bookmark.
- s. If you are operating your own Tivoli PKI system which requires that the request be approved, start the RA Desktop and approve the request that has just been submitted.
- t. Click on 'Check Enrollment Status'. Once the enrollment request has been approved and the certificate generated, Tivoli PKI will display a 'Server and Device Certificate' page. Select Base64-Encoded Raw Certificate for PC (CRLF) or Select Base64-Encoded Raw Certificate for UNIX (LF only) as appropriate:



- u. Click on 'Save Certificate to Disk'. Specify a filename and directory and save the file. (The filename will default to RawCert .b64.)
- v. In the IBM Key Management window, select 'Signer Certificates' from the pull-down list:



- w. Click on 'Add...'. The 'Add CA's Certificate from a File' will be displayed. Specify the file where you saved the **CA** Certificate (C:\Program Files\Tivoli\PDWeb\www\certs\CACertRaw.b64 in our case):

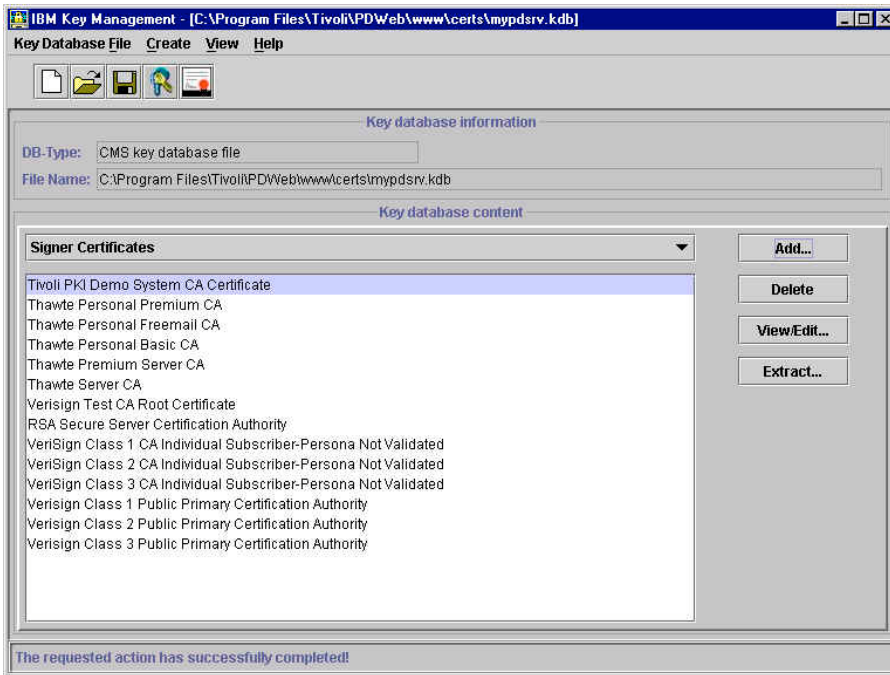


- x. Click on 'OK'. The 'Enter a Label' prompt will be displayed. Enter a label to use for the certificate:

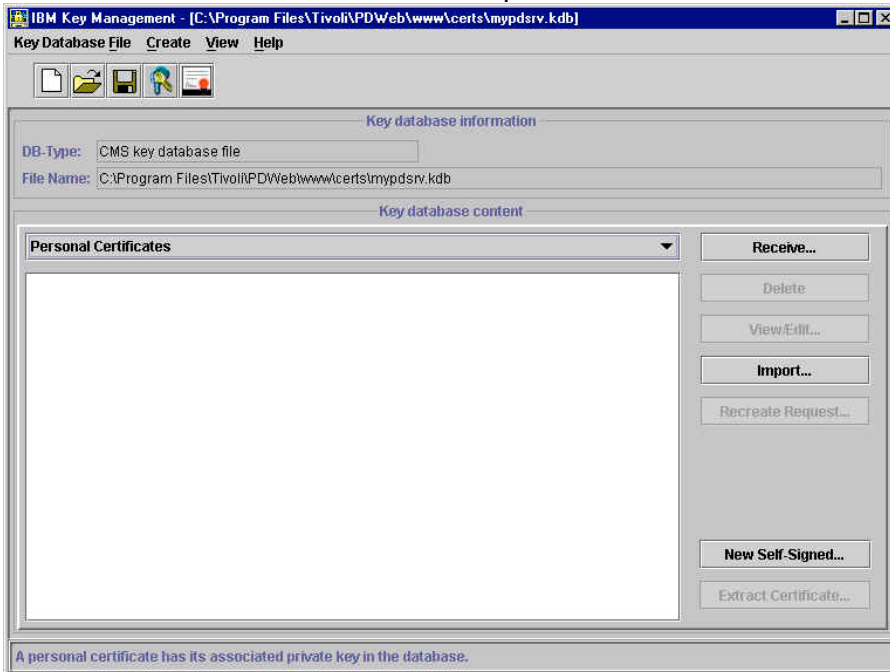


- y. Click on 'OK'. The CA Certificate will be added to the list of Signer Certificates:

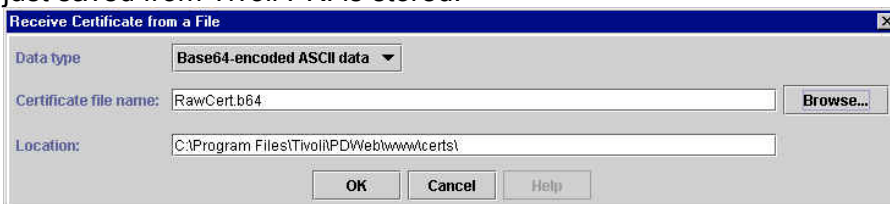




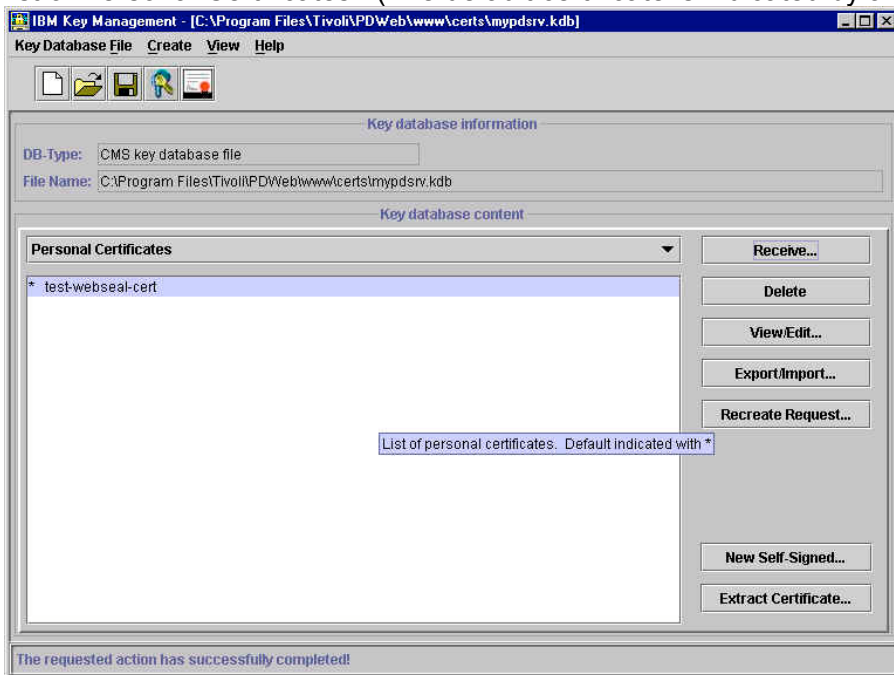
z. Select 'Personal Certificates' from the pull-down list:

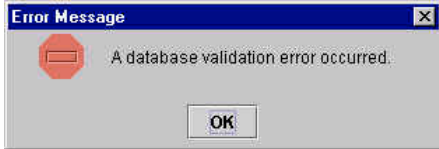


aa. Click on Receive. The 'Receive Certificate from a File' window is displayed. Ensure that the Data type is set to Base64-encoded ASCII data and specify the file in which the certificate you just saved from Tivoli PKI is stored:



bb. Click on 'OK'; the WebSEAL Certificate which has been signed by the CA will be added to the list of Personal Certificates. (The default certificate is indicated by an asterisk (\*).)





**Note:** If you receive an Error Message indicating 'A database validation error occurred', this is likely to be because GSKit will allow the reception only of Personal Certificates which are either self-signed or signed by a CA whose certificate is listed in the list of Signer Certificates. The step described above of receiving the CA Certificate should prevent this error message.

cc. The IBM Key Management utility is no longer required and may be closed.

dd. Back up webseald.conf (Windows: in C:\Program Files\Tivoli\PDWeb\etc; UNIX: in /opt/pdweb/etc).

ee. Edit webseald.conf:

- modify the webseal-cert-keyfile line to point to the key database file (mypdsrv.kdb in our case);
- modify the webseal-cert-keyfile-stash line to point to the key database password stash file (mypdsrv.sth in our case);
- specify the key label by introducing a line in the [ssl] stanza of the following form:  
webseal-cert-keyfile-label = test-webseal-cert

ff. On UNIX, after creating the key database file, change the file ownership of the key database file and stash file to **ivmgr**. Use the appropriate operating system command for changing file

**ownership:**

```
# chown ivmgr <keyfile>  
# chown ivmgr <stashfile>
```

(Need to check whether this is necessary with PD 3.8. \*\*)

gg. Start WebSEAL. (In Windows, start Policy Director WebSEAL. In UNIX issue  
/etc/iv/pdweb start)

hh. Ensure that all the Policy Director services/process have started. If they do not all start, look in the log for the corresponding service/process.

ii. Verify that Policy Director is behaving as is now expected by pointing a web browser at WebSEAL using SSL. Note that a message indicating 'New Site Certificate' or 'The security certificate was issued by a company you have not chosen to trust' (or equivalent), as we have not used a CA whose certificate is installed in the browser by default, but you can choose accept the certificate (either for this session or until it expires) using the browser panels. You should no longer see the Certificate Name Check message.

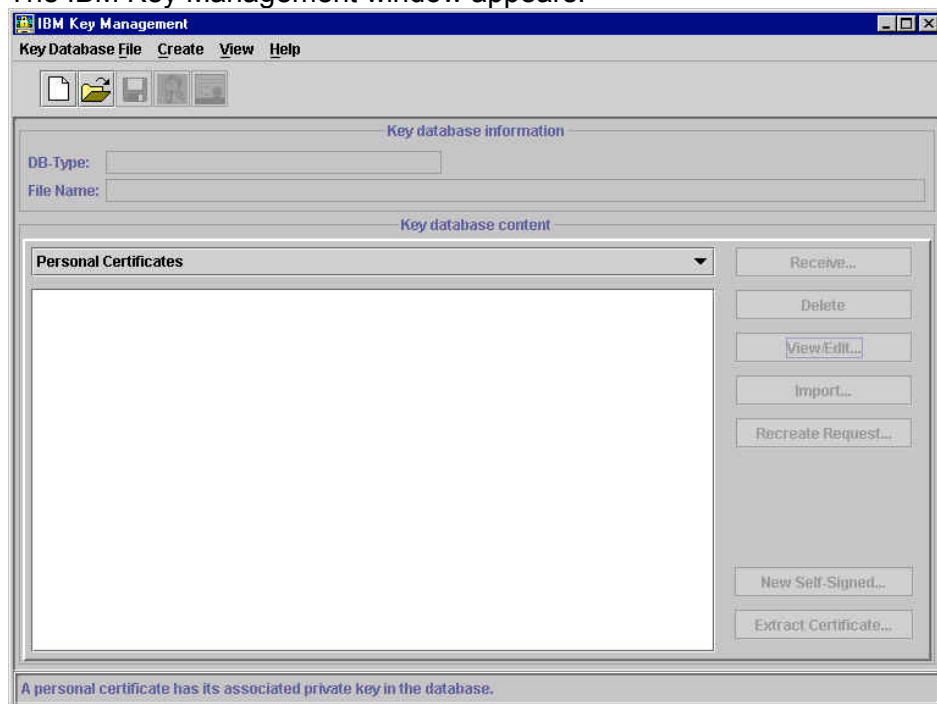
## Approach (c) - Certificate Signing Request sent to Entrust CA

- a. First you may like to back up all the files in C:\Program Files\Tivoli\PDWeb\www\certs on Windows or /var/pdweb/www/certs on UNIX. The default key database and stash file is contained in this directory; we also used this directory to store the key database and stash file which we created.
- b. If WebSEAL is currently running, stop it. (In Windows, select Services and stop Policy Director WebSEAL. In UNIX issue /etc/iv/pdweb stop.)
- c. Start the iKeyman utility:

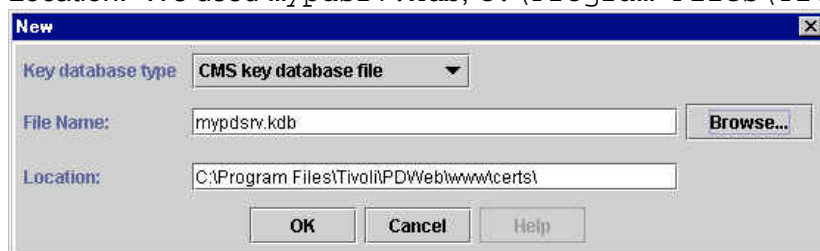
In Windows use 'My Computer' or 'Windows Explorer' find the C:\Program Files\IBM\gsk4\bin directory and double click on **gsk4ikm.exe**.

On UNIX type /usr/bin/gsk4ikm

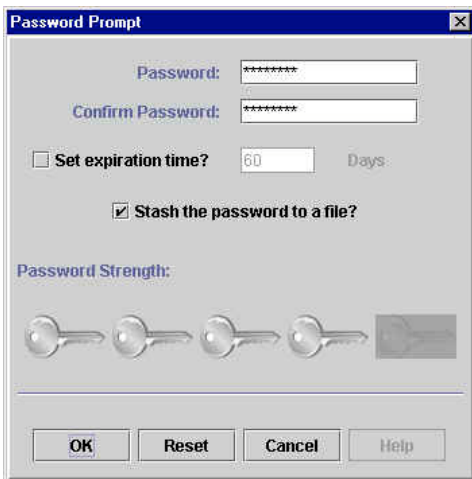
The IBM Key Management window appears:



- d. Create a new Key Database: click on Key Database File -> New, and specify a File Name and Location. We used mypdsrv.kdb, C:\Program Files\Tivoli\PDWeb\www\certs\:



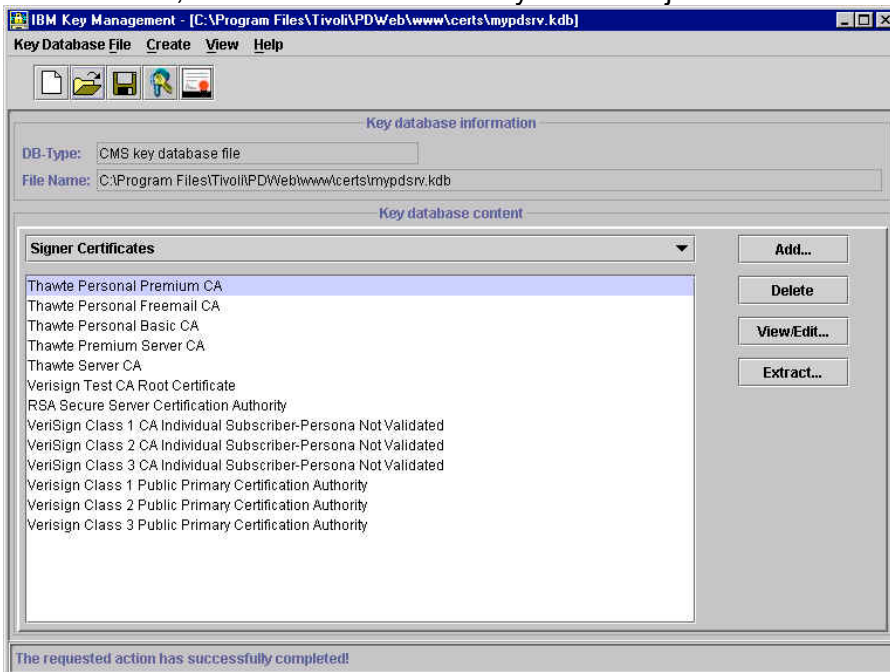
- e. Click on 'OK'. A Password Prompt panel will be displayed. Enter a password (twice) (we used Secure99) and check the 'Stash the password to a file?' box:



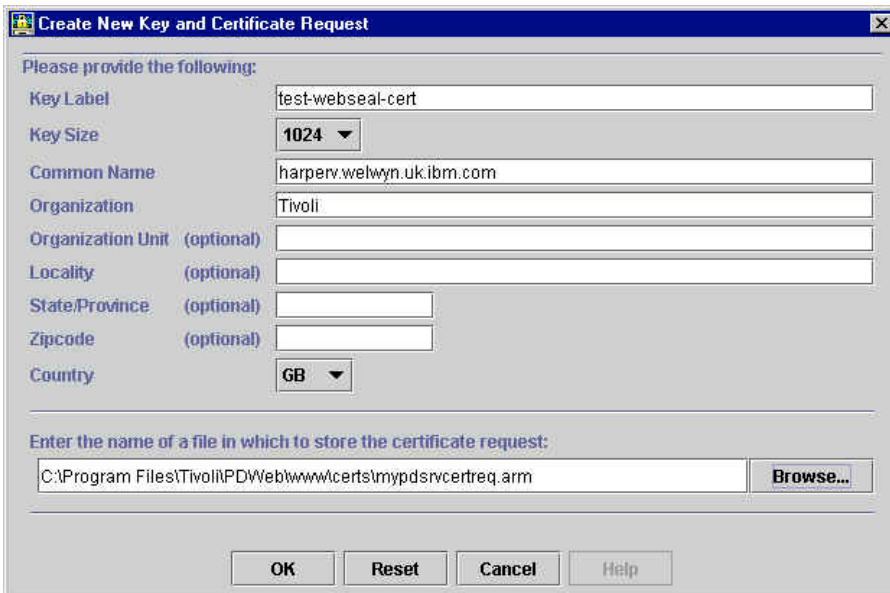
f. Click on 'OK'; an information message will inform you where the password has been saved:



g. Click on 'OK'; information about the key database just created will be displayed:



h. Click on Create -> New Certificate Request; the 'Create New Key and Certificate Request' panel will be displayed. Enter a Key Label (we used `test-webseal-cert`), Organization and Country, and specify the name of a file in which to store the certificate request. Ensure that the Common Name is specified which matches the DNS Domain Name of the WebSEAL machine. (The Common Name may be automatically filled in for you.)

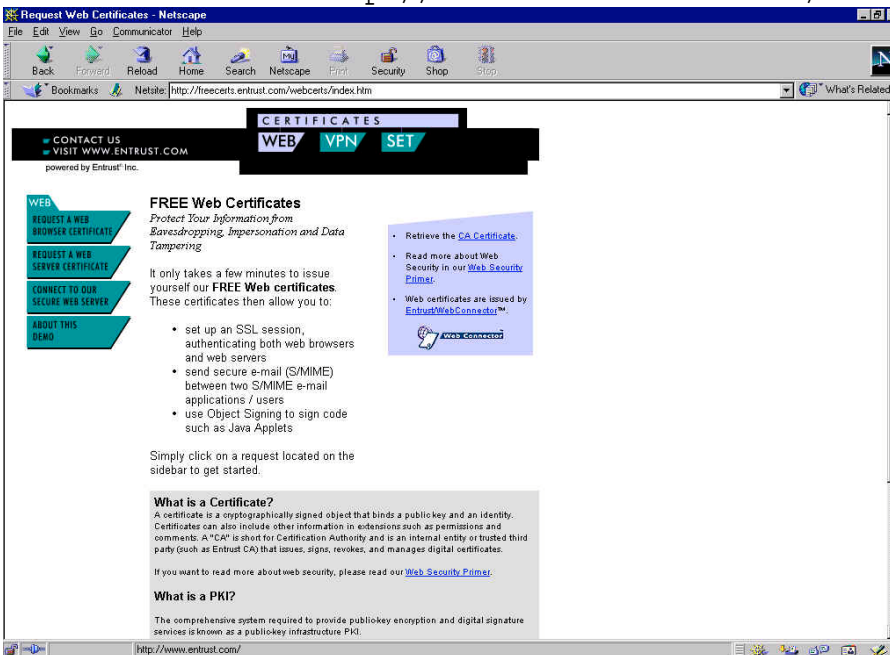


i. Click on 'OK'; an information message will inform you where the certificate request has been stored:



j. Click on 'OK' to dismiss the information message.

k. Point a web browser at <http://freecerts.entrust.com/webcerts/index.htm>:



l. Click on 'Request a Web Server Certificate'. Fill in the input fields, specify the purpose for requesting a certificate and the web browser in use, and click on 'Yes' against 'Do you accept the terms and conditions as set out above':

CERTIFICATES

[CONTACT US](#)  
[VISIT WWW.ENTRUST.COM](#)  
powered by Entrust® Inc.

WEB
VPN
SET

WEB

REQUEST A WEB BROWSER CERTIFICATE

REQUEST A WEB SERVER CERTIFICATE

CONNECT TO OUR SECURE WEB SERVER

ABOUT THIS DEMO

### Step 1 - Accept and Fill out the Application

A Web server certificate allows you to authenticate to Web browsers via SSL. In order to successfully verify other certificates it is also necessary to import the CA key into the Web server. This will be done as part of the process of receiving your Web server certificate.

---

**Note:** You must be a server administrator to install a Web server certificate. Please consult your server documentation for instructions.

Please fill out all information below before proceeding with Step 2 of your certificate request.

First Name:

Last Name:

Company:

Email:

Phone:

**You are interested in Freecerts for the purpose of:**

**Which Web server are you using?**

**ATTENTION:**

PLEASE READ THIS IMPORTANT INFORMATION ABOUT THE FREE CERTIFICATE ISSUED BY THE ENTRUST CERTIFICATE DEMO CA.

BY CLICKING ON "YES" AND/OR BY USING THE FREE CERTIFICATE YOU AGREE AND ACKNOWLEDGE THAT THE CERTIFICATE ISSUED TO YOU BY THE ENTRUST CERTIFICATE DEMO CA IS PROVIDED AND SHALL BE USED EXCLUSIVELY FOR EDUCATION AND TESTING PURPOSES ONLY. UNDER NO CIRCUMSTANCES SHOULD THE FREE CERTIFICATES BE USED FOR COMMERCIAL PURPOSES. EACH FREE CERTIFICATE IS VALID FOR A PERIOD OF SIXTY (60) DAYS. YOU ACKNOWLEDGE AND UNDERSTAND THAT THERE HAS NOT BEEN A BACKGROUND CHECK PERFORMED ON THE CREDENTIALS PRESENTED WHEN REQUESTING THE FREE CERTIFICATE AND YOU FURTHER RECOGNIZE THAT THE CERTIFICATE HAS NOT BEEN

**Do you accept the terms and conditions as set out above.**

Yes  No

\* required fields.

The certificates issued to you on these web sites are intended for demonstration purposes only. They must not be used for commercial purposes. You should also be aware that we do not verify the identity of persons who request certificates. All certificate requests are approved automatically.

©2000 Entrust®, Inc. All Rights Reserved.

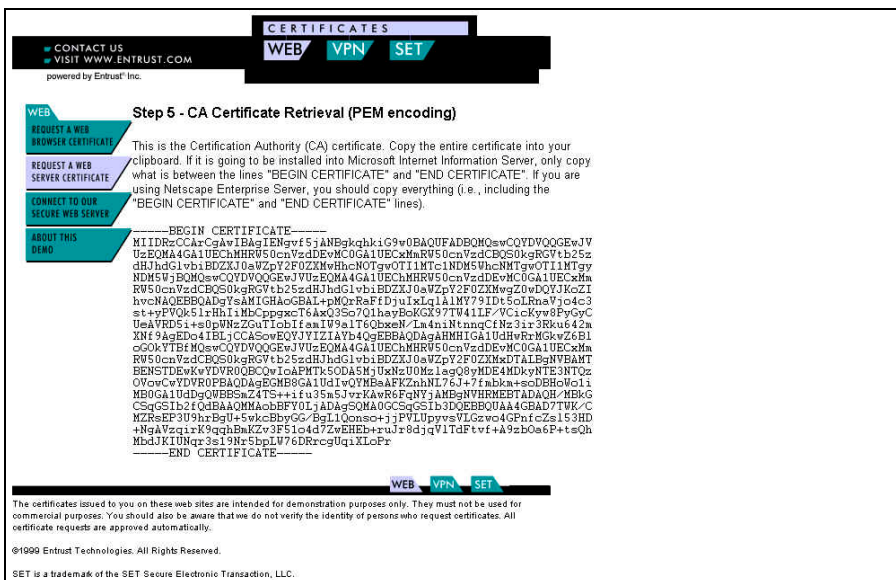
SET is a trademark of the SET Secure Electronic Transaction, LLC.

m. Click on 'Proceed to Step 2'. Specify the server name (in other words the DNS name of the WebSEAL machine). **Note:** this must match the name specified above when the Certificate Request was generated.

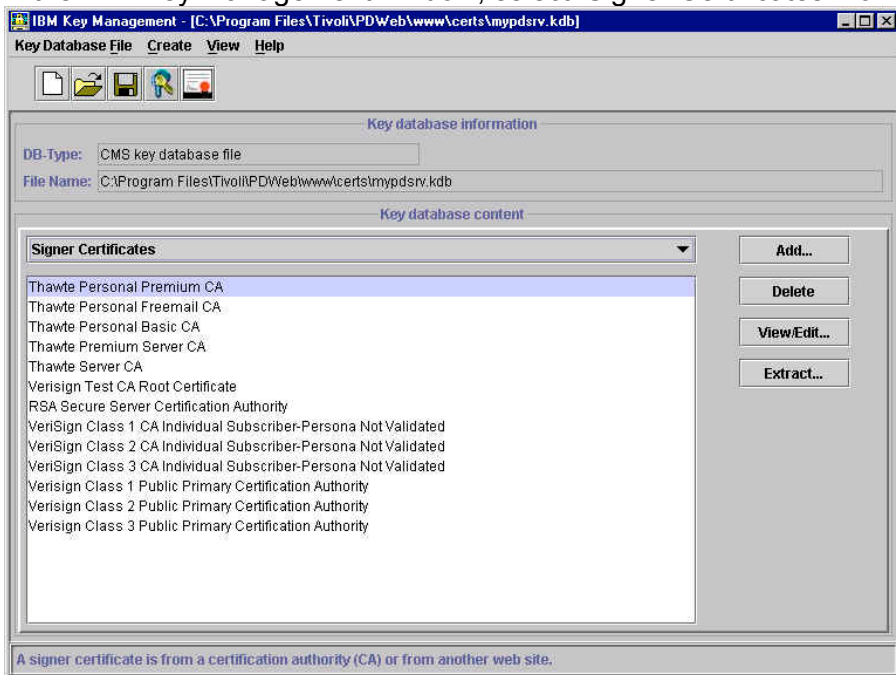




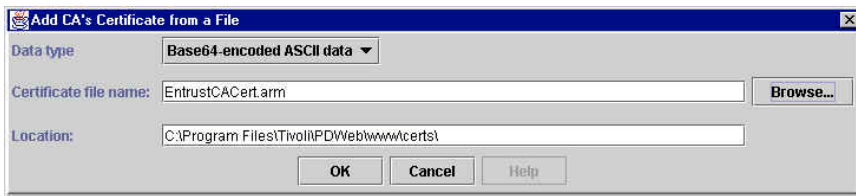




- s. Copy all the text from BEGIN CERTIFICATE to END CERTIFICATE to the clipboard, then paste it into a file; we used C:\Program Files\Tivoli\PDWeb\www\certs\EntrustCACert.arm. Again, you may need to manually edit the file to remove the spaces at the beginning of each line.
- t. In the IBM Key Management window, select 'Signer Certificates' from the pull-down list:



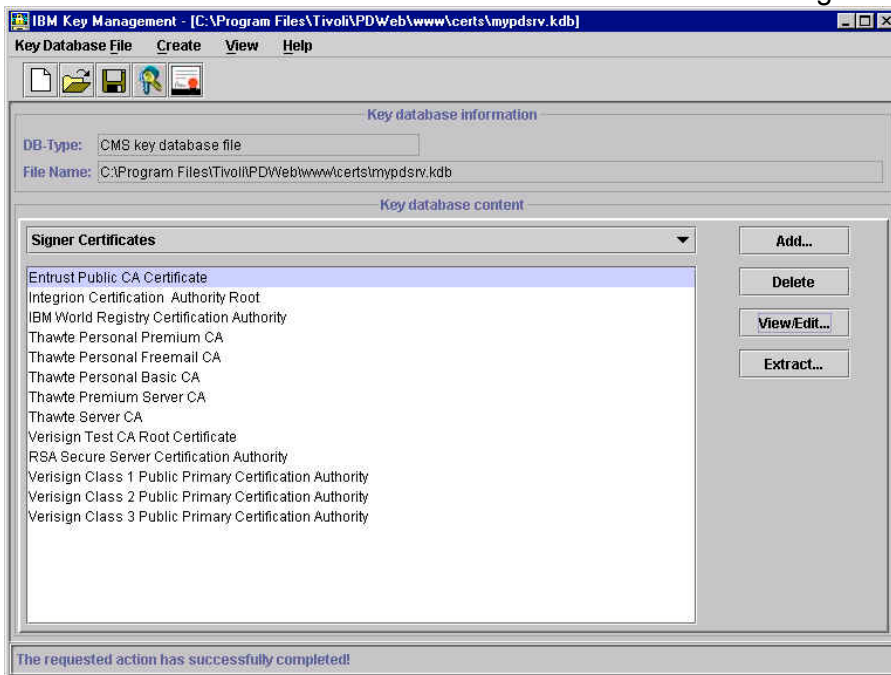
- u. Click on 'Add...'. The 'Add CA's Certificate from a File' will be displayed. Specify the file where you saved the CA Certificate (C:\Program Files\Tivoli\PDWeb\www\certs\EntrustCACert.arm in our case):



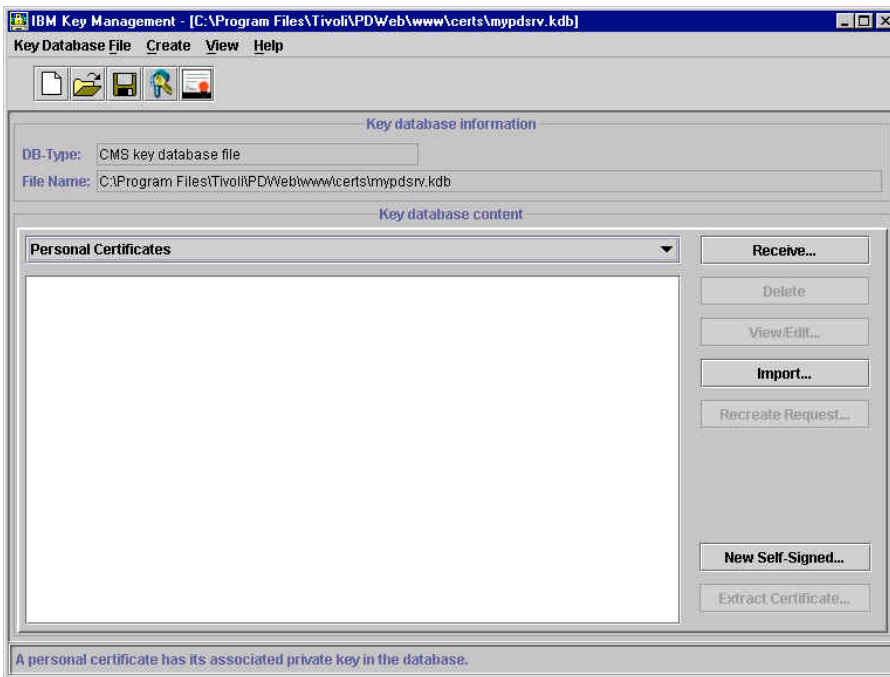
v. Click on 'OK'. The 'Enter a Label' prompt will be displayed. Enter a label to use for the certificate:



w. Click on 'OK'. The CA Certificate will be added to the list of Signer Certificates:



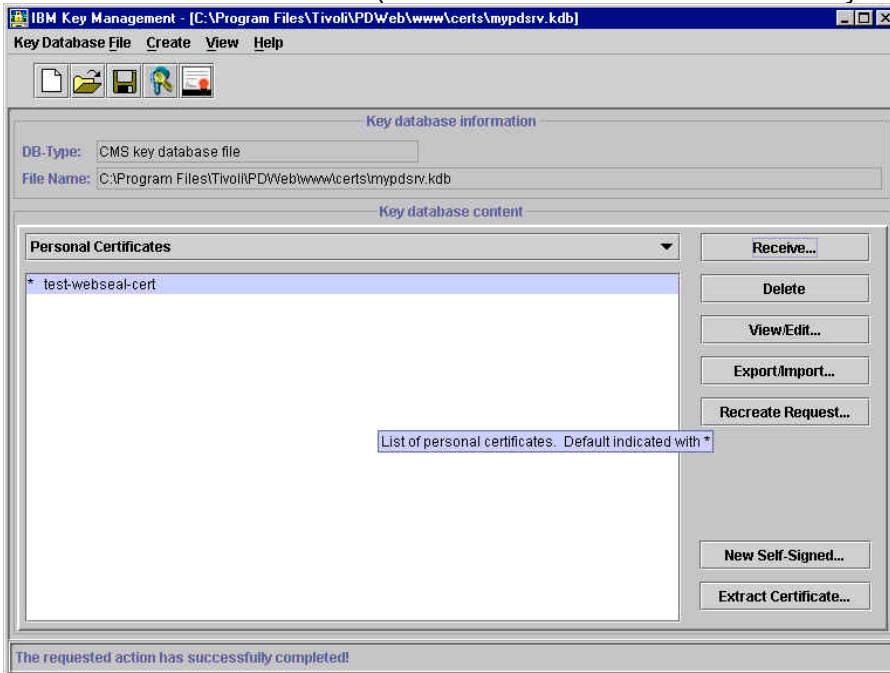
x. Select 'Personal Certificates' from the pull-down list:

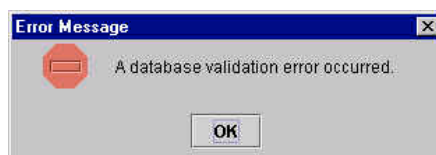


- y. Click on Receive. The 'Receive Certificate from a File' window is displayed. Ensure that the Data type is set to Base64-encoded ASCII data and specify the file in which the certificate you just saved from the Entrust PKI is stored:



- z. Click on 'OK'; the WebSEAL Certificate which has been signed by the CA will be added to the list of Personal Certificates. (The default certificate is indicated by an asterisk (\*).)





**Note:** If you receive an Error Message indicating ‘A database validation error occurred’, this is likely to be because GSKit will allow the reception only of Personal Certificates which are either self-signed or signed by a CA whose certificate is listed in the list of Signer Certificates. The step described above of receiving the CA Certificate should prevent this error message.

- aa. The IBM Key Management utility is no longer required and may be closed.
- bb. Back up `webseald.conf` (Windows: in `C:\Program Files\Tivoli\PDWeb\etc`; UNIX: in `/opt/pdweb/etc`).
- cc. Edit `webseald.conf`:
  - modify the `webseal-cert-keyfile` line to point to the key database file (`mypdsrv.kdb` in our case);
  - modify the `webseal-cert-keyfile-stash` line to point to the key database password stash file (`mypdsrv.sth` in our case);
  - specify the key label by introducing a line in the `[ssl]` stanza of the following form:  
`webseal-cert-keyfile-label = test-webseal-cert`
- dd. On UNIX, after creating the key database file, change the file ownership of the key database file and stash file to `ivmgr`. Use the appropriate operating system command for changing file ownership:
 

```
# chown ivmgr <keyfile>
# chown ivmgr <stashfile>
```

 (Need to check whether this is necessary with PD 3.8. \*\*)
- ee. Start WebSEAL. (In Windows, start Policy Director WebSEAL. In UNIX issue `/etc/iv/pdweb start`)
- ff. Ensure that all the Policy Director services/process have started. If they do not all start, look in the log for the corresponding service/process.
- gg. Verify that Policy Director is behaving as is now expected by pointing a web browser at WebSEAL using SSL. Note that a message indicating ‘New Site Certificate’ or ‘The security certificate was issued by a company you have not chosen to trust’ (or equivalent), as we have not used a CA whose certificate is installed in the browser by default, but you can choose accept the certificate (either for this session or until it expires) using the browser panels. You should no longer see the Certificate Name Check message.

## **Additional notes**

If you are using a Global Certificate (or “step-up certificate”) issued by Verisign, the procedure will be broadly the same as the Certificate Signing Request process describe above, with the addition that you need to add the intermediate certificate from Verisign to the list of signers:

- a. You can download the intermediate CA certificate for Verisign from  
[http://www.verisign.com/support/tlc/class3\\_install\\_docs/ibm/v00g.html](http://www.verisign.com/support/tlc/class3_install_docs/ibm/v00g.html) or  
<http://www.esign.com.au/custsupport/server/install/intermediate/v00g.shtml>
- b. Go to the Signer Certificates pulldown menu and click on ‘Add’.
- c. Specify the base-64 encoded certificate that you downloaded from the web site.

## 21. Setting up client certificate authentication

(Client certificates can be obtained **for demonstration use only** from the Tivoli PKI demonstration site at <http://demota.dfw.ibm.com/YourDomain/index.jsp>. This site is accessible over the Internet.)

- a. Set up a WebSEAL Server certificate as described in the previous chapter.
- b. Edit **webseald.conf** (in C:\Program Files\Tivoli\PDWeb\etc\ Windows or /opt/pdweb/etc/ UNIX): within the [certificate] stanza, there is a statement `accept-client-certs = never`  
Change it to `accept-client-certs = optional`  
or `accept-client-certs = required`
- c. Also in the **webseald.conf** uncomment the entry for **cert-ssl** and specify the library `sslauth.dll` which is provided with PD 3.8 as shown below.

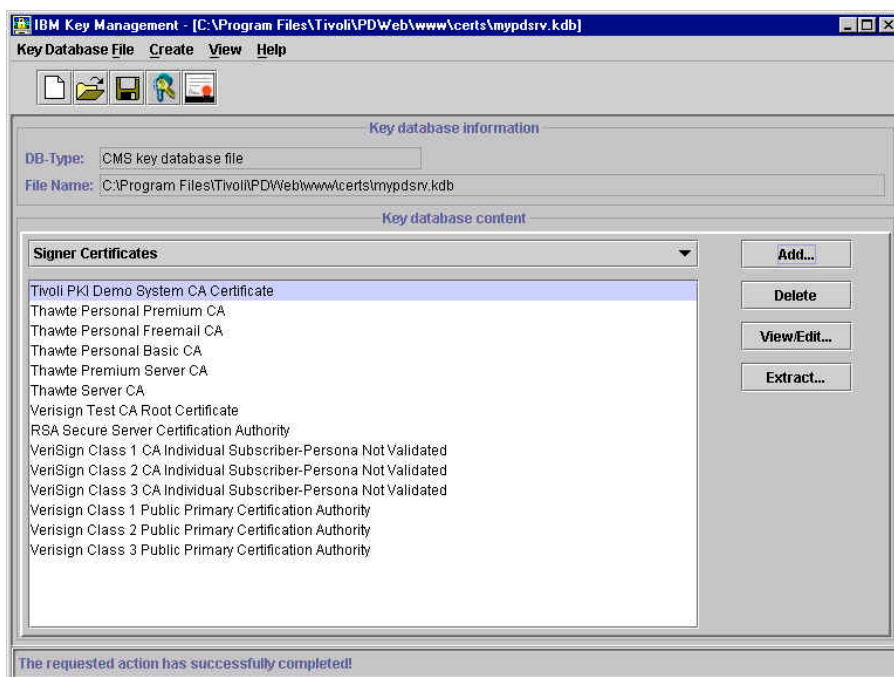
```
[authentication-mechanisms]
#-----
# AUTHENTICATION MECHANISMS AND LIBRARIES
#-----

# List of supported authentication mechanisms and
# their associated shared libraries

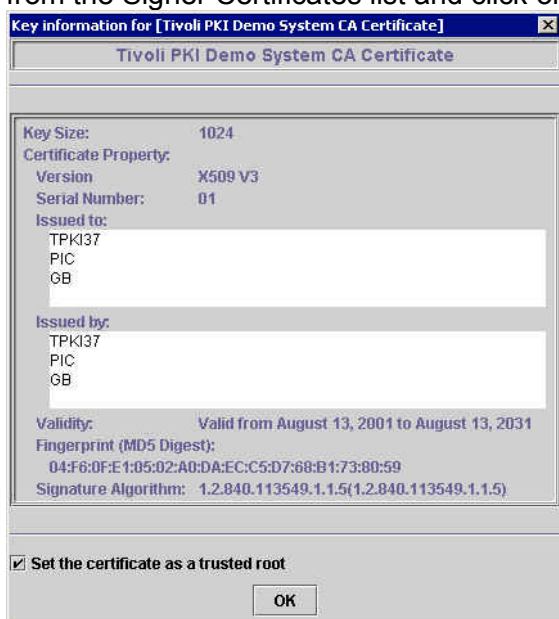
#passwd-cdas      = <passwd-cdas-library>
#passwd-ldap     = <passwd-ldap-library>
#passwd-uraf     = <uraf-authn-library>
#token-cdas      = <token-cdas-library>
cert-ssl         = sslauthn.dll
#cert-cdas       = <cert-cdas-library>
#http-request    = <http-request-library>
#cdsso           = <cdsso-authn-library>
#passwd-strength = <passwd-strength-library>
#cred-ext-attrs  = <cred-ext-attrs-library>

passwd-ldap = C:\Program Files\Tivoli\Policy Director\bin\ldapauthn.dll
cert-ldap = C:\Program Files\Tivoli\Policy Director\bin\certauthn.dll
```

- d. Start the iKeyman utility and open the key database which we configured in the previous chapter. Click on 'Signer Certificates' and add the certificates for the Certification Authority(ies) which we are choosing to trust. (If we are using the Entrust Public CA or a Tivoli PKI CA, we added this certificate when we followed the steps in the previous section.)



- e. For each Certification Authority listed in the Signer Certificates, you need to specify whether certificates issued by that CA are trusted when used for Client Authentication. Select an entry from the Signer Certificates list and click on 'Add':



- f. If you are going to trust client certificates issued by this CA, set the check mark beside 'Set the certificate as a trusted root'; if you do not trust certificates issued by this CA, clear the check mark.
- g. Click on '**OK**'.
- h. Repeat this procedure for each Signer Certificate in the list.
- i. If CRL checking is required, edit the `[ssl]` stanza in `webseald.conf` as described in the Policy Director WebSEAL Administration Guide.
- j. Ensure that the DN specified within the Client Certificate matches the LDAP DN defined for the



corresponding PD user.

k. Re-start WebSEAL to make these changes take effect.

l. Once this is all setup you should now be able to point your browser to a protected resource and use your certificate to authenticate.

---

## 22. Setting up an SSL connection to the LDAP Directory

This section describes the process for configuring SSL support for the LDAP communication between the LDAP Server and the LDAP Client(s).

- If required, install the SSL Runtime Toolkit at the LDAP Server and the LDAP Client(s)
- Create a key database file at the LDAP Server
- Create a self-signed certificate at the LDAP Server
- Create a key database file at the LDAP Client (Policy Director Server)
- Install LDAP Server certificate at the LDAP Client (Policy Director Server)
- If required, set up SSL support for the Directory Management Tool on the LDAP Client(s)

More information is given on these steps in the following paragraphs.

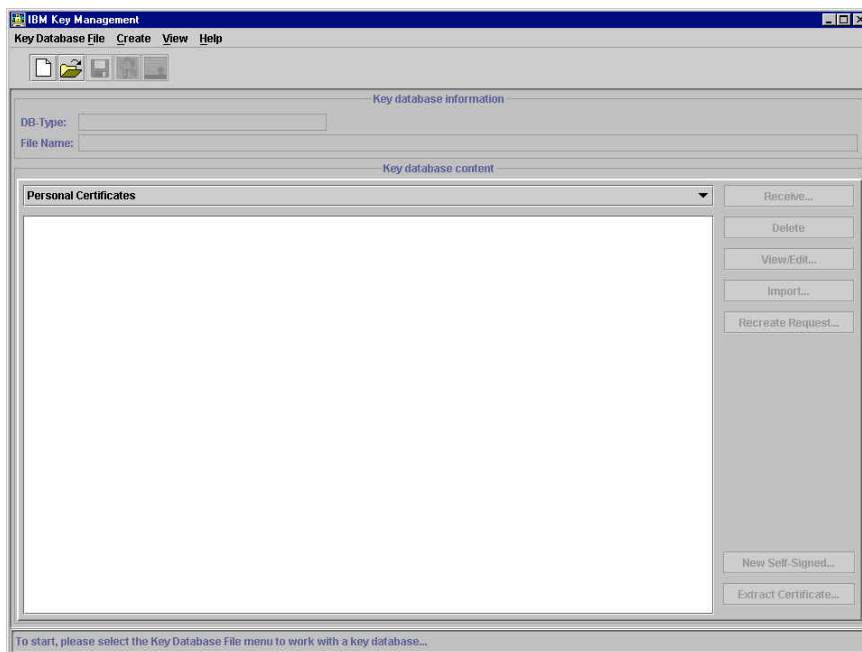
**Note:** *It may be advisable to ‘start simple’ - in other words first to get Policy Director working with an unencrypted connection to the LDAP Directory. Once this is working correctly, you can then follow the steps described in this section, then re-configure the Policy Director Servers to use an SSL connection to the LDAP Directory. (Under NT this last step also requires uninstalling and re-installing Policy Director.)*

Ensure that the IBM Global Security Kit (GSKit) SSL Runtime Toolkit is installed on both the LDAP server and any LDAP clients that will be using SSL. This should be the case as it is required by PD's RTE.

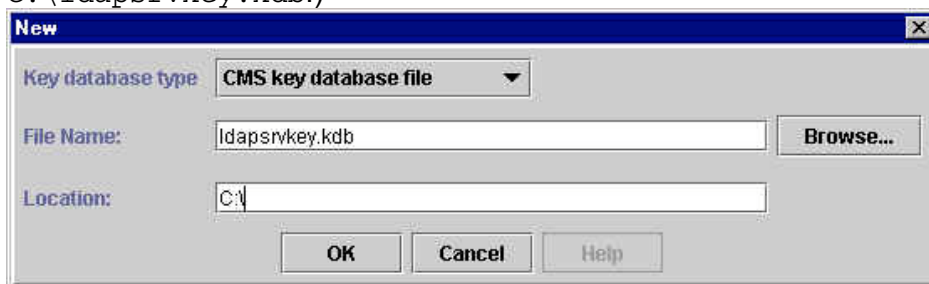
If the SSL Runtime Toolkit is installed you will find `gsk4ikm.exe` in the `C:\Program Files\IBM\GSK4\bin` directory of an NT machine.

### LDAP Server - create the key database file

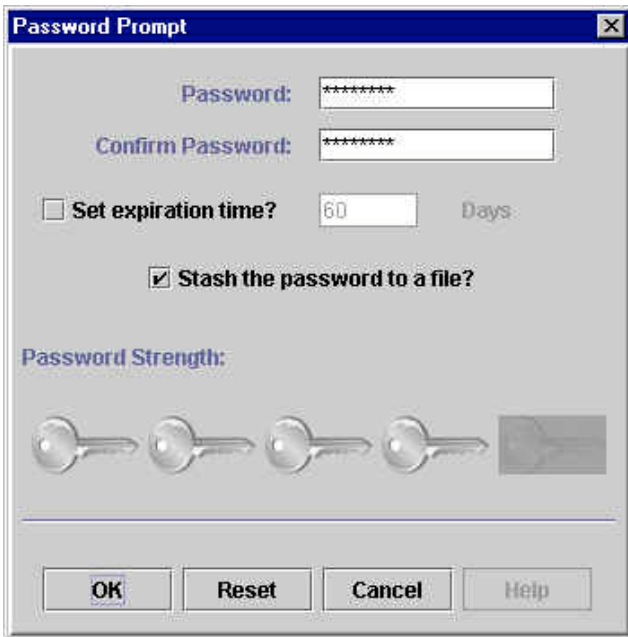
- a. On the LDAP Server machine, start the IBM Key Management tool (`gsk4ikm`):



- b. Click on Key Database File -> New; verify that the 'Key database type' is CMS key database file, and specify a filename and path for the CMS Key Database. (We used C:\ldapsrvkey.kdb.)



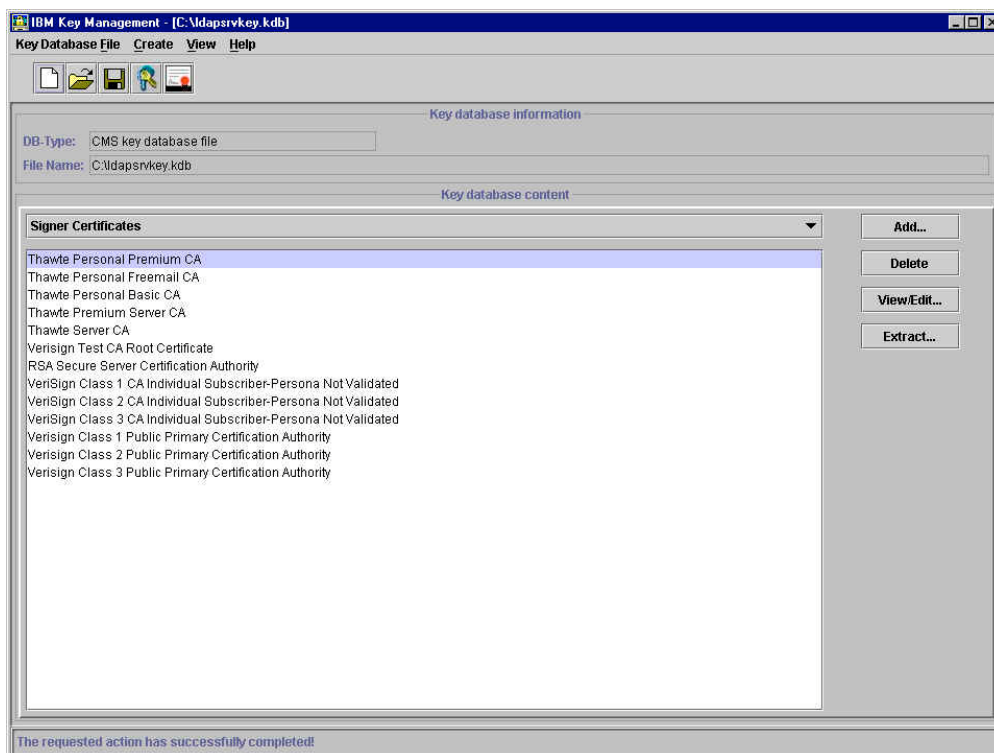
- c. Click on 'OK'. The 'Password Prompt' panel will be displayed. Enter a password (twice) (we used **Secure99**) and check the 'Stash the password to a file?' box:



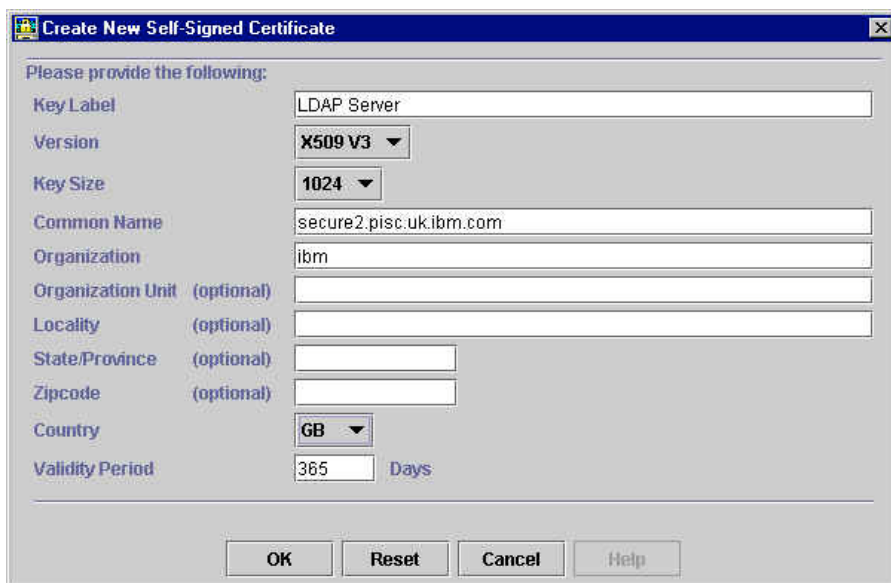
d. Click on 'OK'; an information message will inform you where the password has been saved:



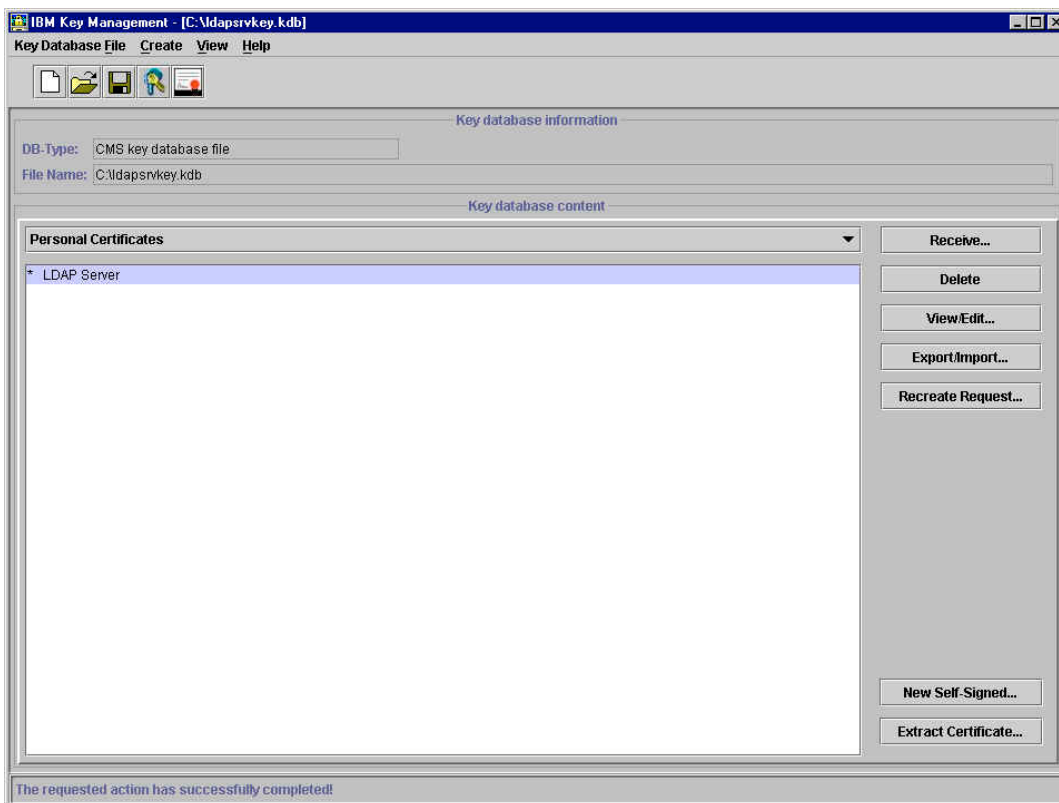
e. Click on 'OK'; information about the key database just created will be displayed at the top of the panel:



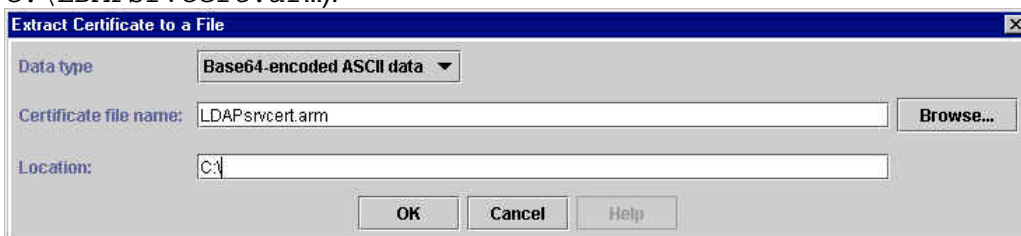
- f. Next create a self-signed certificate for the LDAP Server. Click on Create -> New Self-Signed Certificate.
- g. The 'Create New Self-Signed Certificate' panel will be displayed. Type a name in the 'Key Label' field that GSKit can use to identify this new certificate in the Key Database (we used LDAP Server). Specify a Common Name and Organization (in our case secure2.pisc.uk.ibm.com and ibm) and specify the country (in our case we used GB)



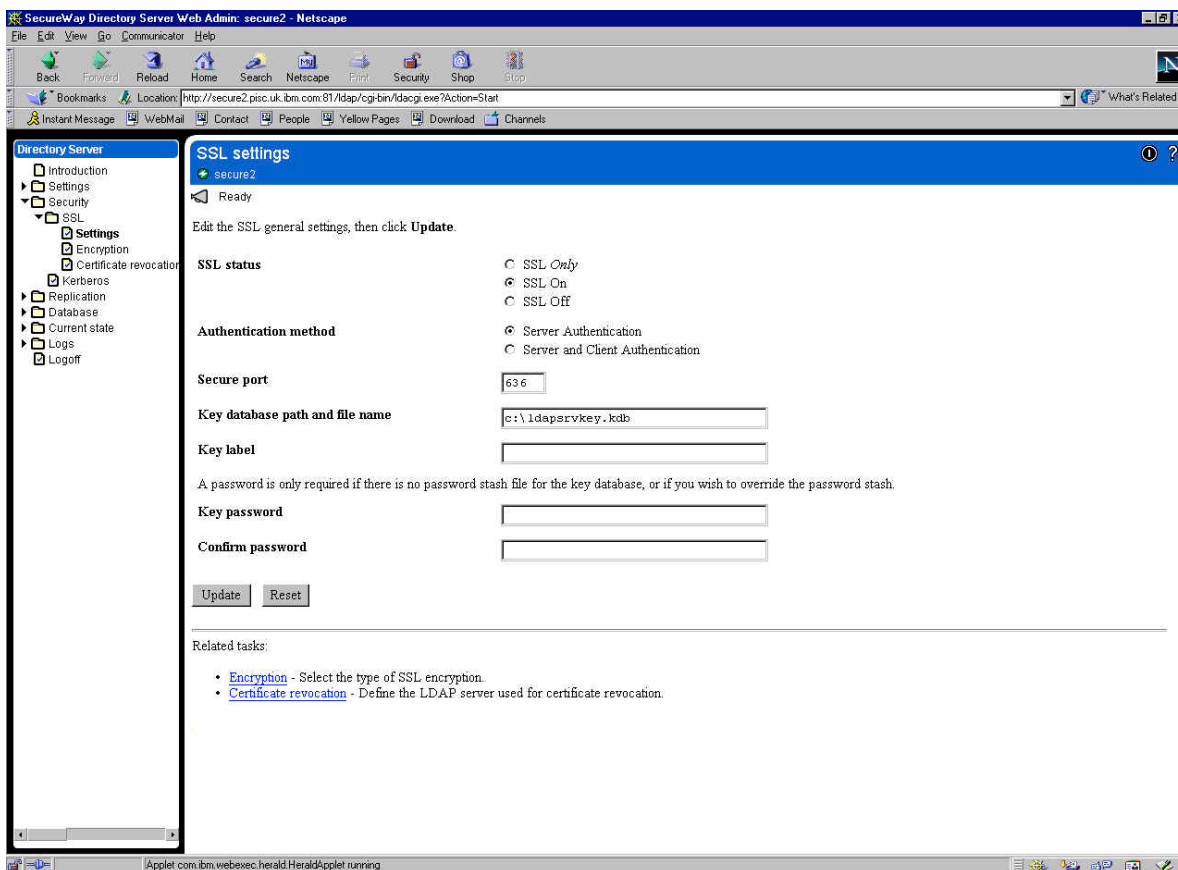
- h. Click on 'OK'. A public/private key pair is generated and certificate created. The certificate just created will appear in the list of 'personal certificates'



- i. Next, the LDAP server’s certificate needs to be extracted to a Base64-encoded ASCII data file. Highlight the certificate that has just been added to the database and click on ‘Extract Certificate...’ which is bottom right on the panel.
- j. The ‘Extract Certificate to a File’ panel will be displayed. Specify the ‘Data type’ as Base64 - encoded ASCII data and specify a filename and directory (we used C:\LDAPsrvcert.arm):



- k. Click on ‘OK’.
- l. Copy the .arm file you have just created to the LDAP Client machine (in other words the Policy Director Server component machine, for instance the WebSEAL machine).
- m. On the LDAP server machine, point a web browser at <http://servername:port number/ldap> and log on as the administrator.
- n. Clicking on *Security* → *SSL* → *Settings*, you will be presented with the LDAP SSL options.



- o. Click on 'SSL On' if you want the LDAP Server to support both SSL and non-SSL access, or 'SSL Only' if you want the LDAP Server to support SSL only. Leave 'Authentication method' as Server Authentication and specify the key database path and file name (C:\ldapsrvkey.kdb in our case).
- p. Click on 'Update'.
- q. Click on 'restart the server' to restart the LDAP server and allow this change to take effect.
- r. To test that SSL has been enabled, run the following command from a command line at the LDAP server:

```
ldapsearch -h servername -Z -K keyfile -P password -b "" -s base
objectclass=*
```

The results should look similar to the following:

```
C:\>ldapsearch -h secure2 -Z -K "c:\ldapsrvkey.kdb" -P Secure99 -b "" -s base
objectclass=*

Namingcontexts=CN=SCHEMA
Namingcontexts=OU=EMEA, O=IBM, C=GB
Namingcontexts=SECAUTHORITY=DEFAULT
Namingcontexts=CN=LOCALHOST
Subschemasubentry=cn=schema
supportedextension=1.3.18.0.2.12.1
supportedextension=1.3.18.0.2.12.3
supportedextension=1.3.18.0.2.12.5
```

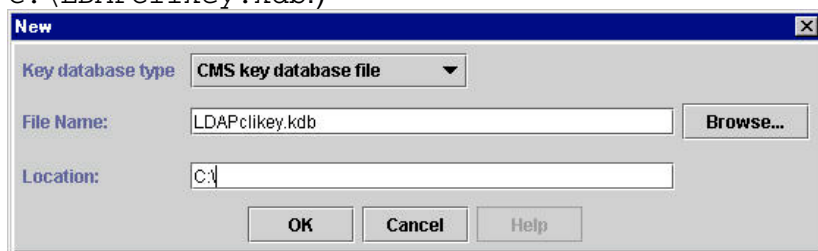
```
supportedextension=1.3.18.0.2.12.6
supportedcontrol=2.16.840.1.113730.3.4.2
supportedcontrol=1.3.18.0.2.10.5
secureport=636
security=ssl
port=389
supportedsaslmmechanisms=CRAM-MD5
supportedldapversion=2
supportedldapversion=3
ibmdirectoryversion=3.2.1
ibm-ldapservicename=secure2.pisc.uk.ibm.com
ibm-adminid=CN=ROOT
ibm-servertype=master
ibm-supportedacimechanisms=1.3.18.0.2.26.2
```

## LDAP Client (Policy Director Server components) - create the key database file

- a. On the LDAP Client machine, start the IBM Key Management tool (gsk4ikm):

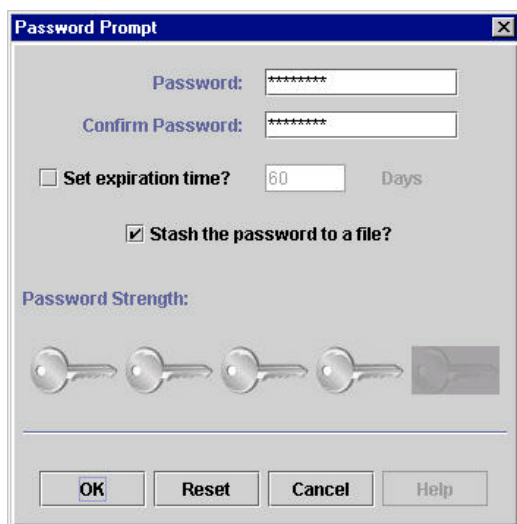


- b. Click on Key Database File -> New; verify that the 'Key database type' is CMS key database file, and specify a filename and path for the CMS Key Database. (We used C:\LDAPclikey.kdb.)



- c. Click on 'OK'. The 'Password Prompt' panel will be displayed. Enter a password (twice) (we used `secure99`) and check the 'Stash the password to a file?' box:

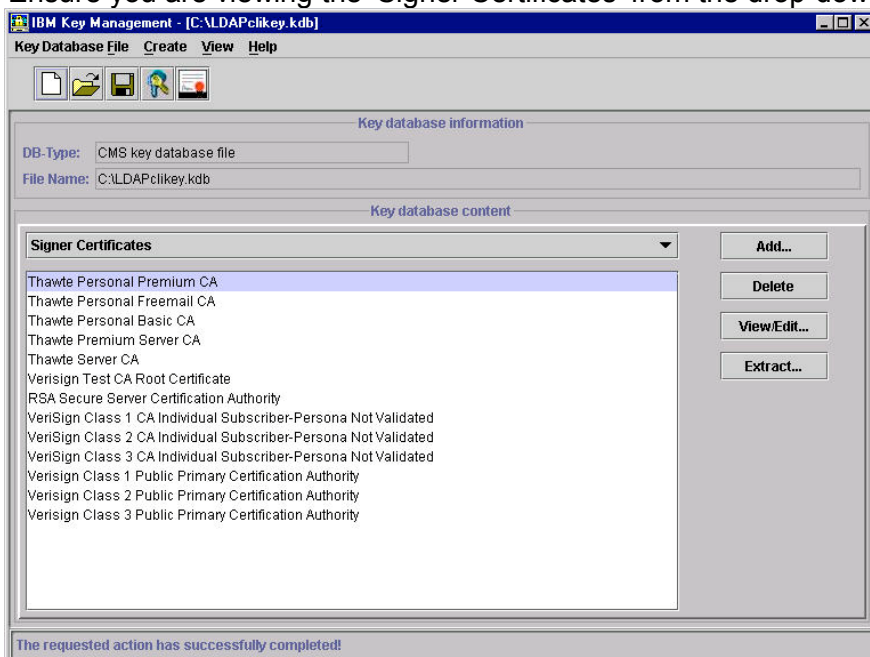




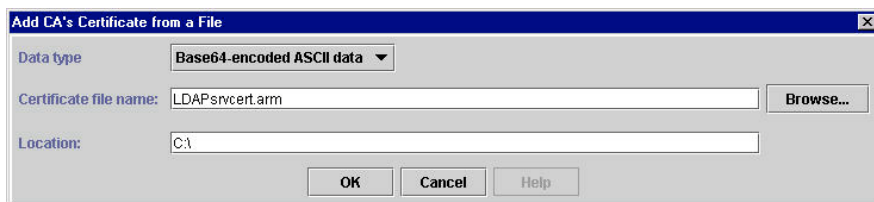
- d. Click on 'OK'; an information message will be inform you where the password has been saved:
- e. Click on 'OK'.

## LDAP Client (Policy Director Server) - install LDAP Server certificate

- a. Ensure you are viewing the 'Signer Certificates' from the drop-down menu:



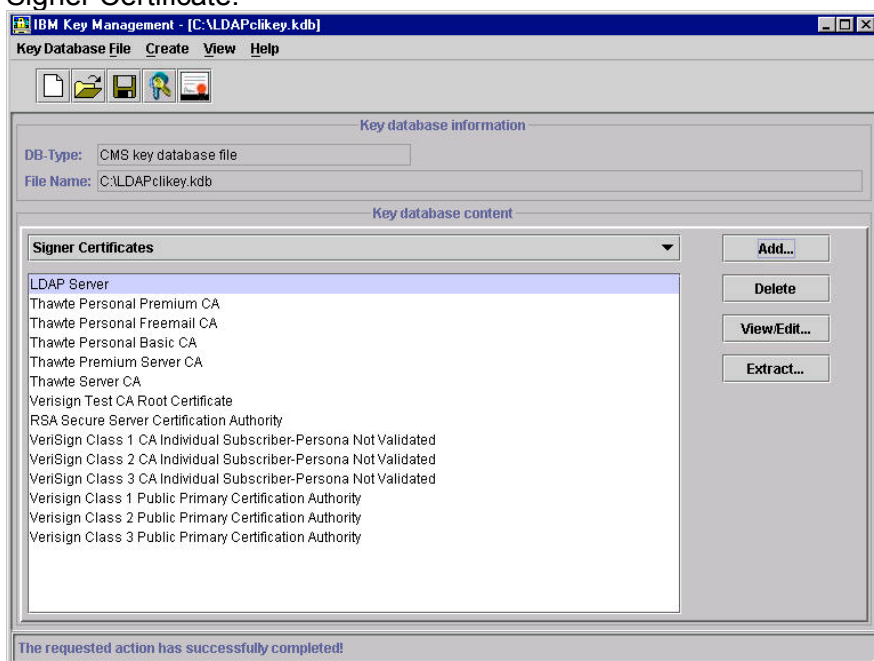
- b. Click on 'Add...': the 'Add CA's Certificate from a File' panel will be displayed. Select the data type as Base64-encoded ASCII data, and specify the name and location of the .arm file which you extracted from the LDAP server: (c:\LDAPsrvcert.arm in our case)



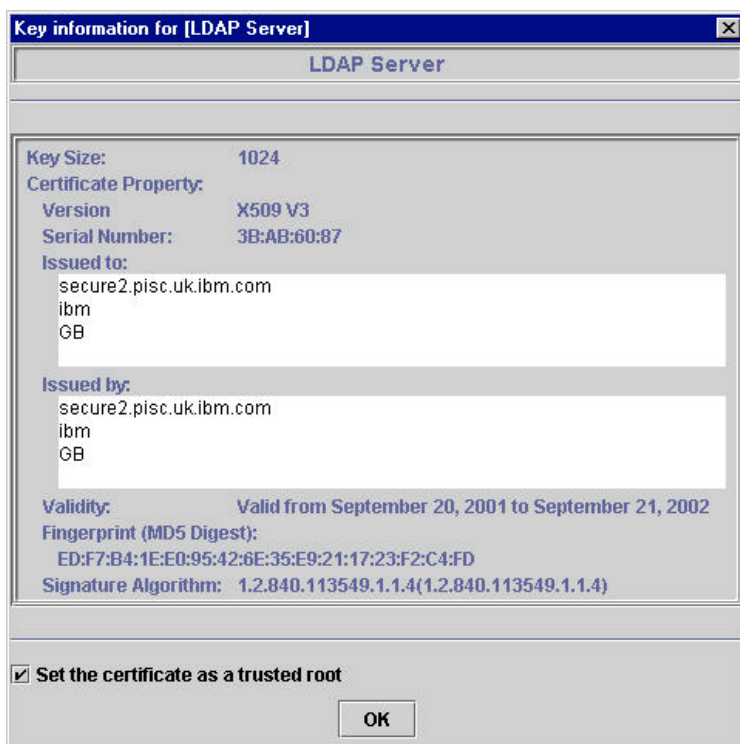
- c. Click on 'OK'; the 'Enter a Label' panel will be displayed. Specify a label for the signer certificate that you are adding. (We used LDAP Server; alternatively you might like to use the machine name of the LDAP server.)



- d. Click on 'OK'; the LDAP Server self-signed certificate appears in the client's Key Database as a Signer Certificate:



- e. Highlight the newly added Signer Certificate and click on 'View/Edit...'. Ensure that it is marked as a trusted root by making sure that 'Set the certificate as a trust root' tick box is selected:



f. Click on '**OK**' to dismiss the dialogue.

g. To test that SSL communication is working correctly between the LDAP Client and Server, run the following command from a command line at the client machine

```
ldapsearch -h LDAP servername -Z -K client keyfile -P password -b "" -s base objectclass=*
```

h. The results should look similar to the following:

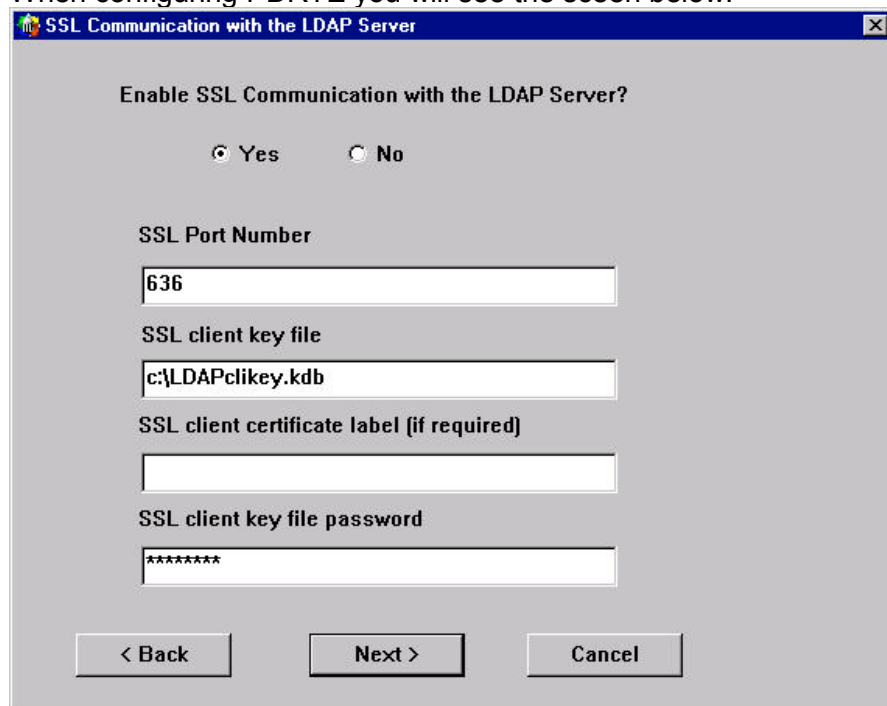
```
C:\>ldapsearch -h secure2.pisc.uk.ibm.com -Z -K "c:\LDAPclikey.kdb" -P Secure99
-b "" -s base objectclass=*

Namingcontexts=CN=SCHEMA
Namingcontexts=OU=EMEA,O=IBM,C=GB
Namingcontexts=SECAUTHORITY=DEFAULT
Namingcontexts=CN=LOCALHOST
Subschemasubentry=cn=schema
Supportedextension=1.3.18.0.2.12.1
Supportedextension=1.3.18.0.2.12.3
Supportedextension=1.3.18.0.2.12.5
Supportedextension=1.3.18.0.2.12.6
Supportedcontrol=2.16.840.1.113730.3.4.2
Supportedcontrol=1.3.18.0.2.10.5
Secureport=636
Security=ssl
port=389
supportedsaslmmechanisms=CRAM-MD5
supportedldapversion=2
supportedldapversion=3
ibmdirectoryversion=3.2.1
ibm-ldapservicename=secure2.pisc.uk.ibm.com
ibm-adminid=CN=ROOT
ibm-servertype=master
ibm-supportedacimechanisms=1.3.18.0.2.26.2
```

## Configuring PDRTE for SSL communication to LDAP

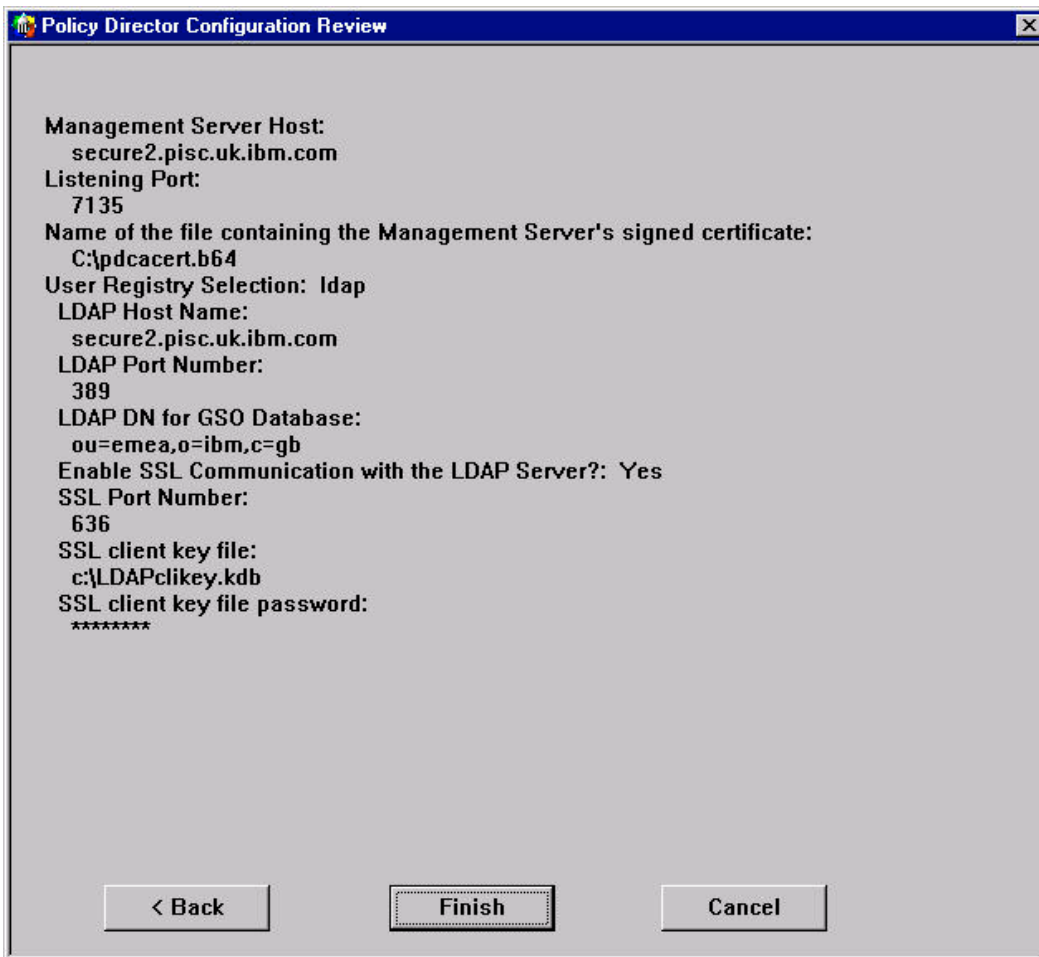
If you wish to use SSL communication between PD components such as WebSEAL and LDAP then you will need to make this decision as you configure the PDRTE. This will mean a couple of different choices than those described in the earlier chapters.

When configuring PDRTE you will see the screen below.



The screenshot shows a dialog box titled "SSL Communication with the LDAP Server". The main question is "Enable SSL Communication with the LDAP Server?". There are two radio buttons: "Yes" (which is selected) and "No". Below this are four text input fields: "SSL Port Number" (containing "636"), "SSL client key file" (containing "c:\LDAPclikey.kdb"), "SSL client certificate label (if required)" (empty), and "SSL client key file password" (containing "\*\*\*\*\*"). At the bottom are three buttons: "< Back", "Next >", and "Cancel".

- a. Specify 'Yes' to the question do you want to enable SSL communication with the LDAP Server. Enter the port number (we used the default) and enter the path and filename of the SSL client key file (in our case c:\LDAPclikey.kdb). Enter the SSL client key file password (**Secure99** in our case) and click '**Next**'. You will see the summary screen below.



- a. Click 'Finish', the PDRTE is configured.
- b. You can then continue and configure any remaining PD servers that you need that will then communicate via this PDRTE to LDAP.

---

## 23. Installation of SecurID token support

**Note:** this section needs to be revised for Policy Director 3.8.

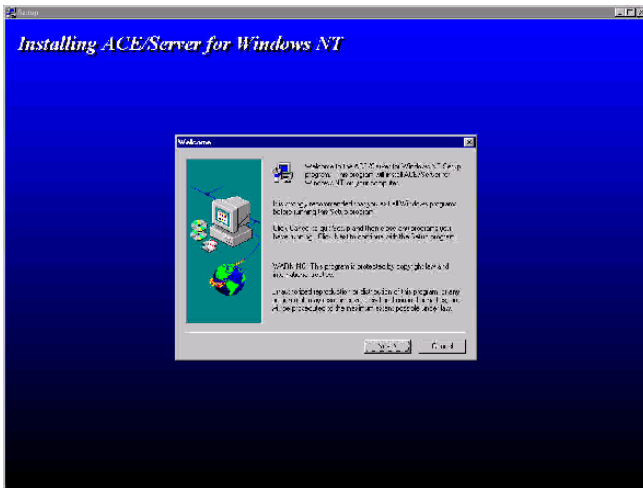
Grateful acknowledgement to Jorge Ferrari, from the WW Security Competency Center, and David Winters - this section is based on their work. This section describes the installation of the SecurID ACE/Server to support Policy Director 3.6 token authentication in a Windows NT environment. The ACE/Server is installed in the same machine where Policy Director is installed - this is an unlikely situation in real world, but it is useful for demonstration purposes. (Refer to the Policy Director red book for a description of how to install the ACE/Server on a machine remote from WebSEAL.)

This assumes that assume you are using the ACE/Server package from Security Dynamics which was supplied with the SecureWay Boundary Server (SBS), so you have:

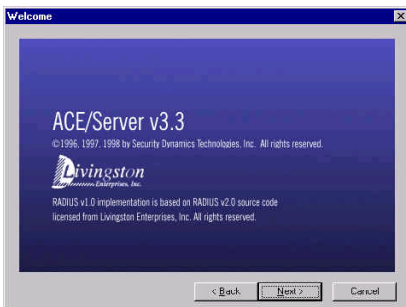
- CD-ROM with the ACE/Server 3.3.1
- CD-ROM with the ACE/Agent CD 4.3 (not used in this installation)
- Diskette with the ACE/Server license code
- Diskette with the tokens record (token Seed Kit), and
- Two SecurID tokens

This also assumes that you have a working Policy Director 3.6 running on NT.

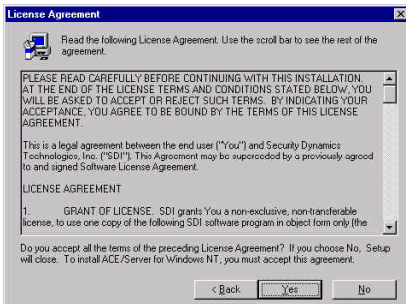
- a. Log in as a Windows NT administrator.
- b. If there is any possibility of the ACE/Server having been previously installed on the machine, delete the file `C:\WINNT\system32\securid`. (This file contains a secret which is used for the cryptographic protection of communication between the ACE client and server.) *You might also want to ensure that the `\ace` directory is deleted (to remove any existing ACE/Server configuration data).*
- c. Insert the ACE/Server V3.3.1 CD-ROM into the CD drive.
- d. Insert the diskette labelled "ACE/Server V3.3.1 2 User Promo License" into the diskette drive.
- e. Using 'My Computer' find the `\aceserv\nt_i386` directory on the CD, and double click on `setup.exe`. An ACE/Server window displays, followed by the Welcome screen:



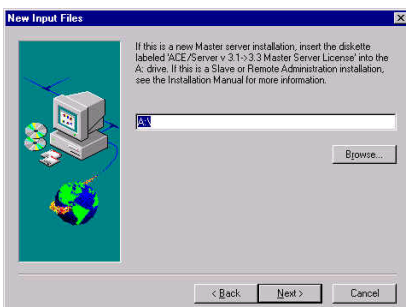
f. Click on **'Next'**. A further Welcome screen will be displayed:



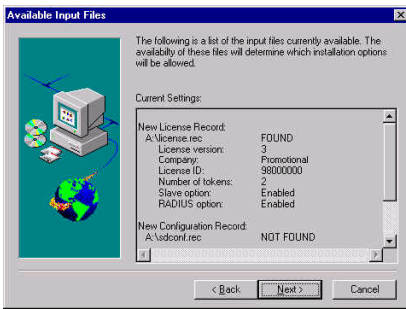
g. Click on **'Next'**. The License Agreement screen will be displayed:



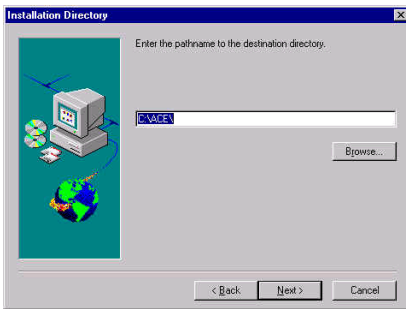
h. Click on **'Yes'**. A 'New Input Files' screen will be displayed. Ensure that the diskette labelled "ACE/Server V3.3.1 2 User Promo License" is inserted in the diskette drive specified.



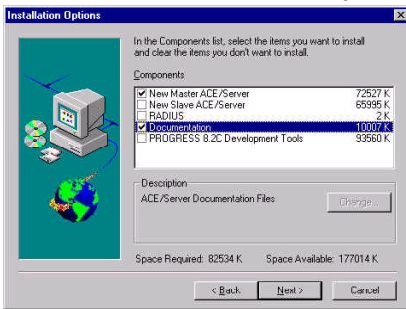
i. Click on **'Next'**. The 'Available Input Files' screen will be displayed:



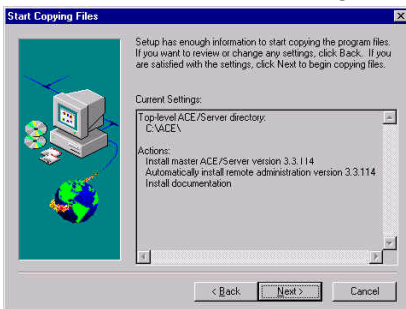
j. Click on **'Next'**. The **'Installation Directory'** screen will be displayed:



k. Click on **'Next'**. The **'Installation Options'** screen will be displayed. Select **'New Master ACE/Server'**, and optionally select **'Documentation'**:

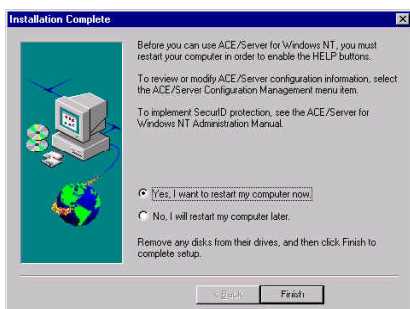


l. Click on **'Next'**. The settings specified will be displayed:

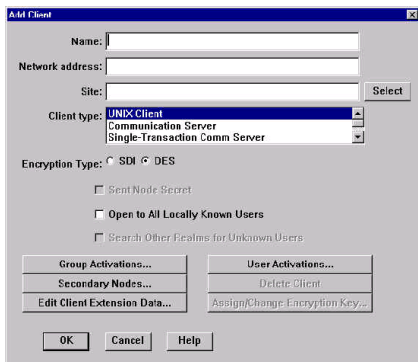


m. Review the settings and click on **'Next'**. The files will be copied across and the **'Installation Complete'** screen will be displayed:

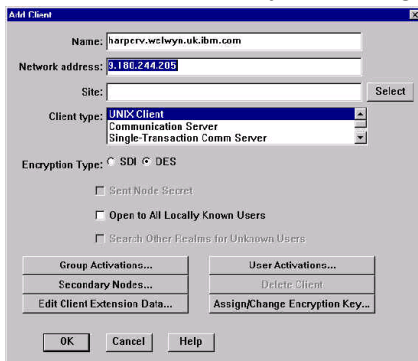




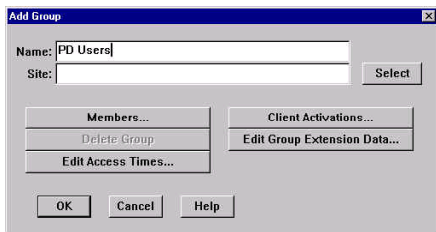
- n. Remove the diskette from the diskette drive. Click on 'Finish'. The system will re-start.
- o. Issue Start -> Programs -> ACE Server -> Database Administration - Host Mode. From the menu bar select Client -> Add Client.... The 'Add Client' panel will be displayed:



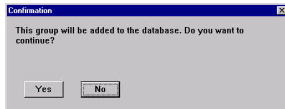
- p. Enter the name of the Policy Director machine in the Name field. When you press Tab to exit the Name field, the IP address of the Policy Director machine will automatically be displayed in the Network address field, based on the information you have in your DNS server or local hosts file. Select a Client type of Single-Transaction Comm Server:



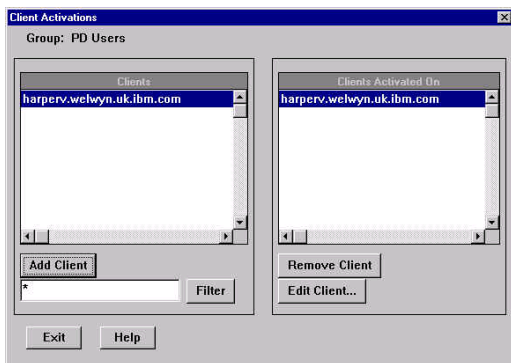
- q. Click on 'OK'. You will be returned to the ACE/Server Administration screen.
- r. From the menu bar, select Group -> Add Group.... The 'Add Group' panel will be displayed. Enter the name of the group you want to activate at the client - in our case we created the group PD Users:



s. Click on 'Client Activations...'. A confirmation message will be displayed:



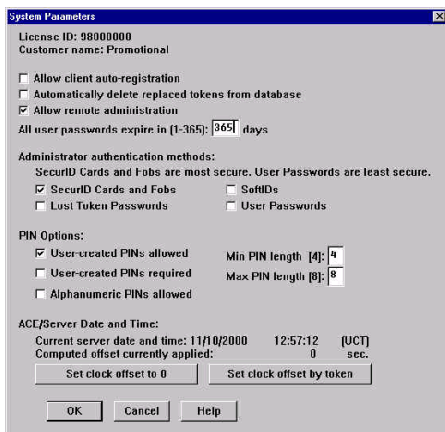
t. Click on 'Yes'. A 'Client Activations' panel will be displayed. Ensure that the Policy Director machine is highlighted under 'Clients', and click on 'Add Client'. The Policy Director machine will be added to the list under 'Clients Activated On':



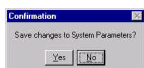
u. Click on 'Exit'.

v. The 'Edit Group' dialog will be displayed again. Click on 'OK'.

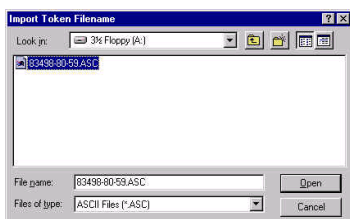
w. Click on System -> Edit System Parameters.... A 'System Parameters' panel will be displayed. Deselect 'User-created PINs allowed' (since Policy Director does not support the user creating his/her PIN number). You may also like to change the password expiry value from 90 days to some other value:



x. Click on 'OK'. A confirmation message is displayed:



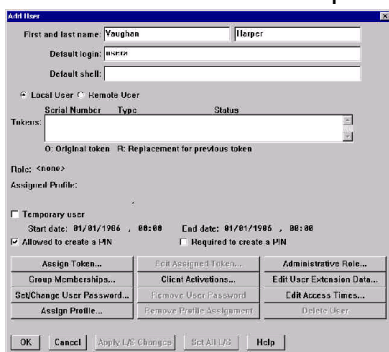
- y. Click on 'Yes'. You will be returned to the ACE/Server Administration screen.
- z. From the manu bar, click on Token -> Import Tokens.... An 'Import Token Filename' panel will be displayed. Insert the diskette containing the SecurID seed values (whose label includes a batch name, a specification of two Records, and the file name specifications) in the diskette drive. Select the file on the floppy disk:



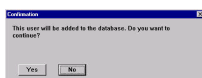
- aa. Click on 'Open'. The 'Import Status' panel will be displayed:



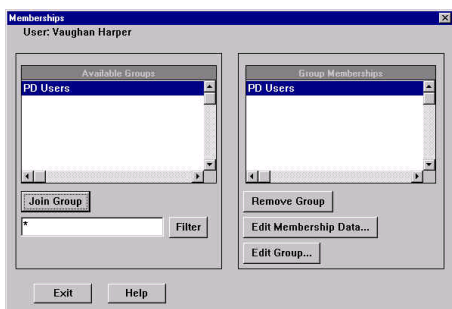
- bb. Click on 'OK'. You will be returned to the ACE/Server Administration screen.
- cc. On the menu bar select on User -> Add User.... The 'Add User' panel will be isplayed. Specify a First and Last name for the user, together with the Default login. Note that the Default login must match the User ID specified in the Policy Director Console:



- dd. Click on 'Group Memberships...'. A Confirmation message will be displayed:



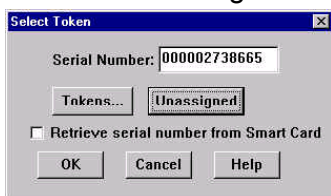
- ee. Click on 'Yes'. The 'Memberships' panel will be displayed. Ensure that the user group created is highlighted under 'Available Groups', and click on 'Join Group'. The group will be added to the list under 'Group Memberships':



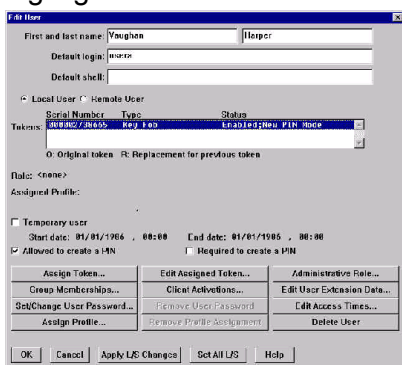
- ff. Click on 'Exit'. The 'Edit User' panel will be displayed again.
- gg. Click on 'Assign Token...'. The 'Select Token' panel will be displayed:



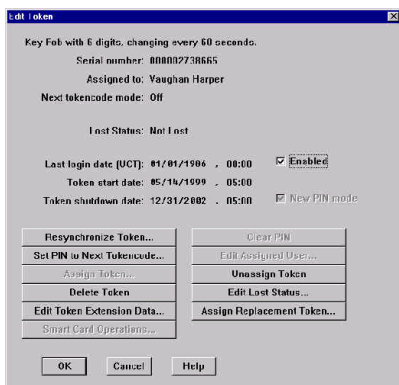
- hh. Click on 'Unassigned'. A SecurID Serial Number will be displayed in the 'Select Token' panel:



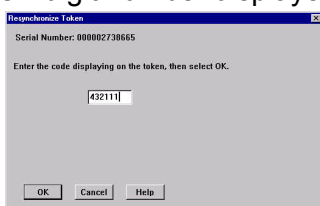
- ii. Click on 'OK'. The 'Edit User' panel will be displayed again, this time with a token specified. Highlight the token:



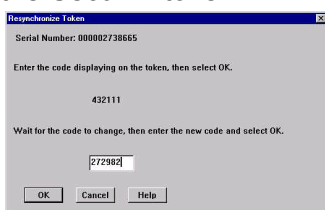
- jj. Find the actual SecurID token whose serial number matches that displayed.
- kk. Click on 'Edit Assigned Token...'. The 'Edit Token' panel will be displayed:



ll. Click on 'Resynchronize Token...'. The 'Resynchronize Token' panel will be displayed. Key the six digit number displayed by the SecurID token:



mm. Click on 'OK'. Wait for the display to change, then key the new six digit number displayed by the SecurID token:



nn. Click on 'OK'. A message should indicate that the token has been successfully resynchronized:



oo. Click on 'OK'. The 'Edit Token' panel will be displayed again.

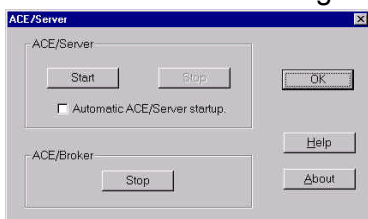
pp. Click on 'Set PIN to Next Tokencode...'. The 'Set PIN to Next Tokencode' panel will be displayed. Enter the Key the six digit number displayed by the SecurID token:



qq. Click on 'OK'. A message indicating that the PIN will be the first 4 digits of the next tokencode:



- rr. Click on '**OK**'. The 'Edit Token' panel will be displayed again.
- ss. Wait for the display to change: the PIN for the SecurID token will be first four digits of the new six digit number displayed by the SecurID token. (In our case the next displayed value was 789538, so the PIN is therefore 7895.) Ensure that you note this PIN value.
- tt. Click on '**OK**' to close the 'Edit Token' window. The 'Edit User' window will be displayed.
- uu. Click on '**OK**' to close the 'Edit User' window. You will be returned to the ACE/Server Administration screen.
- vv. **Copy the ACE/Server configuration file `sdconf.rec` from the `\ACE\data` directory to the `\WINNT\system32` directory.** (This file will tell CDAS what encryption to use to communicate with the ACE/Server and where the server is located.)
- ww. Copy the file `aceclnt.dll` from the `\ACE\prog` directory to the `\WINNT\system32` directory.
- xx. Click on 'Start -> Settings -> Control Panel. Double-click on the ACE Server icon:



- yy. Click on 'Start'. A message indicating that the ACE/Server has been started will be displayed:



- zz. Policy Director `iv.conf` changes:
  - a) Activate forms-based login: in the `[wand]` stanza ensure that the `https-forms-auth` entry is set to `yes`.
  - b) Specify the Token Login Prompt - you must specify a special login form appropriate to this token-based authentication process. Activate the token login prompt page (HTML) by changing:

```
pkms-login-error-page = login.html
#pkms-login-error-page = tokenlogin.html
```

to:

```
#pkms-login-error-page = login.html
pkms-login-error-page = tokenlogin.html
```

c) In the [wand] stanza ensure that the `verify-clients` entry is set to either `optional` or `never`. (Otherwise a client would be forced to use certificate based authentication.)

d) Enable the token CDAS by adding the following line to the [authentication-mechanisms] stanza. For Windows NT the entry is as follows:

```
token-cdas=cdasauthn.dll&entry=../../subsys/intraverse/cdas/server/token/<hostname>
```

For Solaris the entry is:

```
token-cdas= libcdasauthn.so&entry=../../subsys/intraverse/cdas/server/token/<hostname>
```

For AIX the entry is:

```
token-cdas=libcdasauthn.a &entry=../../subsys/intraverse/cdas/server/token/<hostname>
```

aaa. Start DCE, and ensure that all the correct DCE services are running.

bbb. Log in to DCE.

ccc. Perform the DCE configuration required by the token CDAS server:

a) Change directory to `C:\Program Files\Tivoli\Policy Director\cdas_server\bin`

b) At the MS-DOS prompt, issue:

```
cdas_dce_setup <hostname> token <cell-admin-password>
```

c) (Although not relevant to this chapter, the equivalent steps on a UNIX platform involve using a shell script located in the following directory:

```
/opt/intraverse/cdas_server/bin. The following command needs to be entered: #  
sh ./cdas_setup.sh <hostname> token <cell-admin-password>.)
```

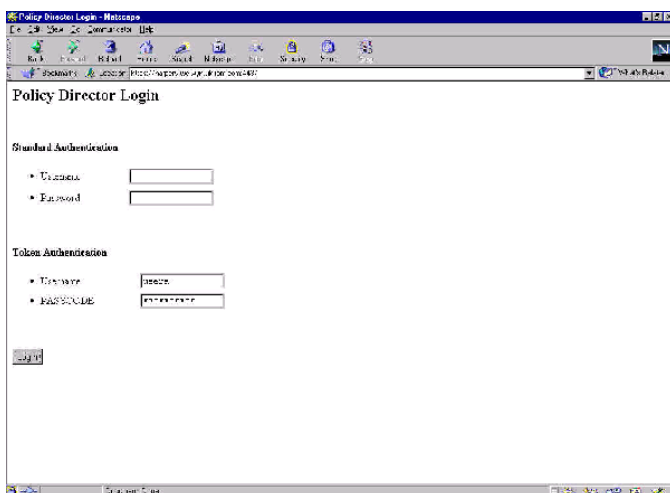
ddd. Start Policy Director, LDAP (if required) etc, and ensure that all the correct services are running.

eee. Start the Token CDAS server. You can do this in one of two ways:

- ◆ In an MS-DOS window change directory to `C:\Program Files\Tivoli\Policy Director\cdas_server\bin` and enter `cdas_server -h <hostname> -r <registry>`

- ◆ Start service from Start -> Settings -> Control Panel, double-click on Services, select Cross Domain Token Authentication Service and click on Start.

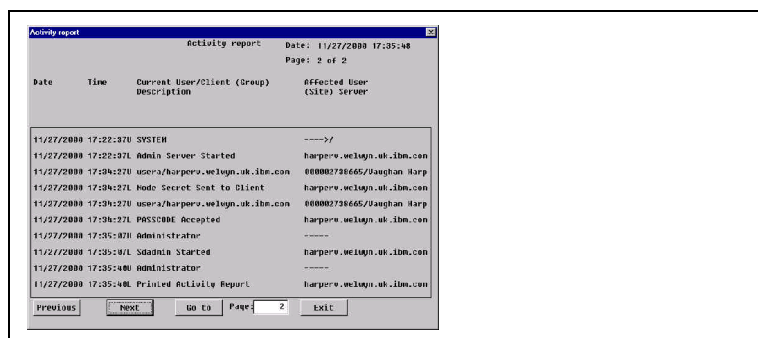
fff. Point a browser at a web page which requires authentication and click on Re-access the page using HTTPS. The token login web page will be displayed. In the Token Authentication Username field key the Policy Director User ID which matches the Default login configured to at the ACE/Server administration screen. In the PASSCODE field type the four digit PIN followed by the six digit SecurID display:



ggg. Clicking on 'Login' should result in successful authentication.

## Problem Determination

In the event of token authentication failing, it is often worth looking at the ACE/Server log. To do this, use Start -> Programs -> ACE Server -> Database Administration - Host Mode, then Report -> Activity. Successful token authentication will result in a report similar to the following:



## Uninstalling

### Problem:

When you uninstall the WebSEAL component of Policy Director 3.6 - that has been configured with the default token (SecurID) CDAS server - the token CDAS server is not removed from the system.

a. Workaround:



You must perform the following steps to manually remove the token CDAS server **before** you begin the normal WebSEAL uninstall procedure. (These steps must be performed as a Windows NT administrator.)

- b. From the Windows NT Services panel, shut down the token CDAS server by selecting "Cross Domain Token Authentication Service" and click the Stop button.
- c. From the Windows Command Prompt, enter the following commands to manually remove the token CDAS server component:  
MSDOS> dce\_login cell\_admin <password>  
MSDOS> cdas\_dce\_remove.exe <host> token  
Where host is the name of the machine where the token CDAS server resides.
- d. You can now start the normal WebSEAL uninstall procedure.

## 24. Sharing an LDAP Directory between Policy Director and Trust Authority

**Note:** This section is very old, and is certainly not definitive: it is left in just in case it may be of use. It gives some notes regarding setting up an LDAP Directory so that it can be shared between Policy Director and Trust Authority.

- a. TA & PD each have their own LDAP requirements, all of which must be met for the products to use the same LDAP Directory successfully.
- b. We set up LDAP for PD first; however this meant installing some of the required software at the levels required by TA. Refer to TA Installation Guidelines document, and elsewhere in this document, for the default steps.
- c. On the LDAP Server, perform the following steps:
  - a) Install DB2 EE as per the Trust Authority Installation Guidelines document
  - b) Install DB2 FP10 as per the Trust Authority Installation Guidelines document
  - c) Install LDAP as per this document
- d. Now follow this document and install the remainder of PD as normal on the same or another machine.
- e. PD should now be up and running, using the LDAP Server.
- f. Now for the TA bit: install the TA server as normal until after you have run the post install configuration, as per the Trust Authority Installation Guidelines document.
- g. Now set up the LDAP server machine as follows:
  - a) On the LDAP server install the JDK 1.1.6 as per the Trust Authority Installation Guidelines document.
  - b) Install IBM SecureWay Directory Server Support (part of the TA install).
  - c) Copy the `V3.Modifiedschema.ta` file from the Trust Authority install directory to the location of your LDAP Directory, as follows:  

```
copy c:\Program Files\IBM\Trust Authority\cfg\V3.Modifiedschema.ta
yourDirectoryPath\etc
```
  - d) The `V3.Modifiedschema.ta` file contains the schema definitions for the Trust Authority object classes `pkiUser` and `PKiCA`
  - e) Edit the existing `slapd.conf` file located in `yourDirectoryPath\etc` to add the following lines:  

```
includeSchema /etc/V3.Modifiedschema.ta
suffix "c=us"
```
  - f) Stop and re-start the LDAP server to make use of these new settings.
- h. Start the Setup Wizard to configure the TA server machine from your chosen browser, and specify configuration values until they are complete.
- i. From the TA server run `CfgStart -i` as normal, but this time `cfgstart` will stop at the point when the LDAP server needs to be configured.
- j. At this point go to the LDAP Server machine and run the TA post installation configuration (Start -> Programs -> IBM SecureWay Trust Authority -> Post Installation Configuration)

k. Next run `CfgStart -i` on the LDAP server.

l. Once this is complete go back to the TA server and run `CfgStart -i` again, this will complete the TA configuration.

m. Once complete TA can be tested in the normal way. Once you have issued a certificate you should be able to check the LDAP directory for the appropriate entry.

---

## 25. Useful LDAP commands

For a full treatment of LDAP, see the excellent red book SG24-5110 *LDAP Implementation Cookbook*. But in the meantime, the following commands may prove useful:

- `ldapsearch -h hostname -b "C=US" "objectclass=*" "*"`  
this lists all attributes for all directory entries with a base of "C=US"
- `ldapsearch -h hostname -b "C=US" "objectclass=*" "modifytimestamp"`  
this lists the time stamps for all directory entries with a base of "C=US"
- `ldapsearch -t -h hostname -b "C=US" "objectclass=*" "*"`  
useful for binary objects - this writes all attributes to files, and displays the names of the files created, for all directory entries with a base of "C=US"
- `ldapsearch -h hostname -b "" -s base "objectclass=*"`  
this lists all the base objects within the directory

## 26. Troubleshooting...

This section is certainly not comprehensive, but it gives a few miscellaneous ideas that *might* help relating to fault finding/problem determination. Not every item is applicable to every platform.

### Policy Director won't start...

- a. Has LDAP started? Are the correct LDAP services running? Try issuing an `ldapsearch` from the machine in question to the LDAP directory.
- b. Have all the Policy Director servers started?

Under AIX, if you type `ps -ef |grep PolicyDirector`, the following processes should be listed: `pdmgrd`, `pdacltd` and if you type `ps -ef |grep pdweb` the following process should be listed: `webseald`.

If not, look at the appropriate log files.

If under UNIX the Policy Director servers won't start it might be worth stopping them all and then deleting any Process ID files left over (e.g. `secmgrd.pid`).

### Problems once Policy Director has started...

Depending on the nature of the problem, doing one of the following steps may help:

- Try running an IP trace between WebSEAL and LDAP. (See below for hints on running traces.)
- Run LDAP in debug mode. If you are using the IBM SecureWay Directory under AIX, look at Contents -> Troubleshooting -> Debugging in the *IBM SecureWay Directory for AIX Installation and Configuration guide* – this is on the **Tivoli SecureWay Policy Director Base for AIX and Linux Version 3.8** CD at `/doc/Directory/install_config_guide/aix/aparent.htm`.

You can try issuing the following:

```
ldtrc on
slapd -h 65535 2>&1 | tee ldap.out
```

This will write maximum debugging information to a file. (65535 is a bitmask value which turns on full debug output and generates the most complete information.)

(Afterwards issue `ldtrc off`)

- Try running Policy Director in debug mode.

- Try running PD services in the foreground with the '-foreground' parameter

## Page Not Found problems...

- Running Policy Director in debug mode, by specifying `logdebug=yes` in the `[wand]` stanza of `iv.conf` will result in lots of useful information being written to `...\www\log\wand_debug_log`. This includes the request from the browser to WebSEAL, the request from WebSEAL to the back-end web server, the response from the web server to WebSEAL, and the response from WebSEAL to the browser. **This is a really useful addition with PD 3.8!**
- Try running an IP trace between WebSEAL and the back-end web server.
- See whether specifying `-j` on the `junctioncp create` command helps. See whether setting up the Junction Management Table helps. **\*\*Need to update command\*\***
- If you are having cookie-related problems, you can get a whole load of useful information from Internet Explorer. To do this, switch on the warnings that IE issues whenever it is invited to set a cookie. When you get the warning you can click on 'More Info', which tells you lots of information about the cookie (Name, Domain, Path, Expires, Data, and whether or not Secure).

To switch this on, do the following:

- select Tools -> Internet Options
- click on Security
- select the correct zone for your target system (Internet, Local Intranet etc)
- click on Custom Level
- select 'Prompt' against 'Allow cookies that are stored on your computer' and 'Allow per-session cookies (not stored)'

## Running IP traces

### On AIX

- To start a trace, do the following:  
`iptrace -a -d 9.180.244.207 -b /tmp/trace207.trace`  
This will trace all traffic between the machine in question and IP address 9.180.244.207, and write this to a binary trace file (/tmp/trace207.trace).
- After the activity you want to capture, to stop the trace issue:  
`ps -ef|grep iptrace`  
to determine the PID of iptrace, then issue:  
`kill pid`  
(where *pid* is the PID which you determined in the previous step)  
(Do **not** issue `kill -9 pid`.)
- To convert the trace to a readable format, type:  
`ipreport /tmp/trace207.trace |more`  
or to write it to a file, type:  
`ipreport /tmp/trace207.trace >/tmp/trace207.report`

### On Solaris

- Type:  
`snoop -o /tmp/trace207 -v 9.180.244.207`  
This will trace all traffic between the machine in question and IP address 9.180.244.207, and write this to a trace file (/tmp/trace207).

### On NT

- The **Network Monitor** comes with Windows NT Server 4.0 but it is not installed by default. To install the monitor, go to the Control Panel, open Network, select the Services tab and click on Add. From the list of services that is displayed, select and install "Network Monitor Tools and Agent". Once the Network Monitor is installed, it is run from the Start menu [Start -> Programs -> Administrative Tools (Common) -> Network Monitor].
- This is lots of useful information on this in *Windows NT TCP/IP Network Administration*, published by O'Reilly. You can find the relevant chapter at [http://www.oreilly.com/catalog/wintcp/sample\\_chpt/tnt\\_11.html](http://www.oreilly.com/catalog/wintcp/sample_chpt/tnt_11.html).

## LDAP Problems

If you suspect LDAP problems, you can sometimes find useful information by going to Start -> Programs -> Administrative Tools (Common) -> Event Viewer, and clicking on Log -> Application.

## Policy Director Debug Mode

- You can run secmgrd by running the following command at an MS-DOS command prompt:  
`secmgrd -foreground -noservice`
- You can also switch on debugging by setting `logdebug=99` in `iv.conf`

## Other problem determination ideas - AIX

### 1. Stop PD services

```
# /etc/etc/iv stop
```

### 2. Start PD

```
#/etc/iv/iv start
```

### 3. Verify LDAP is running

```
# ps -ef | grep slapd
```

### 4. Verify PD is running

```
# /etc/etc/iv status
```



---

## 27. Publications

The majority of these publications should be read **before** reading this document! The Policy Director home page is at [http://www.tivoli.com/products/index/secureway\\_policy\\_dir/](http://www.tivoli.com/products/index/secureway_policy_dir/) (which includes a link to the technical documentation for registered users). For internal users, a link to the technical documents can be found at [http://www-internal.tivoli.com/support/public/Prodman/public\\_manuals/td/TD\\_PROD\\_LIST.html](http://www-internal.tivoli.com/support/public/Prodman/public_manuals/td/TD_PROD_LIST.html)

For Business Partners, there is information on Policy Director on TIPS at [https://www.tivoli.com/teamtivoli/tips/products/enterprise/policy\\_dir\\_doc.html](https://www.tivoli.com/teamtivoli/tips/products/enterprise/policy_dir_doc.html), and for internal users there is information on the MOT at [http://mot.tivoli.com/product\\_info/enterprise/policy\\_dir.html](http://mot.tivoli.com/product_info/enterprise/policy_dir.html).

It is worth referring to the Release Notes at one of those URLs, together with all the product documentation.

It is likely to be worth looking at the Policy Director red book:

SG24-6008      *Tivoli SecureWay Policy Director: Centrally Managing e-business Security*

In addition, there is the FirstSecure red book:

SG24-5498-00    *Understanding IBM SecureWay FirstSecure*

and the LDAP red books:

SG24-4986      *Understanding LDAP*  
SG24-5110      *LDAP Implementation Cookbook*

There is also an FAQ at <http://w3dev.austin.ibm.com/tech/faq/index.html>

And for lots of detail on SSL/TLS, try *SSL and TLS: Designing and Building Secure Systems*, by Eric Rescorla, pub. Addison-Wesley, 2000.

End of Document