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 Chattopadhya 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
Part 1	I - Introduction and Roadmaps	1
1.	Introduction	1
2.	Installation Road Maps	2
	II - Windows Environment	
3.	Windows System preparation (operating system,etc)	
4.	Easy Install	8
4.	- = = = = = = = = = = = = = = = = = = =	
4.		
4.	.3 Easy Install of Policy Director WebSEAL (PDWeb)	17
5.	Easy Install process to Set up Policy Director components on a remote machine	19
5.		
5.		
5.	.3 Changing ports for Web Portal Manager	
6.	Native installation process	
6.	1	
6.	.2 LDAP Server installation (Windows)	
6.		
6.		
6.		51
6.		
6.	5	
6.		
6.	 .9 Policy Director Configuration (Windows) .10 Policy Director RTE + WebSEAL Configuration (Windows) 	
	.10 Foncy Director KTE + webSEAL Configuration (Windows)	
	III - AIX Environment	
Part I		
7.	AIX System Preparation and general AIX Notes	90
8.	LDAP Server installation/configuration (AIX)	92
8.	.1 Operating system pre-requisites	92
8.		
8.		
8.		
8.	5 5	
8. 8.	e	
8.	5	
9.	Policy Director Server installation (AIX)	
	•	
10.	WebSEAL Installation (AIX)	
11.	Policy Director Configuration (AIX)	
12.	Useful commands for Policy Director in the AIX environment	
	LDAP	
	PD	

Policy Director Processes	
Part IV - Solaris Environment	
13. Solaris System Preparation and general Solaris Notes	
14.Easy Installation Process for Solaris14.1IBM SecureWay Directory and Prerequisite Installation and Configuration	
14.1 IDM Secure way Directory and Prefequisite Installation and Configuration	
14.3 WebSEAL Install and Configuration	
15. Policy Director Component Configuration & Unconfiguration (Solaris)	
16. Useful commands for Policy Director in the Solaris environment	
LDAP	
Directory Management Tool steps	
PD	
Solaris	
Part V - Generic Product Configuration	123
17. Initial Policy Director Validation	
18. Further Policy Director Configuration	
Directory Management Tool	
19. Query contents – additional notes	13/
<i>Query</i> contents with Lotus Domino Go Webserver	
Query contents with Netscape Enterprise Server under AIX	
~ ~ ~	
20. Setting up a WebSEAL server certificate	
Approach (b) - Certificate Signing Request sent to Tivoli PKI	
Approach (c) - Certificate Signing Request sent to Entrust CA	
Additional notes	
21. Setting up client certificate authentication	161
22. Setting up an SSL connection to the LDAP Directory	
LDAP Server - create the key database file	
LDAP Client (Policy Director Server components) - create the key database file	
LDAP Client (Policy Director Server) - install LDAP Server certificate	
Configuring PDRTE for SSL communication to LDAP	
23. Installation of SecurID token support	176
Problem Determination	
Uninstalling	
Problem:	
24. Sharing an LDAP Directory between Policy Director and Trust Authority	
25. Useful LDAP commands	
26. Troubleshooting	
Policy Director won't start	
Problems once Policy Director has started	191
Page Not Found problems.	
Running IP traces	
LDAP Problems Policy Director Debug Mode	
Other problem determination ideas - AIX	

27.	Publications	.19	5
-----	--------------	-----	---

Version 0.8 - 21 September, 2001

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.)

Combination (i) – Policy Director Servers, IBM SecureWay Directory (LDAP), WPM and WebSEAL			
Components required:			
 GSKit IBM HTTP Server IBM SecureWay Directory Policy Directory Servers WebSEAL 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, pdweb) Re-boot Configure LDAP Configure Policy Director Server packages (pdrte, pdmgrd, pdacld, pdweb) 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 			

 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 Policy Director Server packages (pdrte, pdmgrd, pdacld) Re-boot Configure DAP Configure Policy Director Server packages (pdrte, pdmgrd, pdacld) Install and Configure Web Portal Manager (WPM) Sequence of steps to follow on AlX/Solaris: Install 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 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)
 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 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)
 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)
 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)
 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)
 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)
 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)
 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)
 pdacld) Re-boot Configure LDAP Configure Policy Director Server packages (pdrte, pdmgrd, pdacld) Install and Configure Web Portal Manager (WPM)
 Configure LDAP Configure Policy Director Server packages (pdrte, pdmgrd, pdacld) Install and Configure Web Portal Manager (WPM)
 Configure Policy Director Server packages (pdrte, pdmgrd, pdacld) Install and Configure Web Portal Manager (WPM) Sequence of steps to follow on AIX/Solaris:
pdmgrd, pdacld) • Install and Configure Web Portal Manager (WPM) Sequence of steps to follow on AIX/Solaris:
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 Ser Web Portal Manager insta Web Portal Manager (WPM 	allation process)	
 Sequence of steps to follow of Install GSKit Install IBM HTTP Server Install LDAP Client Install Policy Director Serve pdacld) Re-boot Configure Policy Director Serve pdmgrd, pdacld) Install and Configure Web F 	r packages (pdrte, pdmgrd, erver packages (pdrte,	
Sequence of steps to follow of Install GSKit Install IBM HTTP Server Install LDAP Client Install Policy Director packa Configure Policy Director packa	ges	

Combination (iv) – WebSEAL only		
Components required:		
• GSKit • LDAP Client • WebSEAL		
Sequence of steps to follow on Windows:		
 Install GSKit Install LDAP Client Install WebSEAL Re-boot Configure WebSEAL 		
Sequence of steps to follow on AIX/Solaris:		
 Install WebSEAL (including pre-requisite packages – this pulls in GSKit and LDAP Client) Configure WebSEAL 		

Combination (v) – IBM SecureWay Directory (LDAP) only

Components required:

- GSKit
- IBM HTTP Server
- IBM SecureWay Directory

Sequence of steps to follow on Windows:

- Install GSKit
- Install IBM HTTP Server
- Install LDAP Server
- Re-boot
- Configure LDAP

Sequence of steps to follow on AIX/Solaris:

- Install GSKit
- Install IBM HTTP Server
- Install LDAP Server
- Configure LDAP Server

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 '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_ldap_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_ldap_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...

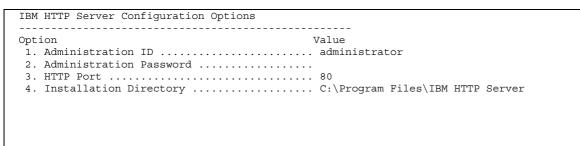
d. This shows the current status of the components required for IBM SecureWay Directory. Press '**Enter**'. The DB2 Configuration options are displayed

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

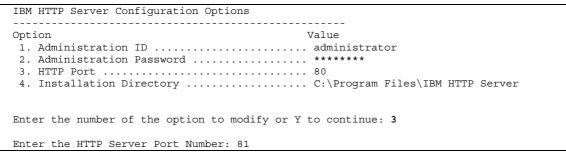
Enter the number of the option to modify or Y to continue:

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



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.



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.

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

Version 0.8 – 21 September, 2001

Enter the number of the option to modify or Y to continue: ${\boldsymbol{y}}$

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 ..... PDLDAP
9. Installation Directory ..... C:\Program Files\IBM\LDAP
Enter the LDAP Administrator Password: *******
Re-enter the password for confirmation: *******
```

I. Enter the password to be used for the LDAP Admin user (cn=root). Type again to confirm. (We used Secure99.)

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
      PDLDAP

      9. Installation Directory
      C:\Program Files\IBM\LDAP
```

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...
```

 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
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 se 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]

IBM SecureWay Directory Server ..... Configured [3.2]

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\EZINSTALL.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

Version 0.8 - 21 September, 2001

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).

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.

Tiv	oli SecureWay Policy Director Runtime Configuration Options
Opt	ion Value
1.	Configure Using This Registry Type ldap
2.	LDAP Server Hostname secure2.pisc.uk.ibm.com
3.	LDAP Server Port
4.	Suffixo=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
10.	Installation Directory C:\Program Files\Tivoli\Policy Director

Enable SSL with LDAP Server? [Y $\mid N$]:

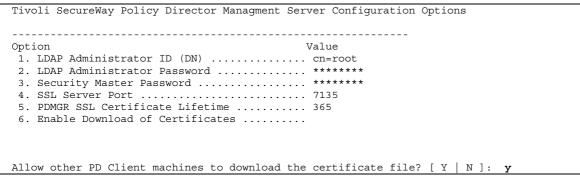
f. At this point you must decide if you will use SSL for communication with the LDAP Server. For this basic install we'll keep things simple by NOT using SSL. The Policy Director Management Server Configuration Options screen is re-displayed.

Version 0.8 - 21 September, 2001

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).

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



- 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 \mid N]:
```

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 IBM Global Security Toolkit 4 IBM SecureWay Directory Client Tivoli SecureWay Policy Director Runtime Tivoli SecureWay WebSEAL Server	Configured Configured	[3.2] [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

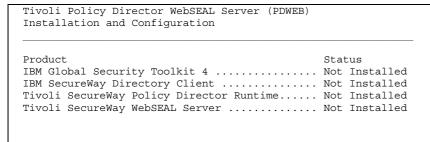
This section describes using the scripts to install the WebSEAL and then the WPM and their prerequisites on separate systems.

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:



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.

Enter the number of the option to modify or ${\tt Y}$ to continue: ${\tt y}$

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



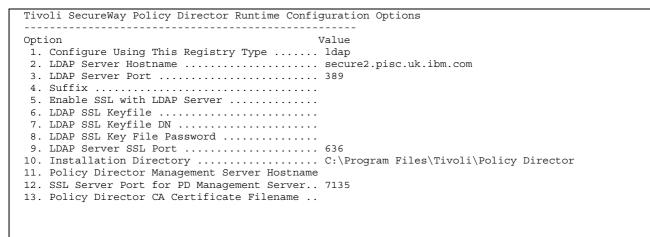
Enter the number of the option to modify or Y to continue: \boldsymbol{y}

 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
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
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).



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.)

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

Enable SSL with LDAP Server? [Y $\mid N]$:

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.

Version 0.8 - 21 September, 2001

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: *******

I. Enter the Password you configured for sec_master during the PD Management Server installation (we used Secure99).

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 IBM Global Security Toolkit 4 IBM SecureWay Directory Client Tivoli SecureWay Policy Director Runtime Tivoli SecureWay WebSEAL Server	Not Installed Not Installed
Installing IBM Global Security Toolkit.	
Tivoli Policy Director WebSEAL Server (PDWEB) Installation and Configuration	
Product IBM Global Security Toolkit 4 IBM SecureWay Directory Client Tivoli SecureWay Policy Director Runtime Tivoli SecureWay WebSEAL Server	Configured [3.2] Installed [3.8]
Installing Policy Director WebSEAL Server.	
To complete the installation/configuration, the Press ENTER to continue	e system must be restarted

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.

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...

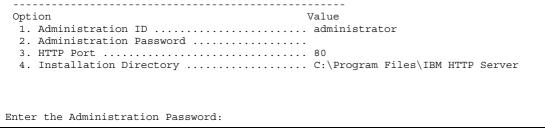
d. Press 'ENTER' to continue. You will see the IBM Global Security Toolkit options displayed

```
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



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

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 Administration ID Administration Password HTTP Port Installation Directory 	******** 80
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 1. Installation Directory	Value C:\Program Files\IBM\LDAP

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

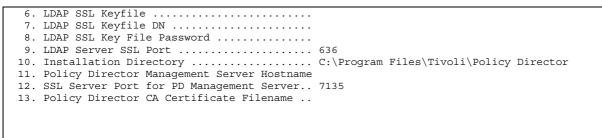
i. Enter 'y' to continue. The PD runtime configuration is displayed.

Tivo	voli SecureWay Policy Director Runtime Configura	tion Options
Opt:	tion Valu	.e
1.	. Configure Using This Registry Type lda	p
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 713	5
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).

Version 0.8 - 21 September, 2001



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 Configurat	ion Options
Option Value	-
1. Configure Using This Registry Type ldap	
2. LDAP Server Hostname secu:	re2.pisc.uk.ibm.com
3. LDAP Server Port 389	
4. Suffix o=ibu	n,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:\P:	rogram 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 $\mid N$]:

 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'.

Opt	ion V	Jalue
1.	Configure Using This Registry Type	ldap
2.	LDAP Server Hostname	secure2.pisc.uk.ibm.com
З.	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 $\ensuremath{\mathtt{PDMgr}}$ 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

Version 0.8 – 21 September, 2001

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 ${\tt Y}$ 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\BM 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:

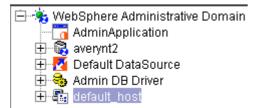
```
### BEGIN PDWPM CONFIG ENTRY ###
Listen 443
LoadModule ibm_ssl_module modules/IBMModuleSSL128.dll
<VirtualHost :443>
```

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 *xxxxxx*:8080 and change all the items that have port 443 specified from *xxxxxx*:443 to *xxxxxx*:8443 as shown below:

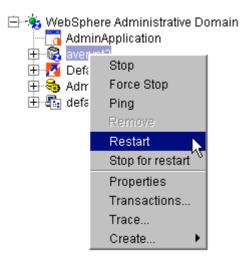
Before	After
Aliases	Aliases
Host Aliases	Host Aliases
localhost	localhost:8080
127.0.0.1	127.0.0.1:8080
averynt2	averynt2:8080
Aliases	Aliases
Host Aliases	Host Aliases
averynt2.pisc.uk.ibm.com	averynt2.pisc.uk.ibm.com:8080
averynt2:443	averynt2:8443
averynt2.pisc.uk.ibm.com:443	averynt2.pisc.uk.ibm.com:8443

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:

Apply.



k. This will show a confirmation. Click on

1 and the Admin console will close.

I. 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

Yes

6. Native installation process

This section describes the techniques for installing Policy Director and it's 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 **\windows\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:

	Setup will install GSK4 in the following folder. To install to this folder, click Next.
-	To install to a different folder, click Browse and select another folder.
	You can choose not to install GSK4 by clicking Cancel to exit Setup.
20	Destination Folder C:\Program Files\ibm\gsk4Browse
	< Back Next> Cancel

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



Setup Complete	Setup has finished installing GSK4 on your computer. Setup can launch the Read Me file and GSK4. Choose the options you want below.
	Click Finish to complete Setup.
	< Back Finish

f. Click on 'Finish'.

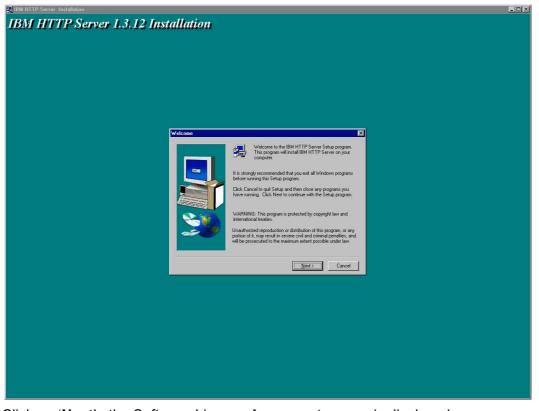
6.2 LDAP Server installation (Windows)

General notes

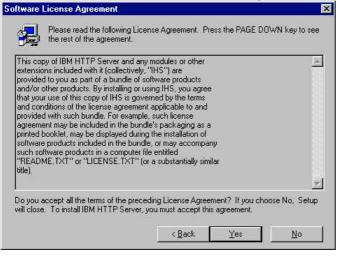
- In Policy Director Version 3.6 and before, it was necessary to install DB2 with the appropriate fixpacks and a web server separately. This is no longer the case with PD 3.7 and above they are installed as part of the IBM SecureWay Directory install.
- Note that installation of LDAP Server does not 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.)

tup Language	
Select the language for th the choices below.	is installation from
U.S. English	M
ОК	Cancel
	Select the language for th the choices below.

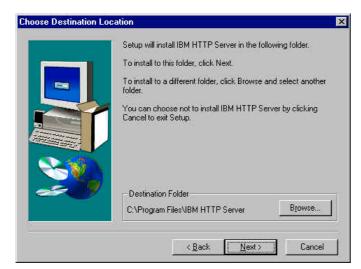
- g. Select a language and click on 'OK'.
- h. The InstallShield runs and the IBM HTTP Server 1.3.12 Welcome screen is displayed:



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' dialogue box is displayed:

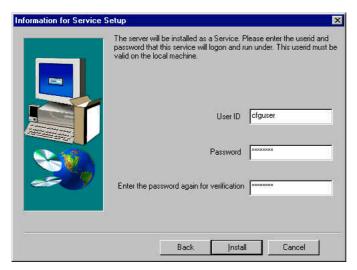


I. Leave 'Typical' selected and click on '**Next**'; the 'Select Program Folder' dialogue box is displayed:



m. Click on '**Next**'; the 'Information for Service Setup' dialogue box is displayed; enter the userid and password under which IBM HTTP Server will run. (We used a user ID of cfguser, password Secure99.)

Version 0.8 – 21 September, 2001



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\Idap32_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:

BM SecureWay D	irectory V3.2	S
	Software License Agreement Please read the accompanying license agreement carefully before using the Program. By selecting "Accept" below or using the Program, you agree to accept the terms of this agreement. If you select "Decline", installation will not be completed and you will not be able to use the Program. International Program License Agreement Part 1 - General Terms PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE PROGRAM. IBM WILL LICENSE THE PROGRAM TO YOU DINLY IF YOU FIRST ACCEPT THE TERMS OF	JAV
	This AGREEMENT, BY USING THE PROGRAM YOU AGREE TO THESE TERMS. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY RETURN THE UNUSED PROGRAM TO THE PARTY (EITHER IBM OR ITS RESELLER) FROM WHOM YOU ACQUIRED IT TO RECEIVE A REFUND OF THE AMOUNT YOU PAID. The Program is owned by International Business Machines Corporation or one of its subsidiaries (IBM) or an IBM supplier, and is copyrighted and licensed, not sold. The term "Program" means the original program and all whole or partial copies of it. A <u>ACCORPI</u> becline Print	
	IBA	

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

	Welcome to the LDAP Setup program. This program will install LDAP on your computer.
	It is strongly recommended that you exit all Windows programs before running this Setup program.
	Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.
	WARNING: This program is protected by copyright law and international treaties.
-	Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

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:

the second second

Please select t	he components that you want to install. Express Install all components that are not already installed Custom For advanced users and system administrators only. You may choose the components you want to install.
	<back next=""> Cancel</back>

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):

	The following components are not currently installe Components		
	✓ Clent-3.2 40276 K ✓ Server 3.2 22449 K ✓ DB2 V6.1 86441 K □IBM HTTP 0 K □ GSKIT 4.01 0 K	✓ Client SDK 1123 ✓ DMT and Jav 2904	
	Description This component contains the libraries and SDK.	client command line utilities, C	
-	Space Required: 149167 K	Available: 4099684	ĸ

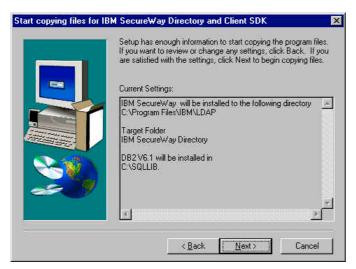
w. Click on 'Next'. The 'Folder Selection' option is shown:



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:

Readme	
?	We recommend that you view the README file for additional information that you may find necessary in order to properly run IBM SecureWay Directory on your system. Would you like to view it now?
	Yes No

- 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:

IDM Coorrallian D	in actory 1/2 2	
IBM SecureWay D	urectory v 5.2	Q
		20
	AND A DOWNLOW	
S - 18	ALL PRIMA	ΤΑΥΖΑ
	Software License Agreement	COMPATIBL
	Please read the accompanying license agreement carefully before using the Program. By selecting "Accept" below or using the Program, you agree to accept the terms of this agreement. If you select "Decline", installation will not be completed and you will not be able to use the Program.	
	International Program License Agreement	
	Part 1 - General Terms	
	PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE PROGRAM. IBM WILL LICENSE THE PROGRAM TO YOU ONLY IF YOU FIRST ACCEPT THE TERMS OF THIS AGREEMENT, BY USING THE PROGRAM YOU AGREE TO THESE TERMS. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY RETURN THE UNUSED PROGRAM TO THE PARTY (EITHER IBM OR IT'S RESELLER) FROM WHOM YOU ACQUIRED IT TO RECEIVE A REFUND OF THE AMOUNT YOU FAID.	
	The Program is owned by International Business Machines Corporation or one of its subsidiaries (IBM) or an IBM supplier, and is copyrighted and licensed, not sold.	
	The term "Program" means the original program and all whole or partial copies of it. A	
	Accept Decline Print	

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]

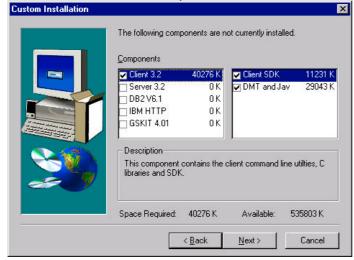
e. Click on 'Next'. The Select Components panel will be displayed:



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



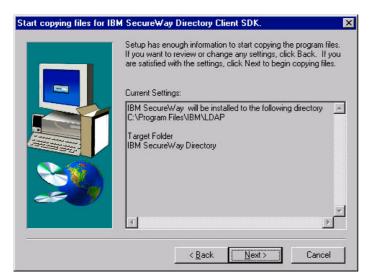
g. Click on '**Next**'. The 'Custom Installation' panel is displayed. Select only the Client component, and deselect all other components:



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:

Headme		
?	We recommend that you view the README file for additional information that you may find necessary in order to properly run IBM SecureWay Directory on your system. Would you like to view it now?	
	Yes: No	

- k. Select 'Yes' or 'No' as you feel appropriate.
- I. The 'Setup Complete' panel is displayed. Select 'No, I will restart my computer later': Setup Complete

	Setup has finished. You must restart the computer to complete the installation
	 Yes, I want to restart my computer now. No, I will restart my computer later;
25	Click finish to complete the Setup.
	< Back Finish

m. Click on 'Finish'.

6.4 Policy Director Servers installation (Windows)

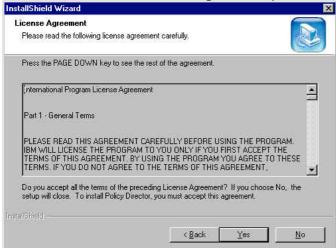
- a. Insert the Tivoli SecureWay Policy Director Base for Windows Version 3.8 CD.
- b. Using 'My Computer' find the \windows\PolicyDirector\Disk Images\Disk1 directory on the CD, and double click on setup.exe. The 'Choose Setup Language' dialogue box is displayed:



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

Install5hield Wizard	
	Welcome to the InstallShield Wizard for Policy Director
	The InstallShield® Wizard will install Policy Director on your computer. To continue, click Next.
A	
RAI	
	Cancel

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



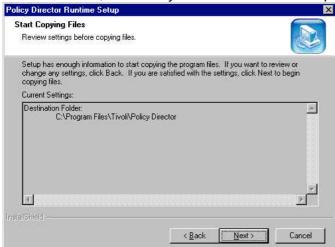
e. Click on '**Yes**'. The 'Select Packages' panel will be displayed. Select the Policy Director packages you require (at a minimum the PDRTE and PDMgr, we chose all the packages here for our install):

elect Packages	
Choose Policy Director Packages	
Policy Director Runtime (PDR1	TE)
Policy Director Management S	erver (PDMgr)
Policy Director Authorization S	erver (PDAcld)
Policy Director Authorization A	DK (PDAuthADK)
Policy Director Authorization A	DK (PDAuthADK)
Policy Director Authorization A	DK (PDAuthADK)
Policy Director Authorization A	DK (PDAuthADK)
Policy Director Authorization A	DK (PDAuthADK)
Policy Director Authorization A	DK (PDAuthADK)
Policy Director Authorization A	
Policy Director Authorization A	DK (PDAuthADK) Select All

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

noose Destination Location	
Select folder where Setup will install files	
Setup will install Policy Director Runtime	in the following folder.
To install to this folder, click Next. To ins another folder.	tall to a different folder, click Browse and select
- Destination Folder	
Destination Folder C:\Program Files\Tivoli\Policy Director	Browse
	Browse

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**'): Policy Director Installation Complete



i. Click on 'OK'.

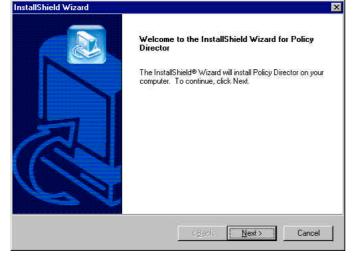
6.5 Install Policy Director Runtime Environment (PDRTE) (Windows)

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

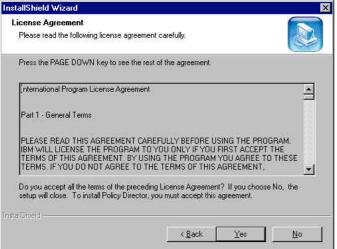
- a. Insert the Tivoli SecureWay Policy Director Base for Windows Version 3.8 CD.
- b. Using 'My Computer' find the \windows\PolicyDirector\Disk Images\Disk1 directory on the CD, and double click on setup.exe. The 'Choose Setup Language' dialogue box is displayed:



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:



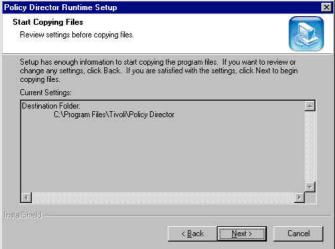
e. Click on '**Yes**'. The 'Select Packages' panel will be displayed. Select Policy Director Runtime (PDRTE) and deselect all other packages:

stallShield Wizard			2
Select Packages			
Choose Policy Director Packages			
Policy Director Runtime (PDRTE)			
Policy Director Management Server (PDMgr)			
Policy Director Authorization Server (PDAcld)		
Policy Director Authorization ADK (PDAuthA			
staliShield		Select All	<u>C</u> lear All

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

ose Destination Location		
elect folder where Setup will install files.		
Setup will install Policy Director Runtime in th	e following folder.	
o install to this folder, click Next. To install t mother folder.	o a different folder, click Br	owse and select
Destination Folder		
C:\Program Files\Tivoli\Policy Director		Browse
c. a regram messaria oncy precior		
Sheld		

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:

Choose S	etup Language 🛛 🔀
	Select the language for this installation from the choices below.
	English
	OK Cancel

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

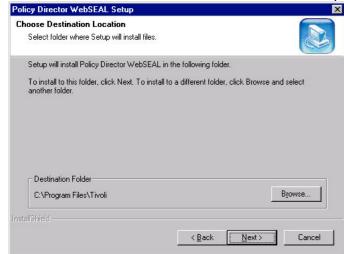


d. Click on 'Next', the 'Policy Director WebSEAL License Agreement' is displayed

cense Agreement			
Please read the following license agreem	ent carefully.		
Press the PAGE DOWN key to see the re	est of the agreement.		
International Program License Agreemen	ıt		<u>_</u>
Part 1 - General Terms			
PLEASE READ THIS AGREEMENT CA IBM WILL LICENSE THE PROGRAM TI TERMS OF THIS AGREEMENT. BY US TERMS. IF YOU DO NOT AGREE TO T	O YOU ONLY IF YOU ING THE PROGRAM	FIRST ACCEPT 1 YOU AGREE TO	THE
Do you accept all the terms of the preced etup will close. To install Policy Director			
Shield			

Version 0.8 - 21 September, 2001

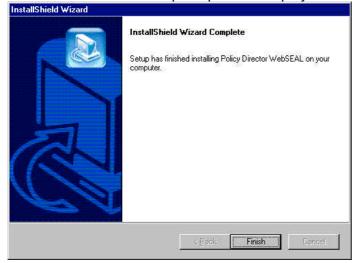
e. Click on 'Yes', the 'Choose Destination Location' panel is displayed.



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

lect Components hoose the components Setup wil	install.
ielect the components you want t stall. PDWeb PDWeb ADKs	o install, and clear the components you do not want to Description Policy Director WebSEAL Server
pace Required on C: pace Available on C: Shield	3666 K 4437199 K

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



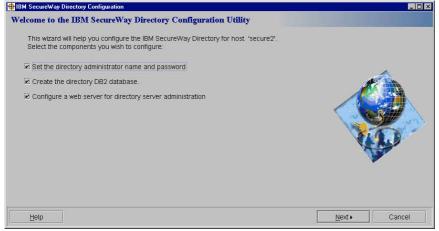
- h. Click on 'Finish'.
- i. At this point the computer can be re-booted by issuing Start -> Shut Down -> 'Restart the computer'.

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:

eryice	Status	Startup	Close
Alerter	Started	Automatic 📐	
ClipBook Server		Manual	Start
COM+Event System		Manual	
Computer Browser	Started	Automatic	Stop
DB2 - DB2	Started	Automatic	-
DB2 - DB2DAS00	Started	Automatic	Eause
DB2 Governor		Manual	Continue
DB2 Security Server		Manual	1255()((110)5)
DHCP Client		Disabled	Startup
Directory Replicator		Manual 💌	
			HW Profiles
itartup Parameters:			

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:

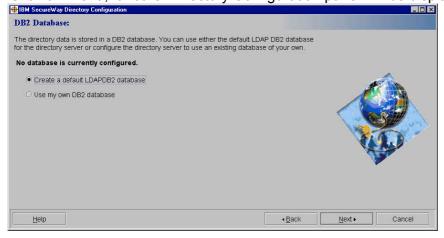


c. Click on '**Next**'; the Directory Configuration panel will be displayed. Enter the Administrator DN and Password (we used cn=root and Secure99).

BM SecureWay Directory Configuration	
Administrator DN:	
Enter a new directory administrator Distinguished Name and password for host 'secure2'. All fields are required. Administrator DN: [cn=root Administrator Password: Type the password again to confirm:	
Help ABack	Next • Cancel

Version 0.8 - 21 September, 2001

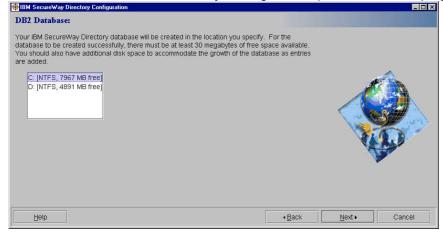
d. Click on 'Next'; another Directory Configuration panel will be displayed:



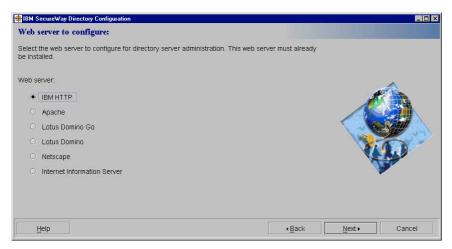
e. Click on 'Next'; another Directory Configuration panel will be displayed:

IBM SecureWay Directory Configuration	
DB2 Database:	
he default DB2 database may be created in the local codepage, or in a universal character set JTF-8). If you anticipate storing data from multiple character sets in your directory, you may wish to se the UTF-8 option. Refer to the Installation and Configuration Guide for additional information.	
Create a Universal DB2 database (UTF-8)	
Create a local codepage DB2 database	
Create a database for Change Log support	
	1
Help • Back	Next Cancel

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



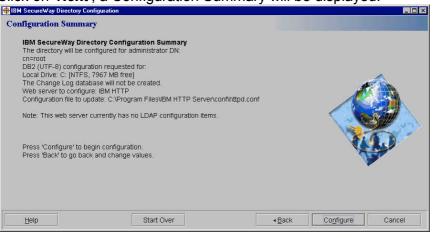
g. Click on '**Next**'; you will be asked which web server you want to configure for directory server administration. Ensure that 'IBM HTTP' is selected:



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

BM SecureWay Directory Configuration			
Web server configuration file:			
Enter the full pathname of the web server configuration file. This file will be configu server administration.	red for directory		
IBM HTTP web server configuration file:			~
C:\Program Files\IBM HTTP Server\conf\httpd.conf	Browse		
Hetp	< <u>₿</u> ack	Next►	Cancel

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 Idapadb2 database:



k. A configuration Summary is then displayed:

IBM SecureWay Directory Configuration	n l	
Configuration Summary		
Directory configuration completed w	ithout errors.	
of Admin DN update:	Success	
Section:	Success	-
Change Log configuration:	Not selected	
I Web server update:	Success	
The web server must be restarted for Administration: http://secure2:80/ldap/index.html	or changes to take effect. Use the following URL to access Server	
Help	Start Over	Ok

- I. 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.

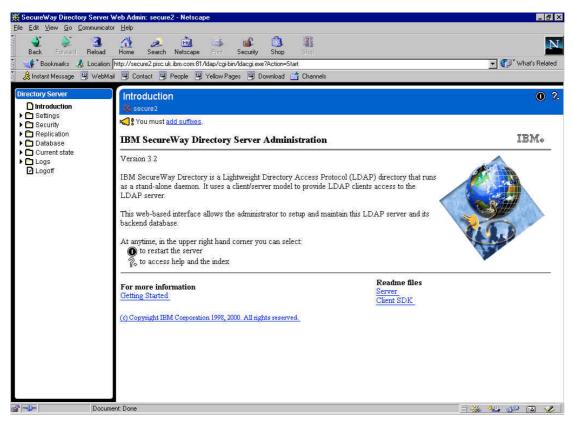
Note: If you have problems with the graphical interface, the LDAP configuration can be performed with the following manual commands:

- 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 -1 C:\LDAPDB2\ (or any directory that has space for the database.)

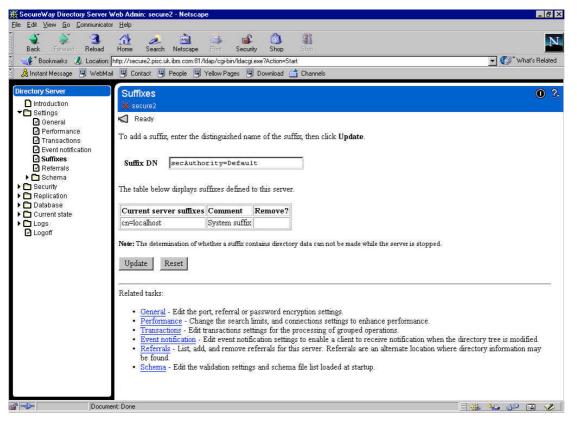
o. Next to add the suffixes you need to LDAP, point a web browser at http://hostname:port number/ldap/index.html (the port number was 81 in our case). The SecureWay Directory Server Logon panel is displayed. Set the User ID to the LDAP Administrator ID and the password to that which was entered previously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

💥 SecureWay Directory Ser	ver Web Admin: secure2 - Netscape	_ @ ×
<u>File Edit View Go Commu</u>	nicator <u>H</u> elp	
Back Forward Relo		N
🛯 🍕 Bookmarks 🙏 Loc	ation: http://secure2.pisc.uk.ibm.com:81/ldap/cgi-bin/ldacgi.exe?Action=Start	👻 🍘 What's Related
🕺 🚴 Instant Message 🖳 W	ebMail 🖳 Contact 🚇 People 🖳 Yellow Pages 🖳 Download 📑 Channels	
A Instark Message W W	bdMail W Contact W People W Yellow Pages Download Channels Logon Secure2 Ready IBM SecureWay Directory Server Administration Please enter the LDAP administrator ID and password and click Logon. Admin ID en=root Password ******** Image: Contact C	?. IBM₀
	Logon (c) Copyright IEM Corporation 1998, 2000. All rights reserved.	
💣 🕬 📃 🛛 🔘	ocument: Done	🐝 🚧 🚳 🖓 🗌

p. Click on 'Logon'. The 'IBM SecureWay Directory Server Administration' panel is displayed. It will indicate 'You must <u>add suffixes</u>' 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 <u>restart the server</u> 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.

💥 SecureWay Directory Server	Web Admin: secure2 - Netscap	e		_ /# ×
<u>File Edit View Go</u> Communica	tor <u>H</u> elp			
Back Forward Reload	🐴 🌌 👼 Home Search Netscape	🤹 🗃 Fint Secur	ty Shop	Step
📔 🌿 Bookmarks 🤳 Location	n: http://secure2.pisc.uk.ibm.com/81/1	dap/cgi-bin/ldacg	i.exe?Action=S	tart 💽 📢 "What's Related
📋 🔏 Instant Message 🛛 WebM	tail 📴 Contact 📴 People 🖳	Yellow Pages 🛛 📱	Download	🗂 Channels
	al Contact P People C SUffixes Suffix P People C Suffix P People C Suffix D Outereas The list was successfull To add a suffix, enter the d Suffix D Outereas Durants of the people People People People Current server suffix, however Current server suffixes icnelocalisat secAuthority=Default Note: The determination of wh Update Reset Related tasks: <u>General</u> - Edit the po <u>Performance</u> - Chan <u>Transcomes</u> - Chan	Yakow Pages y updated. You u ssinguished nar o= ibm, c=gb ffixes defined r the data is no Comment System suffix ether a suffix co rt, referral or p gama ether as	Download must <u>restart i</u> me of the su to this serve t tremoved f Remove? Dassword en initias, and ct initias, and ct initias, and ct initias, sethin cention sethin	Channels Channels Channels Control Channels Control Control
🚰 🕪 🛛 Apple	t com.ibm.webexec.herald.HeraldApple	t running		🗏 🌺 🌄 💷 🗃 🥩

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

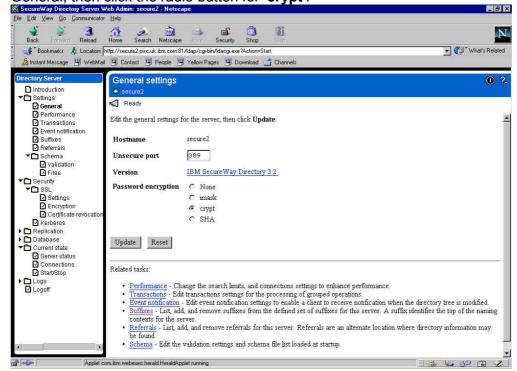
Elle Edit View Go Communicato		0			- 0' X		
Lite Call yew go Communication Back Forward Reload	Home Search Netscape	Pint Sec		Stop	N		
	http://secure2.pisc.uk.ibm.com:81/				Related		
📋 🚴 Instant Message 🛛 🦉 WebMa	il 🖳 Contact 🖳 People 🖳	Yellow Pages	📱 Download	🖆 Channels			
Directory Server	Suffixes			(0 ?.		
T Settings		kundated You	must restart t	the server for this change to take effect.			
General Performance	1923						
Transactions Event notification	To add a suffix, enter the d	istinguished n	ime of the su	ffix, then click Update .			
Suffixes	Suffix DN						
Referrals C Schema							
 Security Replication Database 	The table below displays su beneath that suffix, howeve			rr. To remove a suffix, select the checkbox and click Update . Removing a suffix eliminates access to all directory data from the directory.			
 Current state Logs 	Current server suffixes	Comment	Remove?				
Logoff	cn=localhost	System suffic	1				
-1.1.1.1.1 (19 1 1)	ou=emea, o=ibm, c=gb		Π				
	secAuthority=Default		Г				
	Note: The determination of whether a suffix contains directory data can not be made while the server is stopped. Update Reset						
	Related tasks:						
	Included (Bass)						
	<u>General</u> - Edit the port, referral or password encryption settings. <u>Performance</u> - Change the search limits, and connections settings to enhance performance.						
				onnechons settings to enhance performance. : processing of grouped operations.			
	 Event notification - I 	Edit event noti	fication settin	ugs to enable a client to receive notification when the directory tree is modified.			
	Referrals - List, add, and remove referrals for this server. Referrals are an alternate location where directory information may be found						
	 <u>Schema</u> - Edit the validation settings and schema file list loaded at startup. 						
	a						
Applet o	com ibm.webexec.herald.HeraldApple	et running			Ľ		

Version 0.8 - 21 September, 2001

v. Click on the '<u>restart the server</u>' 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.

$\underline{F}ile \underline{E}dit \underline{V}iew \underline{G}o \underline{C}ommunicato$	и <u>H</u> elp	
Back Forward Reload	Home Search Netscape Pint Security Shop Stop	N
	http://secure2.pisc.uk.ibm.com:81/Idap/cgi-bin/Idacgi.exe?Action=Start	👻 🌍 🔭 What's Related
🎽 🔏 Instant Message 🖳 WebMa	il 🖳 Contact 🖳 People 🖳 Yellow Pages 🖳 Download 📩 Channels	
Directory Server Dintroduction Settings Deformance Transactions Event notification Suffues Referents Beferents Current state Security Current state Server status Connections StartStop Logs Logorf	Stop Secure2 The directory server is running. The directory server is running. To stop the server, click the Stop button. Stop Related tasks: • Server status - Display the current status of the server to review server activity. • Connections - View the current connections to the server.	
Applet i	com.iom.webexec.netaio.netaio.gpiet running	🐝 🐸 🛷 🖬 🎸

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 <u>restart the server</u> for these changes to take effect'. Click on '<u>restart the server</u>' and wait for the server to restart.

Version 0.8 - 21 September, 2001

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:

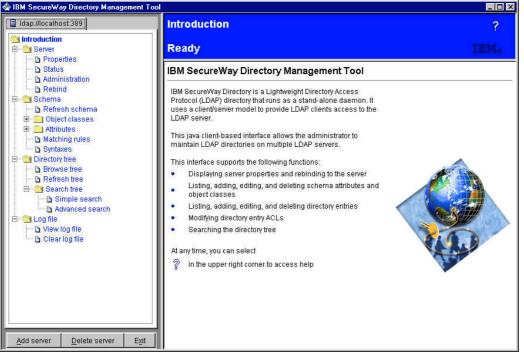
```
Ibm-slapdSuffix: secAuthority=Default
ibm-slapdSuffix: o=ibm, c=gb
```

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):

🍲 IBM SecureWay Directory Management Tool		_ 🗆 ×
🔋 Idap://localhost:389	Rebind	?
Introduction	Ready	IBM.
D Status D Administration D Rebind	Enter a new bind DN and password for the server Idap://localhost.389	
🖻 😋 Schema	C Anonymous Authenticated	
⊕- 🧰 Object classes ⊕- 💼 Attributes	User DN : cn=root User password : *******	
Matching rules Syntaxes Syntaxes Syntaxes Directory tree Browse tree Browse tree Browse tree D Refresh tree Browse tree D Simple search D Clear log file	OK Cancel Help	
Add server Delete server Exit		

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:

🕸 IBM SecureWay Directory Management	Fool								×
Idap://localhost:389	Browse	tree						?	
Introduction	Ready							IBM.	
- D Status - D Administration - D Rebind	ගැට Search	Expand	Add	Edit:	Duplicate	Telete	ACL.	Edit RDN	A
Add server Delete server Exit	k ■ Idap://oc ⊕-cn=local								•

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

Version 0.8 - 21 September, 2001

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.

elect an Ent	ry type, enter the Parent DN, modify the Entry	RDN, then click OK.	
Entry type	Organizational unit 💽		
Parent DN:			
Entry RDN:	ou=emea,o=ibm,c=gb		

f. Click on 'OK'.

jectClass (Object class): 🛛 🚦	organizatio	onalUnit
(DN):	u=emea,	o=ibm,c=gb
ttributes		
ou:	0	emea,o=ibm,c=gb
businessCategory:	0	
description:	2	
destinationIndicator:	0	
facsimileTelephoneNumber:	0	
internationalISDNNumber:	2	
	0	
physicalDeliveryOfficeName:	0	
postalAddress:	2	
postalCode:	0	

- 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:

Configured	
No No No No	View log
	Configure
	Unconfigure
	F
	No No No

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:

	pisc.uk.ibm.com,	509,	
M LDAP Se	rver Information		×
	LDAP Server Information		
	LDAP Host Name		
	secure2.pisc.uk.ibm.com		
	LDAP Port Number		
	389		
	LDAP DN for GSO Database		
	ou=emea,o=ibm,c=gb		
	Next >	Ca	ncel
			O

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

Version 0.8 – 21 September, 2001

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")

SSL Communication with the LDAP Server	×
Enable SSL Communication with the LDAP Server?	
SSL Port Number	
636 SSL client key file	
SSL client certificate label (if required)	
SSL client key file password	
<pre></pre>	

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

rolley Director conligaration ric	11011		
Management Server Host: secure2			
User Registry Selection: Ida	эр		
LDAP Host Name: secure2.pisc.uk.ibm.com			
LDAP Port Number: 389			
LDAP DN for GSO Database	e:		
ou=emea.o=ibm,c=gb			
Enable SSL Communication	n with the LDAP Server?	: No	
< Back	Finish	Cancel	

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:

		Close
nstalled Packages	Configured	Refresh
Policy Director Runtime Environment (PDRTE) Policy Director Management Server (PDMgr) Policy Director WebSEAL (PDWeb) Policy Director Authorization Server (PDAcId)	Yes No No No	View log
		Lonigure
		Unconfigure.
1		F

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):

LDAP Administrator Name	
cn=root	
LDAP Administrator Passv	vord
****	-

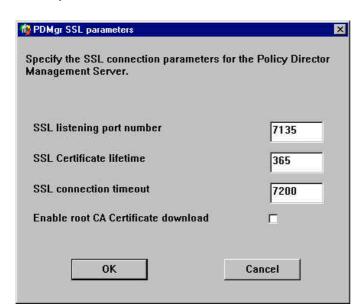
i. Click **'OK'**. The 'Policy Director Administrator Definition' panel is displayed. The Policy Director Administrator Name is fixed as sec_master; specify the password for the Policy Director Administrator (we used Secure99):

olicy Director Administrator Definition	
Specify the user name and password for the Policy Director Administrator.	
Administrator Name	
sec_master	
Administrator Password	

Password confirmation	

OK Cancel	

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.)
- I. Accept these values and click on **'OK'**. A message 'Configuring Policy Director Management Server' is displayed; then an 'Information' panel is displayed:

(i)	
v	C:\Program Files\Tivol\Policy Director\\keytab\pdcacert.b64 You must distribute this file to each machine in your secure domain. It is needed for successful configuration.

- 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'.
- 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):

Version 0.8 – 21 September, 2001

	I for the Policy Director
dministrator (sec_m	asterj.
Administrator Passw	rord

******** /	
******** *	

- q. Click on 'OK'; WebSEAL is then configured.
- r. The 'Policy Director Configuration' panel is displayed once again. Highlight 'Policy Director Authorization Server (PDAcld)' and click on 'Configure'. The 'LDAP Administrator Login' is displayed; enter the Administrator name and password (cn=root and Secure99 in our case):

LDAP Administrator N	lame
cn=root	
LDAP Administrator P	assword

	Cancel

s. Click on **'OK'**. The 'Policy Director Administrator Password' panel is displayed; enter the Policy Director Administrator password (Secure99 in our case):

Specify the password Administrator (sec_m	d for the Policy Director naster).
Administrator Passw	vord

- 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:

stalled Packages	Configured	Refresh
olicy Director Runtime Environment (PDRTE) olicy Director Management Server (PDMgr) olicy Director WebSEAL (PDWeb) olicy Director Authorization Server (PDAckd)	Yes Yes Yes Yes	View log
		Gorfig)re.
		Unconfigure
		×

- 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:

		Refresh
nstalled Packages	Configured	
olicy Director Runtime Environment (PDRTE) olicy Director WebSEAL (PDWeb)	No No	View log
		Configure
		Unconfigure

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:

secure2.pisc.uk.ibm.com
7135
Cancel

Version 0.8 - 21 September, 2001

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.

Name of the file containing the Management Server's signed certificate	C:\pdcacert.b64	
	Choose file	
< Back Next > Cancel		

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).

erver Information	×
LDAP Server Information	
LDAP Host Name	
secure2.pisc.uk.ibm.com	
LDAP Port Number	
389	
LDAP DN for GSO Database	
ou=emea,o=ibm,c=gb	
Next >	Cancel
	LDAP Server Information LDAP Host Name secure2.pisc.uk.ibm.com LDAP Port Number 389 LDAP DN for GSO Database 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")

Enable SSL Communication with the LDAP Server?	
C Yes © No	
SSL Port Number	
636	
SSL client key file	
SSL client certificate label (if required)	
SSL client key file password	
1 - 1 <mark>.</mark>	

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

Policy Director Configuration Re	TICH		
Management Server Host:			
secure2.pisc.uk.ibm.com			
Listening Port:			
7135 Name of the file containing t	the Management Con-	or's signed sertificate:	
C:\pdcacert.b64	uie manayement serv	er s signeu ceruncale.	
User Registry Selection: Id	ар		
LDAP Host Name:			
secure2.pisc.uk.ibm.com			
389			
LDAP DN for GSO Databas	e:		
ou=emea,o=ibm,c=gb			
Enable SSL Communicatio	n with the LDAP Serve	r?: No	
< Back	Finish	Cancel	

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:

Installed Packages Config	Refresh
Policy Director Runtime Environment (PDRTE) Yes Policy Director WebSEAL (PDWeb) No	View log
	Configure
	Unconfigure

- 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:

80	Port to use for uns	secure HTTP reques	ts
100			
Allow HTTI	S access		
Allow III II	0 000000		
443	Port to use for HT	TPS requests	
443			
and the second s			

I. 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 \windows\websphere directory on the CD, and double click on setup.exe. The 'Choose Setup Language' dialog box appears:

3	Select the language for this installation from the choices below.
	English

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

IBM WebSphere Application Server 3.5 Standard Edition
WebSphere Application Server X ATTENTION: Before you continue, you must shut down all Web Servers you plan to turn with WebSphere Attention: WebSphere Wind Control of the strength of the st
<u>Leed></u>

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

istallation Options	×
Select the installation option you prefer and then click next.	
 Quick Installation 	
Everything you need to support production-level applications intended to run on servers with single-node configurations; includes IBM HTTP Server, InstantDB, and JDK 1.2.2.	
C Custom Installation	
Choose to install specific components of the total install package; specify the use of other supported databases and web servers.	ŧ
< <u>B</u> ack <u>N</u> ext > Cancel	

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:

Username	cfguser			
Password	******			
Confirm Password	*****			

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

C:\WebSphere\AppServer	Browse.	

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



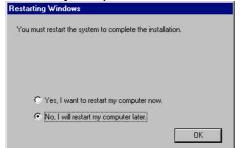
k. Click on '**Next**'; the files are copied across; you are prompted to confirm the directory containing the IBM HTTP Server configuration file:

Path: C:\Program Files\IBM HTTP \	Server\conf
2irectories:	
🗁 c:\ 📃	OK
BM HTTP Server	Cancel
*	

I. 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
```

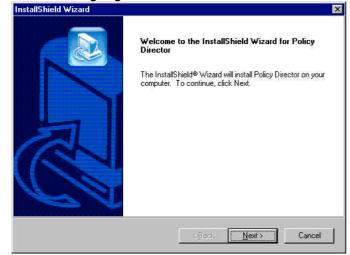
- q. Re-boot the computer by issuing Start -> Shut Down -> 'Restart the computer'.
- r. Use Start -> Settings -> Control Panel -> Services (NT) or Start -> Programs -> Administrator Tools -> Services (2000) to start the IBM WS AdminServer.
- s. Ensure that WebSphere Application Server has started correctly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

9) 🕨 🖷 😭 🐨 🗉 🦻	. •			
WebSphere Administrative Domain Composition	Node:secure2 General	Node name: Current State: Desired State: Start Time: Host name: Host system type: Install root: Process ID: Deployed JAR directory: Dependent classpath:	Secure 2 Running Running Jul 30, 2001 5:27,55 PM secure 2 x86 C :WebSphereVopServer 51 C :WebSphereVopServer 51	
			Apply	<u>R</u> eset
		Console Messages		
/30/01 5:30 PM : AUDIT [secure2/ /30/01 5:30 PM : AUDIT [secure2/	adminServer]: XP adminServer]: XP adminServer]: XP adminServer]: XP adminServer]: XP adminServer]: XP adminServer]: XP	LCO0531: Importing J LCO0531: Importing : LCO0531: Importing ! LCO0531: Importing : LCO0531: Importing : LCO0531: Importing :	ApplicationServer : Default Serve ServletEngine : Default Servlet E WebApplication : WSsamplesIDB_app Servlet : Error Reporting Facilit Servlet : File Serving Enabler Servlet : Auto-Invoker	ngine Y

- 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):

stallShield Wizard			
Select Packages			
Choose Policy Director Packages			
V Policy Director Web Portal Man	nager (PDWPM)		
		Select All	filear All
taliShreid		Select All	

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

imunnau	un 🔼
٩	All Policy Director components have been installed. Installation completed successfully.
	Click OK to exit.
	OK

- 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:

		Close
installed Packages	Configured	Refresh
Policy Director Runtime Environment (PDRTE) Policy Director Management Server (PDMgr) Policy Director WebSEAL (PDWeb) Policy Director Authorization Server (PDAcId)	Yes Yes Yes Yes	View log
Policy Director Web Portal Manager (PDWPM)	No	Configure
		Unconfigure
4		F

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

stalled Packages	Configured	Refresh
licy Director Runtime Environment (PDRTE) licy Director Management Server (PDMgr) licy Director WebSEAL (PDWeb) licy Director Authorization Server (PDAcId) licy Director Web Pottal Manager (PDWPM)	Yes Yes Yes Yes Yes Yes	View log
		Unconfigure.
	6	F
	J	

- 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 comunication 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 hostames listed under HostAliases. In our case the new entries were secure2:4443 and secure2.pisc.uk.ibm.com:4443:

WebSphere Advanced Administrative C Console View Help	console		_ 🗆 🗵

WebSphere Administrative Domain AdminApplication Gescure2 Default DataSource Admin DB Driver Admin DB Driver E E Essential form	Virtual Host:default_host General Advanced Virtual Host Name: default_host Aliases Host Aliases Secure 2 pisc.uk.lbm.com.4443		
		Apply	<u>R</u> eset
	Console Messages		
8/1/01 12:11 PM : AUDIT [secure2/ 8/1/01 12:11 PM : AUDIT [secure2/		rver" ver" (pid "536	

gg. Click on 'Apply'.

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

9) 🕨 📲 🚰 🔚 🔍 🔹		
→ WebSphere Administrative Demain Nod → Administrative Demain Gene → Administrative Demain Force Stop → Restart Force Stop for restart Properties Transactions Trace Create	rral Node name: Current State: Stat Time: Host name: Host system spec Instal root: Process ID:	Secure2 Running Running Jul 30, 2001 5;27:55 PM secure2 x86 C-WebSphereVuppServer 51 S-WebSphereVuppServer 51 S-WebSphereVuppBerver/deployedEJBs
		<u>Apply</u> <u>R</u> eset
	Console Messages	
/30/01 5:43 PM : AUDIT [secure2/Default /30/01 5:43 PM : AUDIT [secure2/Default	t Server]: SRVE0091I: [Servlet I t Server]: SRVE0130I: Servlet at t Server]: SRVE00481: Loading se t Server]: SRVE0091I: [Servlet I t Server]: SRVE01301: Servlet at .HodifyAttributes" running	LOG]: "File Serving Enabler: init" vallable for service: "File Serving Enabler" ervlet: "35P 1.1 Processor" LOG]: "JSP 1.1 Processor: init" vallable for service: "JSP 1.1 Processor"

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



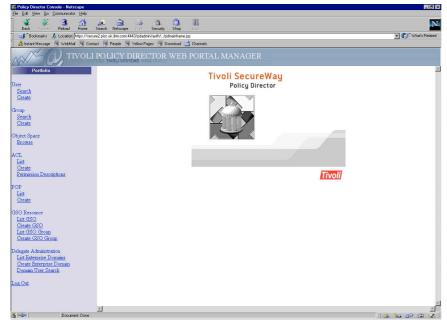
- jj. Click on '**Yes**'. As part of restarting WebSphere Application Server the WebSphere console is closed.
- kk. Use Start → Programs → IBM WebSphere → Application Server V3.5 → Administrator's Console; the presence of the symbol to the right of the machine name indicates that the Default Server is running:
- II. You can use the console to verify that WPM is running:

WebSphere Administrative Domain AdminiApplication AdminiApplication Secure2 Secure2 Secure2 Secure2 Secure2 Secure2 Secure3 Default Server Secure3 Secure4 Secure4 Secure5 Secure5 Secure6 Secure7 Secure7 Secure6 Secure7 Secure7 S			
I CA DETAUL DOST	AdminApplication secure2 Default Server Default Server Default Server Default Server Default Server default_app Default Server Error Reporting Facility Default DataSource Default DataSource	General Advanced Web Application Name: Current State: Desired State: Start Time: Enabled: Description: Virtual Host Virtual Host Web Application Web Path:	pdadmin Lost Contact Running → True Policy Director Web Admin Tool default_host default_host pdadmin
Console Messages			<u>Apply</u> <u>R</u> eset

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):

🔆 Policy Director Login - Netscape	_ 5 ×
Elle Edit View Go Communicator Help	
Back Forward Reload Home Search Netscope Print Security Step Step	N
🐩 🎲 Bookmarks 🥻 Location: [https://secure2.pisc.uk.ibm.com/4443/pdadmin/auth/handleLogin.jsp	💌 🌔 What's Related
🕺 İnstant Message 🖳 WebMail 🗒 Contact 🔯 People 🖳 Yellow Pages 🖳 Download 📑 Channels	
Tivoli SecureWay	
Policy Director	
Tivoli	
User ID: sec_master	
Password: Login	
(≝ =D= Document: Done	

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

Version 0.8 - 21 September, 2001

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.

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

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, <code>lslpp -l |grep X11.Dt.lib</code> to determine the level of <code>X11.Dt.lib</code> 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 Updat	ce from LATEST Avai	lable Software			
	alues in entry field R making all desired				
* SOFTWARE to ins PREVIEW only? COMMIT software SAVE replaced f AUTOMATICALLY i EXTEND file sys OVERWRITE same VERIFY install	(install operation of e updates? Eiles? install requisite so stems if space neede or newer versions? and check file size ponding LANGUAGE files?	will NOT occur) oftware? ed? es?	[Entry Fi /dev/cd0 [+ 1.3.12.0 no yes no yes no no yes no yes no yes	_	> rve> + + + + + + + + + + + +
F1=Help F5=Reset F9=Shell		F3=Cancel F7=Edit Enter=Do	F4=Li F8=In		

- 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 <code>./apachectl stop</code>, or else issue <code>ps -ef|grep httpd</code> to determine the PID and then issue <code>kill process id</code> 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
- I. 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 Upda	te from LATEST Avai	lable Software		
	alues in entry fiel R making all desire			
* SOFTWARE to in PREVIEW only? COMMIT softwar SAVE replaced AUTOMATICALLY EXTEND file sy OVERWRITE same VERIFY install	(install operation e updates? files? install requisite s stems if space need or newer versions? and check file siz ponding LANGUAGE fi	will NOT occur) oftware? led? :es?	[Entry Fields] /dev/cd0 [gskit no yes no yes yes no no yes no yes no yes	> + + + + + + + + + + + + + + + + + + +
F1=Help F5=Reset F9=Shell	F2=Refresh F6=Command F10=Exit	F3=Cancel F7=Edit Enter=Do	F4=List F8=Image	

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.

Version 0.8 - 21 September, 2001

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 Avail	able Software		
Type or select values in entry field Press Enter AFTER making all desired			
 * INPUT device / directory for softw * SOFTWARE to install PREVIEW only? (install operation w COMMIT software updates? SAVE replaced files? AUTOMATICALLY install requisite so EXTEND file systems if space neede OVERWRITE same or newer versions? VERIFY install and check file size Include corresponding LANGUAGE fil DETAILED output? Process multiple volumes?	vill NOT occur) oftware? od? es?	[Entry Fields] /dev/cd0 [db2_06_01.cnvucs no yes no yes yes no no yes no yes	> + + + + + + + + + + + + + + + + + + +
F1=HelpF2=RefreshF5=ResetF6=CommandF9=ShellF10=Exit	F3=Cancel F7=Edit Enter=Do	F4=List F8=Image	

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?
                                                                                +
                                                       ves
  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

Version 0.8 - 21 September, 2001

- 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 libDSP.a.
Plugin of type PREOPERATION is successfully loaded from libevent.a.
Plugin of type AUDIT is successfully loaded from libevent.a.
Plugin of type EXTENDEDOP is successfully loaded from libevent.a.
Plugin of type EXTENDEDOP is successfully loaded from libevent.a.
Plugin of type DATABASE 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

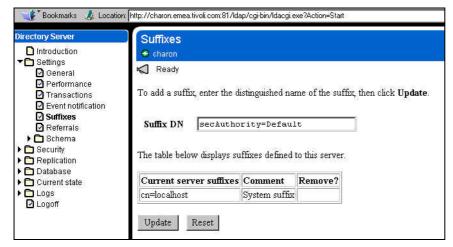
a. Point a web browser at http://hostname:port number/ldap/index.html (the port number was %1 in our case). The SecureWay Directory Server Logon panel is displayed. Set the User ID to the LDAP Administrator ID and the password to that which was entered previously (cn=root and Secure99 in our case):

SecureWay Directory Se	rver Web Admin: charon - Netscape	_ 8 ×
<u>File E</u> dit <u>V</u> iew <u>G</u> o <u>C</u> omm	inicator <u>H</u> elp	
	oad Home Search Netscape Print Security Shop Stop	N
🛛 🌿 Bookmarks 🧔 Lo	ation http://charon.emea.tivoli.com:8013/ldap/cgi-bin/ldacgi.exe?Action=Start	🔽 🌍 🗸 What's Related
📑 IBM 🖳 Internet 📹	Lookup 📩 New&Cool 🖳 RealPlayer	
Directory Server	Logon	?-
	IBM SecureWay Directory Server Administration	IBMø
	Please enter the LDAP administrator ID and password and click Logon. Admin ID cn=root Password ********	
	Logon (c) Copyright IBM Corporation 1998, 2000. All rights reserved.	

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:

📲 Bookmarks 🦧 Loc	ation: http://charon.emea.tivoli.com:81/Idap/cgi-bin/Idacgi.exe?Action=Start
Directory Server	Introduction
D Introduction	A charon
 Contraction Contraction Security 	Kan a suffixes.

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.)

Bookmarks 🥻 Location:	nttp://charon.emea.tivoli.com:81/ld	ap/cgi-bin/Idacgi.exe?Action=Star	t	🛨 🌍 What's Related
Directory Server Directory Server Directory Server Settings General Performance Transactions Event notification Suffices Referrals Schema Security Referrals Directory Servert	To add a suffix, enter the d Suffix DN ou=emea, The table below displays su		ffix, then clic	• ?. Removing a suffix
 Current state Logs 	Current server suffixes	Comment	Remove?	
🖸 Logoff	cn=localhost	System suffix		
	secAuthority=Default	Contains no directory data	Г	
	Update Reset	n, (v		

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:

rectory Server	Suffixes				
D Introduction	😔 charon				
General	The list was successfully updated. You must restart the server for this change to take effect.				
	To add a suffix, enter the di	istinguished name of the suf	fix, then click	pdate.	
Referrals Constraints Schema Security				uffix, select the checkbox and cli data is not removed from the dir	
Referrals C Schema Security Replication	The table below displays su	ctory data beneath that suff			
Referrals Schema Sccurity Replication Database Current state	The table below displays su eliminates access to all dire Current server suffixes	ctory data beneath that suff	ix, however th		
Referrals Schema Security Replication Database Current state Logs	The table below displays su eliminates access to all dire Current server suffixes cn=localhost	ctory data beneath that suff Comment	ix, however th Remove?		

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:

Directory Server	Stop
Introduction	Charon
Settings General	The directory server is running.
Performance	The directory server is currently running. To stop the server, click the Stop button.
 Event notification Suffixes 	Stop
Referrals Content in the second se	
Security	Related tasks:
Replication	
 Database Current state Server status 	 <u>Server status</u> - Display the current status of the server to review server activity. <u>Connections</u> - View the current connections to the server.
Connections	
Logs	

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 <u>restart the server</u> for these changes to take effect'. Click on '<u>restart the server</u>' 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:

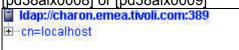
- run the Directory Management Tool on the same AIX box as that on which the directory is located;
- run the Directory Management Tool on a remote system and point it at the AIX box on which the directory is located.
- b. To start the Directory Management Tool on an AIX XWindows system, type dmt on the 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 "Idap://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):

Add server	1000 J
	?
Ready	IBM.
Connect to directory server Server name : Idap:// Port : 389 Use SSL; □ Certificate name : □ Authentication type : ○ None ⓒ Simple ⓒ BASL External ⓒ CRAM MD5 User password : ******* Keyclass file name : □ Keyclass file password : *******	C Kerberos

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:

IBM SecureWay Directory Management T	ool
📔 Idap://charon.emea.tivoli.com:389	Introduction
Introduction	Ready
Properties D Status D Administration	IBM SecureWay

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: [pd38aix0008] or [pd38aix0009]



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):

-]IE	M SecureWay Directory Management Tool		•
ldap://localhost:389	Rebind	?	
Introduction Server Properties Status	Ready	EM₀	
Administration	Enter a new bind DN and password for the server Idap://localhost.389		
Refresh schema Object classes Attributes	Anonymous Authenticated User DN: En=root.		
Matching rules Syntaxes Directory tree Browse tree	User password : ***********************************		
Refresh tree Search tree Sarch tree	OK Cancel Help		
Advanced search Log file View log file			
🖵 🗈 Clear log file			
Add server Delete server Exit	Delote		

Version 0.8 - 21 September, 2001

Tivoli Policy Director V3.8 – Installation Guidelines/Cookbook

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 redisplayed, showing the hostname in the top left hand corner:

— IBI	M SecureWay Directory Management Tool	· 🗆
Introduction	Browse tree	?
Server Properties Status Administration	Ready	
☐ ☐ Rebind	Operation Image: Search Image: Searc	
Object classes Attributes Matching rules Syntaxes	I Ida¤//localhost:389 Image: cn=localhost	
Directory tree Browse tree Brefresh tree Search tree		
Simple search Advanced search Log file		
Clear log file		
Add server Delete server Exit	I	

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.

Add an LD	AP Entry	×
Select an En	try type, enter the Parent DN, modify the Entry RDN, then click OK.	
Entry type	Organizational unit 💌	
Parent DN:		
Entry RDN:	ou=emea,o=kibm,c=gb	

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

Tivoli Policy Director V3.8 – Installation Guidelines/Cookbook

bject class: organizational N: ou=emea,o=ib Attributes	
ou: businessCategory: description: destinationIndicator: facsimileTelephoneNumber: internationalISDNNumber:	2 emea,o=kibm,c=gb 2
l: Office phone: physicalDeliveryOfficeName: postalAddress:	2 [] 2 [] 2 []

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:

Idap://charon.emea.tivoli.com:389	
一品 ou=emea,o=ibm,c=gb	
⊡-cn=localhost	

I. 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:

* INPUT device * SOFTWARE to PREVIEW only COMMIT softwa SAVE replace AUTOMATICALL EXTEND file OVERWRITE san VERIFY insta Include corre DETAILED out	? (install operation are updates? d files? Y install requisite s systems if space need ne or newer versions? ll and check file siz esponding LANGUAGE fi	ware will NOT occur) software? led? ses?	[Entry Field /dev/cd0 [PD no yes no yes yes no no yes no yes no yes	ls] > + + + + + + + + + + + + + + + + + +
F1=Help	F2=Refresh	F3=Cancel	F4=List	

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 Availab	le Software		
Type or select valu Press Enter AFTER m	es in entry fields. aking all desired ch	nanges.		
* SOFTWARE to insta PREVIEW only? (in COMMIT software u SAVE replaced fil AUTOMATICALLY ins EXTEND file syste OVERWRITE same or VERIFY install an	stall operation will pdates? es? tall requisite softw ms if space needed? newer versions? d check file sizes? ding LANGUAGE filese	NOT occur) vare?	<pre>[Entry Fields] /dev/cd0 [_all_latest no yes no yes yes no no yes no yes no yes no yes</pre>	+ + + + + + + + +
	F6=Command	F3=Cancel F7=Edit Enter=Do	F4=List F8=Image	

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]: 1Enter 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 DASCOM, Inc. All Rights Reserved. 2001-09-25-10:22:34.244-01:00I---- 0x1354A0A0 pdmgrd NOTICE ivc general ivmgrd. cpp 638 0x0000001 Server startup 2001-09-25-10:22:34.332-01:00I---- 0x1354A0A0 pdmgrd NOTICE ivc general ivmgrd. cpp 643 0x0000001 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 (PDAcld) 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 (PDAcld) Configuration 2. Policy Director WebSEAL (PDWeb) Configuration x. Return to Policy Director Setup Menu Please select the menu item [x]: 1Enter 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 ivacld 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 DASCOM, Inc. All Rights Reserved. 2001-09-25-10:39:54.939-01:00I---- 0x1354A0A0 pdacld NOTICE ivc general ivacld. cpp 410 0x0000001 Server startup 2001-09-25-10:39:54.978-01:00I---- 0x1354A0A0 pdacld NOTICE ivc general ivacld. cpp 415 0x0000001 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]: 1Enter 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 DASCOM, 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 ivacld
- /etc/iv/iv stop Stops pdmgrd and ivacld
- /etc/iv/iv status Displays status of pdmgrd and ivacld
- /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, pdacld 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
IBM SecureWay Directory Server 3.2 .... Not Installed
Press ENTER to continue...
```

- d. The details show will varry 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'

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:

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. Tivoli Policy Director V3.8 - Installation Guidelines/Cookbook

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] IBMldmzh TIBM SecureWay Directory Messages (zh)
9. [Not Installed] IBMldmzh TIBM 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:

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 Sst Keyfile
 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 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.
```

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

Version 0.8 – 21 September, 2001

```
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 Diectory client where 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
```

Version 0.8 – 21 September, 2001

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
Enab	ble 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)
- I. 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	
2. LDAP Administrator ID (DN)	
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 con	figuration:
1, 1 5	2

- o. This completes the manditory 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 Policy Director V3.8 - Installation Guidelines/Cookbook

```
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.

Version 0.8 - 21 September, 2001

Enable SSL between PD and LDAP on Domino? (Y $\mid N)$:

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

Version 0.8 - 21 September, 2001

is starting an error message may be displayed indicating 'An error occurred connecting to server "Idap://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):

🚭 IBM SecureWay Directory Management Tool		_ D ×
	Add server	?
	Ready	IBM.
	Connect to directory server Server name: Idap:// Charon.emea.tivoli.com Port: 389 Use SSL: Image: Connect Content Co	Kerberos
Add server Delete server Exit	OK Cancel Help	

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

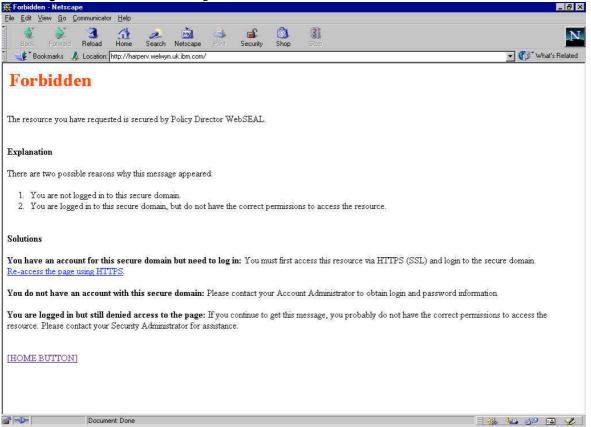
Solaris

- 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 <u>Re-access the page using HTTPS</u>, 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):



gned by: Tivoli Systems		ficate that is being presented:	
secret key) More Info			
e signer of the Certificate promises you that the holder of this Certificate is	Encryption:		More Info
o they say they are. The encryption level is an indication of how difficul uld be for someone to eavesdrop on any information exchanged betweer	who they say th	e Certificate promises you that the holder ey are. The encryption level is an indicat	of this Certification of how difficul

🔆 New Site Certificate - Netscape	X
New Site Certificate	
Are you willing to accept this certificate for the purposes of receiving encrypted information from this web site?	
This means that you will be able to browse through the site and receive documents from it and that all of these documents are protected from observation by a third party by encryption.	
C Accept this certificate for this session C Do not accept this certificate and do not connect	
Accept this certificate forever (until it expires)	
<back next=""> Cance</back>	
SDauk Next> Calles	



🔆 New Site Certificate - Netscape
New Site Certificate
You have finished examining the certificate presented by: harperv.welwyn.uk.ibm.com
You have decided to accept this certificate and have decided not to have Netscape Communicator warn you before you send information to this site.
If you change your mind, open Security Info from the Communicator Menu edit Site Certificates.
Click on the Finish button to begin receiving documents.
🔆 Certificate Name Check - Netscape



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):

Tivoli Policy Director V3.8 - Installation Guidelines/Cookbook

Username a	nd Passwo	rd Required	×
Enter userna charon emea			
User Name:	sec_master	1	
Password:	*****		
	0K.	Cancel	

- 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:

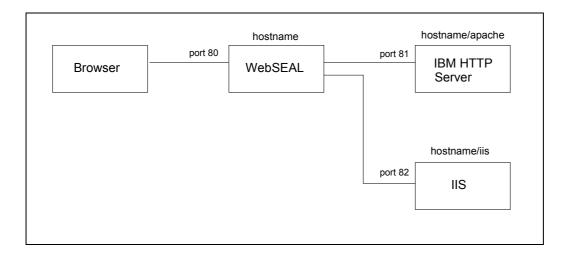


Tivoli Policy Director V3.8 – Installation Guidelines/Cookbook



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:

Tivoli Policy Director V3.8 – Installation Guidelines/Cookbook

```
# 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
  ivacld-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 juntioned 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
```

Version 0.8 - 21 September, 2001

```
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>
```

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 $/\mbox{cgi-}$

Tivoli Policy Director V3.8 – Installation Guidelines/Cookbook

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.

/₩₩ Service Pr	operties for harpe	erv.		2
Service Director	ies Logging Adva	nced		
<u>I</u> CP Port: <u>C</u> onnection Time <u>Maximum Conne</u>		seconds		
Anonymous Lo	gon IUSR_HARPERV			_
Password:	*****			=
Password Auth	onymous	oonse		
C <u>o</u> mment:				
	OK	Cancel	Apply	Help

- 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)

W Service Properties for harperv rvice Directories Logging Advanced			D
Directory C:\netPub\www.root C:\netPub\scripts C:\netPub\www.root\cgi-bin	Alias <home> /Scripts /cgi-bin</home>	Address	Erro
C:\WINNT\System32\inetsrv\iisadmh	/iisadmin Remove	Edit Prope	tion
Enable Default Document Default Document: Default.htm	Дениче		
Directory Browsing Allowed			

- Click on 'OK. I)
- Click on Properties -> Stop Service in Internet Service Manager to stop IIS. m)
- Click on Properties -> Start Service to re-start IIS. n)
- Ideally obtain a copy of query contents.exe written specifically to cope with the 0) 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\ietsrv\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\.;

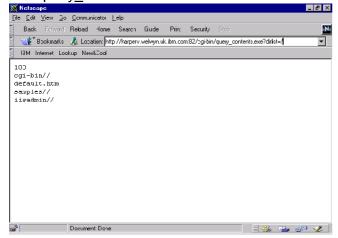
```
edit c:\winnt\guery contents.cfg to specify
docroot=c:\inetpub\wwwroot
```

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 /cgibin/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 lline 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 orgaization 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: Tivoli Policy Director V3.8 – Installation Guidelines/Cookbook

y Database File Create View Help	
	tabase information
Key	database content
Personal Certificates	▼ Receive
	Delete
	View/Edit
	Import
	Recreate Request
	New Self-Signed
	Extract Certificate
ersonal certificate has its associated private key in the d	atabase.

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

New		×
Key database type	CMS key database file 🛛 🔻	
File Name:	mypdsrv.kdb	Browse
Location:	C:\Program Files\Tivoli\PDWeb\www\certs\	
	OK Cancel Help	

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:

Key database information B-Type: CMS key database file lie Name: C:\Program Files\Tivol\PDWeb\www\certs\mypdsiv.kdb		
Key database content		
Signer Certificates	-	Add
Fhawte Personal Premium CA		Delete
Fhawte Personal Freemail CA		1
Thawte Personal Basic CA		View/Edit
Thawte Premium Server CA		
Fhawte Server CA		Extract
/erisign Test CA Root Certificate		1
RSA Secure Server Certification Authority /eriSion Class 1 CA Individual Subscriber-Persona Not Validated		
/ensign Class 1 CA Individual Subscriber-Persona Not Validated		
/eriSign Class 2 CA Individual Subscriber-Persona Not Validated		
/erisign Class 5 CA Individual Subscriber Persona Not Validated		
/erisign Class 2 Public Primary Certification Authority		
/erisign Class 2 Fublic Frimary Certification Authority		
-Tan 12 12		

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.)

Key Label		test-webseal-cert	
Version		X509 V3 🔻	
Key Size		1024 💌	
Common Name		harperv.welwyn.uk.ibm.com	
Organization		Tivoli	
Organization Unit	(optional)		
ocality	(optional)		
State/Province	(optional)		
Zipcode	(optional)		
Country		GB 🔻	
Validity Period		365 Days	

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

iatabase File Create View Help	
Key database information	
Type: CMS key database file	
Name: C:\Program Files\Tivoli\PDWeb\www.certs\mypdsrv.kdb	
Key database content	
rsonal Certificates	▼ Receive
est-webseal-cert	Delete
	View/Edit
	Export/Import
	Recreate Request
List of personal certificates. Default indicate	ed with *
	New Self-Signed
	Extract Certificate

- 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).
- I. 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:

BM Key Management	
Key Database File Create View Help	
Key database info	rmation
DB-Type:	
File Name:	
Key database c	ontent
Personal Certificates	Receive
	Delete
	View/Edit
	Import
	Recreate Request
	New Self-Signed
	Extract Certificate
A personal certificate has its associated private key in the database.	

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

ew	41	2
Key database type	CMS key database file 🔹	
File Name:	mypdsrv.kdb	Browse
Location:	C:\Program Files\Tivoli\PDWeb\www\certs\	
	OK Cancel Help	

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:

Password: Confirm Password:	+***
Set expiration time?	60 Days
🗹 Stash the pa	ssword to a file?
ssword Strength:	

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:

Key database information		
B-Type: CMS key database file		
Ile Name: C:\Program Files\Tivoli\PDWeb\www\certs\mypdsrv.kdb		
Key database content		
Signer Certificates	•	Add
Thawte Personal Premium CA		Delete
Thawte Personal Freemail CA		
Thawte Personal Basic CA		View/Edit
Thawte Premium Server CA		
Thawte Server CA		Extract
/erisign Test CA Root Certificate		1
RSA Secure Server Certification Authority		
/eriSign Class 1 CA Individual Subscriber-Persona Not Validated		
/eriSign Class 2 CA Individual Subscriber-Persona Not Validated		
/eriSign Class 3 CA Individual Subscriber-Persona Not Validated		
/erisign Class 1 Public Primary Certification Authority /erisign Class 2 Public Primary Certification Authority	_	
/erisign Class 2 Public Primary Certification Authority /origins Class 3 Public Primary Certification Authority	_	
/erisign Class 3 Public Primary Certification Authority		

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.)

lease provide the	ronowing.		
Key Label		test-webseal-cert	
(ey Size		1024 🔻	
Common Name		harperv.welwyn.uk.ibm.com	
Organization		Tivoli	
Organization Unit	(optional)		
.ocality	(optional)		
State/Province	(optional)		
lipcode	(optional)		
Country		GB 🔻	
-			
Enter the name of	a file in whi	ch to store the certificate request:	
C:\Program Files	(Tivoli\PDWe	eb\www\certs\mypdsrvcertreq.arm	Browse
			25

i. Click on 'OK'; an information message will inform you where the certificate request has been stored:

nformatio	n	2
ů	A new certificate request has been successfully created in the file: C:\Program Files\Trivoli\PDWeb\www.certs\mypdsvcertreq.arm. You must send the file to a certification authority to request a certificate.	
	OK	

- 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.)
- I. Select Enrolment Type as Server or Device Certificate and Action as Enrol:

Tivoli SecureWay	
Tivoli PKI	
WA -	Credential Central
Before enrolling for any certificate, you must first (<u>CA) certificate</u> in your browser. This certificat enrollment facility in a secure, authenticated sessi	e enables your browser to connect to the
After the CA certificate is installed in your brows certificate preregistration. If eligible, you can rene certificate. From this page, you can also check th	w, revoke, or suspend an existing browser
1. Select the Enrollment Type:	
 Browser Certificate for Netscape Comm Internet Explorer 50 or later. 	aunicator or Navigator 4.05 or later, and Microsoft
	requested only by system administrators, enrollment generates a PKCS #10 certificate request and ed in Base64-encoded or binary format.
	er an applicant for a certificate. After the certificate Trust Authority Client (or other PKIX compatible ificate.
Select an option from the Action list. Rene browser certificates.	ew, Revoke, and Suspend apply only to
3. Click OK to continue.	
Certificate Enrollment	
Enrollment Type: Server or	Device Certificate 🔽
Action: Enroll	• OK

- 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:

💥 Server and Device Certificate En			_ 8 ×
<u>File Edit View Go Communicator H</u>	<u>i</u> elp		
Back Forward Reload H	🚹 🎿 🚵 斗 🐴 ome Search Netscape Print Security	Shop Stop	N
🧵 ॳ Bookmarks 🙏 Location: http	s://demota.dfw.ibm.com/YourDomain/PKCS107Cert_	EnrolLisp	🚽 🍘 What's Related
	Tivoli SecureWay	<u>></u> ∕///	
		Server and Device Certificate	
	To request a certificate for a server or o and accepts a raw or PKCS #7 certific	levice that generates a PKCS #10 certificate request ate in response:	_
	1. Complete both parts of the enrol	lment form. All fields are case-sensitive.	
	2. Click Submit Enrollment Requ	iest.	
	request. If your request is approved, yo	ive instructions for checking the status of your ur certificate will be displayed on-screen. Copy and d then follow your server's instructions to install the	
	Registration Information		
	Select the type of certificate you need (see <u>description</u>).	Type of Certificate: (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.	Save CA Certificate to File	
Document	Done		

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 BEGINE NEW CERTIFICATE REQUEST to END NEW CERTIFICATE REQUEST, then copy this to the 'PKCS #10 Certificate Request' area on the browser input form:

	Ka. SHIR
Tivoli PKI	
Server and Device Cer	ertificate
To request a certificate for a server or device that generates a PKCS #10 certificate requ and accepts a raw or PKCS #7 certificate in response:	uest
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 a save the certificate response to a file, and then follow your server's instructions to install th certificate.	
Registration Information	
Select tha type of certificate: (beguted) description). Type of Certificate: (beguted) Web Server Authentication (1-Year)	
If this is the first time that you are requesting server of device enrollment, you need to save the CA certificate to a file and install in your server or the device prior to installing the server or device certificate.	
Type your first name or given name and, pitionally, your middle name or initial.	
Type your last name, family name, or sumame. [Required] Harper	
Type your s-mail address; including the at sign (@) and any periods (). This s-mail address is required by some certificate types, such as those used for secure s-mail.	
Select this option to receive an e-mail notification when your request has been finalized	
	-
Type a Challenge Question and a Response Challenge Question: (Optional)	
that are special to you and easy to remember. If you are asked the same Challenge Question when you check your errollment status, you must respond with Challenge Response: (Optimal)	
that are special to you and easy to remember. If you are asked the same Challenge Question when you check your	
that are special to you and easy to remember. If you are asked the same Challenge Question when you check your errollment status, you must respond with Challenge Response: (Optimal)	
that are special to you and eary to remember 17 you are asked the same Challenge Question when you check your enrollment atlank, you must respond with the same Challenge Response. Certificate Request Information PKCS #10 Certificate Request: (Sequest)	3 5 5 8 9 9
that are special to you are asked the same Challenge Question when you check your remollment atlank, you must represent white the same Challenge Response. Challenge Response: (Optional) Certificate Request Information PKCS #10 Certificate Request: (Seguid) Copy and pasts here the content of the PKCS #10 certificate request (Seguid) Life are the content of the PKCS #10 certificate request (Seguid) Life are the content of the PKCS #10 certificate request (Seguid) Life are the content of the PKCS #10 certificate request (Seguid) Life are the certificate request to a file, open the file in a test editor such as Noteped, and then copy and past here the certificate request to a file, open the file in a test editor such as Noteped, and then copy and past here the certificate request to a file, open the file in a test editor such as Noteped, and then copy and past here the certificate request of past of the PKCS #10 Certificate Request: (Seguid) NBXIO Such as the servers of device for which you are request the certificate request to a file, open the file in a test editor such as Noteped, and then copy and past the certificate request to a file, open the file in a test editor such as Noteped, and then copy and past the certificate request to a file, open the file in a test editor such as Noteped, and then copy and past the certificate request to a file, open the certificate request to affile, open the certificate request to a file, open the file in a test editor such as Noteped, and then copy and past the certificate request to a file, open the certificate file and the certificate file and the certificate file as the certificate file as the cerificate file as the certificate file as the certificat	3 5 5 5 8 9 7 9 9
that are special to you and easy to remember. If you are saded the special or white you are saded the special with the same Challenge Response. Certificate Request Information Corrificate Request Information PKCS #10 Certificate Request: (%quad) Corrificate Request Information Corpy and pasts here the conduct of the PKCS #10 Certificate Request: (%quad) Corpy and pasts here the conduct of the PKCS #10 Certificate Request: (%quad) Corpy and pasts here the conduct of the PKCS #10 Certificate Request: (%quad) SKE of PKCS #10 Certificate Request: (%quad) Corpy and pasts here the conduct of the PKCS #10 Certificate Request: (%quad) Corpy and pasts here the certificate request to a file, open the file in a teat editor such as Noteped, and there corpy and pasts here etificate request to affile, open the file in a teat REMONARCE TREE INFORMATE	3 5 5 5 8 9 7 9 9 9 9 9
that are special to you are ased the same Challenge Question when you check your renolment states, you must seep on whith the same Challenge Response. (Qutanu) Certificate Request Information Copy and pasts here the content of the PICOS #10 certificate Request: (Sequate) (Copy and pasts here the content of the PICOS #10 certificate Request: (Sequate) (Copy and pasts here the content of the PICOS #10 certificate request (Sequate) (December 2000 Certificate Request: (Sequate) (Copy and pasts here the content of the PICOS #10 certificate request (Sequate) (December 2000 Certificate Request: (Sequate) (Copy and pasts here the content of the PICOS #10 certificate request (Sequate) (December 2000 Certificate Request: (Sequate) (Copy and pasts here the content of the PICOS #10 certificate request (Sequate) (December 2000 Certificate Request: (Sequate) (Copy and pasts here the content of the PICOS #10 certificate request (Sequate) (December 2000 Certificate Request: (Sequate) (Copy and pasts here the certificate request here. The data you certer helwer will werefide the data is your PICCS #10 Breth exame field. Leave the Michael Michael Michael (Sequate) (Comment Name: (Optimal) (Comment Name: (Optimal)) (Comment Name:	3 5 5 5 5 8 9 7 9 9 9
that are special to you are ased the same Challenge Question when you check your remember If you are aside the same Challenge Question when you check your Challenge Response: ((bjtami)) Certificate Request Information Certificate Request (control of the same challenge Response) Cortificate Request Information PKCS #10 Certificate Request: (control of the same challenge Response) Cortificate Request Information PKCS #10 Certificate Request: (control of the same challenge Response) Copy and pasts here the content of the PKCS #10 certificate request (see samplo have segmentable) PKCS #10 Certificate Request: (control of the same challenge Response) This RefTCS to Information PKCS #10 Certificate Request: (control of the same challenge Response) If you are you do sate here the content of the PKCS #10 certificate request (control of the same disc and then copy and pasts the entificate request to a file, open the file in a test request here. PKCS #10 certificate Request: (control of the same field. Locket Response) Difficate Request the entificate request here. PKCS #10 certificate Request the same field. Locket field hash type a bready entered the task in your PKCS #10 for the same field. Locket field hash type a bready entered the task in your PKCS #10 for the same field. Locket field hash type a bready entered the task in your PKCS #10 for the same field. Locket field hash type a bready entered the task in your PKCS #10 for the same field. Locket field hash type a bready entered the task in your PKCS #10 for the same field. Locket field hash type a bready entered the task in your PKCS #10 for the same field. Locket field hash type a	3 5 5 5 8 9 7 9 9
this we special to you are ased the same Challenge Question when you check you remember If you are ased the same Challenge Response. Challenge Response: (Quuma) Certificate Request Information PKCS #10 Certificate Request: (Squad) Corresponder States and the same of the same challenge Response. PKCS #10 Certificate Request: (Squad) Corresponder States and the same of the same challenge Response. PKCS #10 Certificate Request: (Squad) Corresponder States and the same of the same challenge Response. PKCS #10 Certificate Request: (Squad) Corresponder States and the same of a same of the same distance of the same field. Level field black if you are agained the field is the hostename of your sequest and the contain the Common Name. Type the leggly regulated name of your engagest and the contain the Common Name. Organization Name: (Quimal) Type the name of your division or department, such as Human Resources of Software Organizational Unit: (Quimal) Type the name of your division or department, such as Human Resources of Software Organizational Unit: (Quimal)	3 5 5 5 8 9 7 9 9
that are special to you are aside the same Challenge Question when you check your recolument failers, you must expond with the same Challenge Response. Challenge Response: (tytenul) Certificate Request Information Certificate Request: (cytenul) Copy and pasts here the content of the PKCS #10 certificate request (see ampli) that was generated by the server of device for which you saved the was generated by the server of device for which you saved the resplication of different endities in request (see ampli) that was generated by the server of device for which you saved the resplication of dots much as holgs and copy and pasts here the content of the PKCS #10 certificate request (see ampli) that was generated by the server of device for which you saved the resplication of dots much as holgs and much copy and pasts the certificate request here. PKCS #10 Certificate Request: (cytemu) The data you exter hele with copy and pasts the certificate request here. Common Name: (cytema) The data you exter hele with ext of the PKCS #10 request and do are the second field. The prove PKCS #10 request and do are which to everify it. The data you exter hele with ext of the field is required if the PKCS #10 certificate request doe and contain the Common Name. Common Name: (cytema) Type the legally registered name of your organization Resources on Software Development. Organization Name: (cytema) Type the satter address of your Sheet Address: (cytema)	3 5 5 5 5 8 9 7 9 9 9
this we special to you are saded the same Challenge Question when you check you renolment failing, you must repeated with the same Challenge Response. Challenge Response: (Quuma) Certificate Request Information PKCS #10 Certificate Request: (Squard) Corresponder State States and the States and th	3 5 5 5 8 9 7 9 9 9 9 9
this we special to you and easy to remember if you are saded the same Challenge Question when you check you recommend sharp, you must expendent sharp of the same Challenge Response. Challenge Response: (typend) Certificate Request Information Certificate Request Informa	3 c b c b b b v v v v

- 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 Erollment 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:

Server and Device Certificate
Your enrollment request has been approved and your certificate is as follows:
MIIDEDCCAm2gAwIBAgICAZIwDQYKoZIhvcNAQEFBQAwYDELMAKGAIUEBhMCVVHxG jAYBGNVBACTEVIvdXigT3 JnYUSpemF0 GuSyMHRgwFgTVVQCLEwSUcnVzdCBBdXRob3 JpAHKxCaX28gNVBAHTI HgXdNDIFIdCVvmLGSBD71AF90W1X38JUXHZMHTT AFWUMJASJSJXHZMATHATHIHLMGwCQTVVQCEwJH0JSTHBECGmSJ3om73ixKARKT AZNVFJTFHBECGMSJ3Om75ixKARTAZIJHEBHACGmSJ3Om75ixKARTAN'HRYWF AYKCIImiZPyLGOBGRHGdZVm3J1MKFCXITSBACGmSJ3Om75ixKARTAN'HRYWF AYKCIImiZPyLGOBGRHGdZVm3J1MKFCXITSBACGmSJ3Om75ixKARTAN'HRYWF AYKCIImiZPyLGOBGRHGdZVm3J1MKFCXITSBACGmSJ3Om75ixKARTAN'HRYWF AYKCIImiZPyLGOBGRHGdZVm3J1MKFCXITSBACGmSJ3Om75ixKARTAN'HRYWF AYKCIImiZPyLGOBGRHGdZVm3J1MKFCXITSBACGmSJ3Om75ixKARTAN'HRYWF AYKCIImiZPyLGOBGRHGdZVm3J1MKFCXITSBACGmSJ3Om75ixKARTAN'HRYWF AYKCIImiZPyLGABGRHGAZVm3J1MKFCXITSBACGmSJ3Om75ixKARTAN'HRYWF AYKCIImiZPyLGABGRHGAZVm3J1MKFCXITSBACGmSJ3Om75ixKARTAN'HRYWF AYKCIImiZPyLGABGRHGAZVm3J1MKFCXITSBACGMSJ3OM75ixKARTAN'HRYWF AYKCIImiZPyLGABGRHGAZVm3J1MKFCXITSBACGMSJ3OM75ixKARTAN'HRYWF AYKCIImiZPyLGABGRHGAZVm3J1MKFCXITSBACGMSJ3OM75ixKARTAN'HRYWF AYKCIIMIZPYLGAUXFCXITSPYTSWXGBABGRFYOTYSFXARTAN'HX GAIUDAVEKJYWZELAYTFAWGABARTAN'HYWFUDDAKGGGFBYFDCCATAGBGWNHSABCTAHHANG GAIUDAVEKJWZELAYTFAWGABARTATSBACFWYFVDF03BACCATAGBGWNHSABCTAHHANG GAIUDAVEFBQAHGFCGCJFFBWAHTATSBACFWYFDDIJAWCCATRABGRHMABGWDOVJXK oZIhvCNAQEFBQAHGFCGGTFBWAHTATSBACFWYFDDIJAWCCATRABGRMAHGWDOVJXK oZIhvCNAQEFBQAHGFGCGFBWZ3XZEQH71LJUWJQYPC4SC9BBGG2C0SRGDIFFE
To install this certificate to your server, first select the certificate format required by your server and click Save Certificate to Disk . Then import the file to your server by following instructions provided by your server's certificate and key management program. If this machine is also your server, you should still save the file as a backup and then follow your server's instructions to install the certificate.
Certificate File Format:
C Base64 Encoded PKCS #7 Certificate for PC (CRLF) C Base64 Encoded PKCS #7 Certificate for UNIX (LF only) C Base64 Encoded Raw Certificate for PC (CRLF) C Base64 Encoded Raw Certificate for UNIX (LF only) C Binary FKCS #7 Certificate C Binary Raw Certificate
Save Certificate to Disk Return to Credential Central

- 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:

Reveal and the second s	
lle Name: [C:\Program Files\Tivoli\PDWeb\www.certs\mypdsv.kdb Key database content	
Signer Certificates	▼ Add
Thawte Personal Premium CA Thawte Personal Freemail CA	Delete
Thawte Personal Basic CA Thawte Premium Server CA	View/Edit
Thawte Server CA /erisign Test CA Root Certificate RSA Secure Server Certification Authority	Extract
/eriSign Class 1 CA Individual Subscriber-Persona Not Validated /eriSign Class 2 CA Individual Subscriber-Persona Not Validated /eriSign Class 3 CA Individual Subscriber-Persona Not Validated	
Verisign Class 1 Public Primary Certification Authority Verisign Class 2 Public Primary Certification Authority Verisign Class 3 Public Primary Certification Authority	

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\Tivo Add CA's Certificate fro	oli\PDWeb\www\certs\CACertRaw.b64	our case
Data type	Base64-encoded ASCII data 🔻	
Certificate file name:	CACertRaw.b64	Browse
Location:	C:\Program Files\Tivoli\PDWeb\www.certs\][
	OK Cancel Help	

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:

B-Type: CMS key database file le Name: C:\Program Files\Tivoli\PDWeb\www.certs\mypdsrv.kdb Key database content		
le Name: C:\Program Files\Tivoli\PDWeb\www\certs\mypdsrv.kdb		
Kou database content		
rvey udiabase content		
Signer Certificatés	•	Add
ivoli PKI Demo System CA Certificate		Delete
'hawte Personal Premium CA		
'hawte Personal Freemail CA		View/Edit
'hawte Personal Basic CA		
'hawte Premium Server CA		Extract
hawte Server CA		
/erisign Test CA Root Certificate		
RSA Secure Server Certification Authority		
/eriSign Class 1 CA Individual Subscriber-Persona Not Validated		
/eriSign Class 2 CA Individual Subscriber-Persona Not Validated		
/eriSign Class 3 CA Individual Subscriber-Persona Not Validated		
/erisign Class 1 Public Primary Certification Authority		
in the e uty down and the pathology and the pathology of		

z. Select 'Personal Certificates' from the pull-down list:

Key database information	
-Type: CMS key database file	
e Name: C:\Program Files\Tivoli\PDWeb\www\certs\mypdsrv.kdb	
Key database content	
ersonal Certificates	Receive
	Delete
	View/Edit
	Import
	Recreate Request
	New Self-Signed
	Extract Certificate

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:

Receive Certificate fro	m a File	×
Data type	Base64-encoded ASCII data 🔻	
Certificate file name:	RawCert.b64	Browse
Location:	C:\Program Files\Tivoli\PDWeb\www\certs\	
-	OK Cancel Help	

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 (*).)

Key database information	
Type: CMS key database file	
e Name: C:\Program Files\Tivoli\PDWeb\www.certs\mypdsrv.kdb	
Key database content	
ersonal Certificates	Receive
test-webseal-cert	Delete
	View/Edit
	Export/Import
	Recreate Request
List of personal certificates. Default indicate	1 with *
	New Self-Signed
	- non con cigitain

	Error Message	1
	A database validation error occurred.	
	ОК	
Note: If you receive an Erro	or Message indicating 'A database	e validation error occurred', this is
2	, ,	sonal Certificates which are either list of Signer Certificates. The step
o o ,	g the CA Certificate should prever	•

cc. The IBM Key Management utility is no longer required and may be closed.

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: 👪 IBM Key Management - 🗆 × Key Database File Create View Help Key database information DB-Type: File Name Key database content **Personal Certificates** • Recreate Request New Self-Signed.
 - A personal certificate has its associated private key in the database.
- d. Create a new Key Database: click on Key Database <u>File</u> -> New, and specify a File Name and Location. We used mypdsrv.kdb, C:\Program Files\Tivoli\PDWeb\www\certs\:

New		>
Key database type	CMS key database file 🔹	
File Name:	mypdsrv.kdb	Browse
Location:	C:\Program Files\Tivoli\PDWeb\www\certs\	
	OK Cancel Help	

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:

Confirm Password:	****
Set expiration time?	60 Days
	ssword to a file?
sword Strength:	
$ \rightarrow	

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:

Key database information	
B-Type: CMS key database file	
le Name: C:\Program Files\Tivoli\PDWeb\www\certs\mypdsiv.kdb	
Key database content	
Signer Certificatés	▼ Add
Fhawte Personal Premium CA	Delete
Fhawte Personal Freemail CA	1
Fhawte Personal Basic CA	View/Edit
Fhawte Premium Server CA	
Fhawte Server CA	Extract
/erisign Test CA Root Certificate RSA Secure Server Certification Authority	
/eriSign Class 1 CA Individual Subscriber-Persona Not Validated	
/eriSign Class 2 CA Individual Subscriber-Persona Not Validated	
/eriSign Class 2 CA Individual Subscriber-Persona Not Validated	
/erisign Class 1 Public Primary Certification Authority	
/erisign Class 2 Public Primary Certification Authority	
consign stass 21 dens i innar), sonansansansing	

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.)

Browse

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:

e <u>E</u> dît <u>V</u> iew <u>G</u> o <u>C</u> omm	unicator <u>H</u> elp	
Back Forward Re	🚹 🏠 🧀 🚵 🛋 📦 🦥 Ioad Home Search Netscape Prot Security Shop Stop	N
🆋 Bookmarks 🤌 M	letsite. http://freecerts.entrust.com/webcerts/index.htm	💌 🌍 🖤 What's Related
CONTACT US VISIT WWW.ENTE Dowerd by Entruct Inc. REQUEST A WEB REQUEST REQUEST REQUEST REQUEST REQUEST REQUEST	UST.COM	
	What is a Certificate? A cettifacte is a corporaphically signed object that binds a public key and an identify. Certificates can also include other information in extensions such as permissions and comments. A "Cell's is inder for Certification Authority and is an instand al entity or tutated thid party (such as Entrut CA) that issues, signs, revokes, and manages digital cartificates.	
	If you want to read more about web security, please read our <u>Web Security Primer</u> . What is a PKI?	
	The comprehensive system required to provide publickey encryption and digital signature services is from as a publickey infrastructure PKI.	
	http://www.entrust.com/	

I. 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
VISIT WWW_ENT	RUST.COM WEB VPN SET
powered by Entrust" Inc	
REQUEST A WEB	Step 1 - Accept and Fill out the Application
BROWSER CERTIFICATE REQUEST A WEB SERVER CERTIFICATE CONNECT TO OUR SECURE WEB SERVER	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:
ABOUT THIS DEMO	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: * Vaughan
	Last Name: * Harper
	Company:
	Email: * vaughan_harper8uk.ibm.com
	Phone:
	You are interested in Freecerts for the purpose of: *
	Which Web server are you using?
	Other
	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 ARREE AND ACHRONIZEDE THAT THE CERTIFICATE ISSUED TO YOUR BY BECLUSINGEY. FOR DUCATION AND THE ORIGINAL STATUS OF THE DECOMMENDATION OF THE ORIGINAL STATUS OF THE ORIGINAL NO CIRCUMSTANCES SHOULD THE FREE CERTIFICATES E USED FOR COMMERCIAL PUPPOSES. EACH TREE CERTIFICATES FULL OF A PERIOD OF SITT (80) DAYS. YOU ACKNOWLEDGE AND UNDERSTAND THAT THERE WAS ITS BEAT AARKORNING CHECK PERFORMED ON THE CAN DYNUF FURTHER RECOONLET THAT THE CERTIFICATE SHOULD THE CAN DYNUE AND YOU FURTHER RECOONLET THAT THE CERTIFICATE AS NOT SEEN
	Do you accept the terms and conditions as set out above. *
	C Yes C No
	Proceed to Step 2
	 required fields.
The certificates issued to you	WEB VPR GET
commercial purposes. You sho certificate requests are approv	uid also be aware that we do not verify the identity of persons who request certificates. All ed automatically:
@2000 Entrust®, Inc. All Right	s Reserved.
SET is a trademark of the SET	f 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.

ile <u>E</u> dit ⊻iew <u>G</u> o <u>C</u> om		
	诸 🏠 🥕 🚵 斗 🛋 🔕 🧌	Ň
📲 Bookmarks 🎉	Netsite: http://freecerts.entrust.com/cgi/bin/register.pl	💌 🌍 * What's Related
CONTACT US VISIT WWW.ENT powered by Entrust" In WEB REQUEST A WEB BROWSER CERTIFICATE REQUEST A WEB SERVER CERTIFICATE		
CONNECT TO OUR SECURE WEB SERVER ABOUT THIS DEMO	as www.myserver.com. Server Name: harperv.welwyn.uk.ibm.com Proceed to Step 3	
commercial purposes. You sh certificate requests are appro ©2000 Entrust©, Inc. All Righ		

- n. Click on 'Proceed to Step 3'.
- o. 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 BEGINE NEW CERTIFICATE REQUEST to END NEW CERTIFICATE REQUEST, then copy this to the Request area on the browser input form. Ensure that Options is set to 'displayed as PEM encoding of certificates in raw DER':

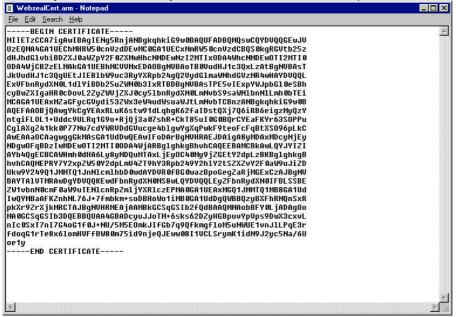
	CERTIFICATES
VISIT WWW_ENT	WEB VPN SET
powered by Entrust" Inc	
WEB REQUEST & WEB	Step 3 - Retrieve Certificate
BROWSER CERTIFICATE REQUEST A WEB SERVER CERTIFICATE CONNECT TO OUR SECURE WEB SERVER	The Authorization Code and Reference Number are used to retrieve your certificate from the Entrust/PKI. Typically to adhere to a company's security policy, authorization codes would be transmitted to users out-of-band (eg. telephone, secure e-mail) to ensure that the certificate issued remain secure and trusted.
ABOUT THIS DEMO	However, for the purpose of this demo, your Authorization Code has been supplied automatically and is displayed below.
	Auth Code: 60102110102-T082 Ref Number: 08908059
	In the fields below, you must paste the certificate request from your server. You can choose to view the certificate response in raw DER format or in PKCS #7. This depends on the format which is needed by your server.
	Options: displayed as PEM encoding of certificate in raw DER
	Please enter your server certificate request (PKCS#10 request) in the following field. Make sure that your Common Name (CN) matches the reference number of the certificate being retrieved when generating the request. If you do not know how to generate this request, please consult your server documentation.
	BEGIN NEW CERTIFICATE REDUEST Millight Common Section 2000 Securit/DJEP MA00A1UEChM0V02222 V0DDEbu-V0X-XX22LaDH85bit 3ag5/minur230M16HA00G5ag58lb3D2 AA0HADCB0KBgDDFEudrag30300ug6Am28ag0318etH02EH02EH02EH02EH02EH02EH02EH02EH02EH02E
	Submit Request Reset
	with B with B<
©1999 Entrust Technologies.	
SET is a trademark of the SET	Secure Electronic Transaction, LLC.

p. Click on 'Submit Request'. The web site will respond with a Server Certificate (in raw DER):

Version 0.8 - 21 September, 2001

CERTIFICATES
CONTACT US WEB VPN SET
powered by Entrust Inc.
WEB Step 4 - Server Certificate Retrieval
REQUEST A WEB
This is your dever certaincale (in faw DErV), copy the entire certaincale into your
SERVER CERTIFICATE what is between the lines "BEGIN CERTIFICATE" and "END CERTIFICATE". If you are
connect to due using Netscape Enterprise Server, you should copy everything (i.e., including the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines) For instructions on how to
secure your server using this certificate, please consult your server documentation.
audul twis DECIN_CERTIFICATE BW0 MILETCCA7: gast Haal ENDS Fin ANBERdah: G9*0BA0UFADBOMO.wcQVDY0QCEvJV UZEDMAAGAIUECAHRWS Dc.VYadDEvMC0GAIUECAHRWS Dc.VYadDEOSDG/RXV1EA5z GHJAGAIUECAHRWS Dc.VYadDEvMC0GAIUECAHRWS Dc.VYadDEOSDG/RXV1EA5z GHJAGI vis BDZXJO AU ZyZYF2CZXM-MILENDROWEN ZITXI XXOZA MWNDRWDT I XNTI 0 ODA44';CE2zELMAKGAIUEEDMKCVMAEDAOSMYBACTEDVUGHI 1::3'GxLat BBYWDBacT JLYudH1::3'GyUELY I TERLIB'US: STYRED 2'4'GQZYGGLiawBMC4GYERAYHANTDVQOL EXYFDINYAKNOI 1: HIEND 2'SUZYNDD 3 I ANTFDDEWWBACTESV'LENFYWJDALO HOSEDN CCA2ALTDEHNUCCYNLS SZUZYND 3 I ANTFDDEWWBACTESV'LENFYWJDALO HOSEDN CCA2ALTDEHNUCCYNLS SZUZYND 3 I ANTFDDEWWBACTESV'LENFYWJDALO HOSEDN ACEFAADBJOARG KALLAKSKULLAKSKUYJALLOHSKÓ ZI ALD XLONG KALLANDEN KALHONDO HOSEN CCA3ALTDEHNUCCYNLS SZUZYND 3 I ANTFDDEWWBACTESV'LENFYWJDALO HOSEDN ACEFAADBJOARG KALAKAKUPY 7NN/CA'YWRDGY'LUGAYHALANDEN KALHONDO HOSEN CCA3ALTANE KALAKAKUPY 7NN/CA'YWRDGY'LUGAYHALANDEN KALHONDO HOSEN ACEFAADBJOARG KALAKAKUPY TANYCAYWRDGY BAGAYES HANG KALANDEN KALHONDO HOSEN CCA3ALTANE KALAKALANDEN KALANDEN KALANDEN KALHONDO HOSEN MCGAADAGAUGAUHANGA KALANDEN K
END CERTIFICATE Client Authentication
If you wish to perform client authentication with users who have been issued certificates from this demo, you must also import the CA certificate into your Web server.
Retrieve the CA Certificate
WEB VPN SET
The certificates issued to you on these web sites are intended for demonstration purposes only. They must not be used for communical purposes. You should also be aware that we do not verify the identity of persons who request certificates. All certificate request are approved automaticality.
©1990 Entrust Technologies. All Rights Reserved.
SET is a trademark of the SET Secure Electronic Transaction, LLC.

q. 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\WebsealCert.arm. You may need to manually edit the file to remove the spaces at the beginning of each line:



r. Click on 'Retrieve the CA Certificate'. The PEM encoding of the CA Certificate will be displayed:

CERTIFICATES
VISIT WWW.ENTRUST.COM
VISIT WWW.ENTROST.COM
pomico of Linda no.
Step 5 - CA Certificate Retrieval (PEM encoding)
REQUEST A WEB
ROWSER CENTIFICATE This is the Certification Authority (CA) certificate. Copy the entire certificate into your
REQUEST A WEB /clipboard. If it is going to be installed into Microsoft Internet Information Server, only copy
SERVER CERTIFICATE what is between the lines "BEGIN CERTIFICATE" and "END CERTIFICATE". If you are using Netscape Enterprise Server, you should copy everything (i.e., including the
CONNECT TO OUR PIECE/CONTRIPTING A CONTRICT AND CONTRICT TO CONTRICT AND CONTRACT AND CONTRACT AND CONTRACT AND CONTRACT
SECURE WEB SERVER
ASOUT THIS HIDR2CCATCAAVBAGIENOVG5jANBqKghkiG9v0BA0UFADB0HQsvCQYDVQQGEvJV
UzEQMA4GA1UEChMHRW50cnVzdDEvMC0GA1UECxMmRW50cnVzdCBQS0kgRGVtb25z
dIJhaGlvbiBDZXJ0aWZpYZF0ZXMwHhcNOTgv0TI1MTc1NDBVhcNMTgw0TI1MTgy NDM5WiBONGwC0YDV0CGEvJVUzEOMAACA1UECHMRFV50cnVzdDzv4DCGA1UECMm
RW50cnVzdCBQS0kqRGVtb25zdHJhdG1vbiBDZXJ0aVZpY2F0ZXMvqZ0vDQYJKcZI
hvcNAOEBB0ADgYsAMIGHAoGBAL+pM0rRaFfDjulxLqlAlMY97Dt5OLRa4jo4C3 st+PV0k51rBlibLoppcgrCf84x352701havB0K2897TM41LFVCicKw8PvGvC
UeAVRD5i+s0pWnzZGuTIobIfamIW9alT6QbxeN/Lm4niNtnnqCfNz3ir3Rku642m
XNf9AgEDo4IBLjCCASowEQYJYIZIAYD4QgEDBAQDA3AHNHCSAIUdHwFxMGXwZ6BL GOVYTBHY0seCQYDVQCBEJVUJEZONA4GAIUECAHNFS9CsnVadDEWCOGAIUECxMa
RW50cnVzdCBQS0kqRGVtb25zdHJhdG1vbiBDZXJ0aVZpY2F0ZXMxDTALBqNVBAMT
BENSTDE¥KvFDVRODBCQvIoAPMTKSODASHjUxNzUDMzIaq09yDDE4MDkyNTE3NTOz OVovCvFDVROPBADDAGGOBBGAIUdIvOYMBaFKZnANI75J+7 inbka+soDBHoUoli
MBOGALUDgoWBB5mZ4T5++ii355.JvrKawR67qNVjAMBgVVHMEBTADAOH/MBKG CSgr5Lb2f0DBAAOMMabbBFVDLiADaGSMAOCSGr5Lb3D0EBBOUAA4GBAD7TWK-C
CsqbsIDzTQdBaAQMMaODBTYULJADagSQMAUCCsqbsID3UDEB9U0AA4GBAD/1WK/C MZRSEF3U9hFBdU+5WcBbvGC/BqL1Oonsor+iPVLDovsVUCGva4Gbhc/Zs153BD
+NgAVzqirK9qqhBmKZv3F5io4d72wEHEb+zu3r8djqVlTdFtvf+A9zbOa6P+tsQh MbdJKUNng7s19Mf5bDLY6DFrcqUuXLoFr
WEB VP/N SET
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 avained that we do not verify the identify or beyond reading used fortificates. All
commercial purposes, you should also be avalet that we do not verify the identity of persons who request centricates. All certificate requests are approved automatically.
@1999 Entrust Technologies. All Rights Reserved.
SET is a trademark of the SET Secure Electronic Transaction, LLC.

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:

Key database information	
DB-Type: CMS key database file	
ile Name: C:\Program Files\Tivoli\PDWeb\www\certs\mypdsrv.kdb	
Key database content	
Signer Certificates	▼ Add
Thawte Personal Premium CA	Delete
Thawte Personal Freemail CA	1.
Thawte Personal Basic CA Thawte Premium Server CA	View/Edit
Thawte Premium Server CA Thawte Server CA	1
Verision Test CA Root Certificate	Extract
RSA Secure Server Certification Authority	
VeriSign Class 1 CA Individual Subscriber-Persona Not Validated	
VeriSign Class 2 CA Individual Subscriber-Persona Not Validated	
VeriSign Class 3 CA Individual Subscriber-Persona Not Validated	
Verisign Class 1 Public Primary Certification Authority	
Verisign Class 2 Public Primary Certification Authority	
Verisign Class 3 Public Primary Certification Authority	

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):

Data type	Base64-encoded ASCII data 🔻	
Certificate file name:	EntrustCACert.arm	Browse
Location:	C:\Program Files\Tivoli\PDWeb\www.certs\	

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:

DB-Type: CMS key database file ife Name: C:Program Files/Tivol/IPD/Web/www/certs/mypdsrv.kdb Key database content Signer Certificates Add Entrust Public CA Certificate Integrion Certification Authority Root IBM World Registry Certification Authority Thawte Personal Freemial CA Thawte Personal Freemial CA Thawte Personal Basic CA Thawte Personal Freemium Stever CA Yerisign Test CA Root Certificate RSA Secure Server Certification Authority		Key database information		
Signer Certificates Add Entrust Public CA Certificate Delete Integrion Certification Authority Root Wiew/Edit IBM World Registry Certification Authority Delete Thawte Personal Premium CA Thawte Personal Premium CA Thawte Personal Basic CA Extract. Thawte Personal Basic CA Thawte Personal Basic CA Thawte Personal Basic CA Extract. Thawte Personal Basic CA Extract.		rey database mioi madon		
Signer Certificates Add Entrust Public CA Certificate Delete Integrion Certification Authority Root Use Structure IBM World Registry Certification Authority View/Edit Thawte Personal Premium CA Thawte Personal Freemail CA Thawte Personal Basic CA Extract. Thawte Personal Basic CA Extract. Thawte Personal Basic CA Extract. Strawer CA Versign Test CA Root Certificate RSA Secure Server Certification Authority Extract.	B-Type: CMS key database file			
Signer Certificates Add Entrust Public CA Certificate Delete Integrion Certification Authority Root Use Structure IBM World Registry Certification Authority View/Edit Thawte Personal Premium CA Thawte Personal Freemail CA Thawte Personal Basic CA Extract. Thawte Personal Basic CA Extract. Thawte Personal Basic CA Extract. Strawer CA Versign Test CA Root Certificate RSA Secure Server Certification Authority Extract.	ile Name: C:\Program Files\Tivoli\PDWeb\	www.icertsimypdsrv.kdb		
Entrust Public CA Certificate Integrion Certification Authority Root IBM World Registry Certification Authority Thawte Personal Premium CA Thawte Personal Basic CA Thawte Personal Basic CA Thawte Personal Basic CA Thawte Server CA Versigin Test CA Root Certificate RSA Secure Server Certification Authority		Key database content		
Integrion Certification Authority Root IBM World Registry Certification Authority Thawte Personal Premium CA Thawte Personal Freemail CA Thawte Personal Basic CA Thawte Premium Server CA Thawte Premium Server CA Yerisign Test CA Root Certificate RSA Secure Server Certification Authority	Signer Certificates			Add
IBM World Registry Certification Authority Thawte Personal Premium CA Thawte Personal Freemail CA Thawte Personal Basic CA Thawte Personal Basic CA Thawte Personal Basic CA Thawte Server CA Versign Test CA Root Certificate RSA Secure Server Certification Authority	Entrust Public CA Certificate			Delete
Thawte Personal Premium CA Thawte Personal Freemail CA Thawte Personal Basic CA Thawte Personal Basic CA Thawte Personal Basic CA Thawte Server CA Thawte Server CA Verisign Test CA Root Certificate RSA Secure Server Certification Authority			1	
Thawte Personal Freemail CA Thawte Personal Basic CA Thawte Personal Basic CA Thawte Premium Server CA Thawte Server CA Versign Test CA Root Certificate RSA Secure Server Certification Authority				View/Edit
Thawte Personal Basic CA Thawte Premium Server CA Thawte Server CA Versign Test CA Root Certificate RSA Secure Server Certification Authority				
Thawte Premium Server CA Thawte Server CA Verisign Test CA Root Certificate RSA Secure Server Certification Authority				Extract
Thawte Server CA Verisign Test CA Root Certificate RSA Secure Server Certification Authority			1	
Verisign Test CA Root Certificate RSA Secure Server Certification Authority				
RSA Secure Server Certification Authority				
	가슴 선생님한 것 두 성장 것 것 위해 있지만 것이 같은 것 것 것 같은 것이 있다. 것 같은 바람이 있는			
	RSA Secure Server Certification Automite	a with and		
Versign Class 2 Public Primary Certification Authority	Verisign Class 1 Public Primary Certificatio			
	Verisign Class 1 Public Primary Certificatio Verisign Class 2 Public Primary Certificatio			

x. Select 'Personal Certificates' from the pull-down list:

BBM Key Management - [C:\Program Files\Tivoli\PDWeb\www\certs\mypdsrv.kdb]	
Key Database <u>File</u> <u>Create</u> <u>View</u> <u>H</u> elp	
Key database information DB-Type: CMS key database file File Name: C:\Program Files\Tivoli\PD\Web\www\certs\mypdsrv.kdb	
Key database content	
Personal Certificates	Receive
	Delete
	View/Edit
	Import
	Recreate Request
	New Self-Signed
	Extract Certificate
personal certificate has its associated private key in the database.	

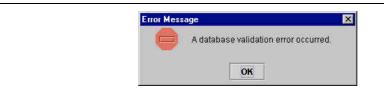
y. Click on Receive. The 'Receive Certificate from a File' window is displayed. Ensure that the Data type is set to Base64-encoded ASCII data and specify the file in which the certificate you just saved from the Entrust PKI is stored:

😹 Receive Certificate	from a File	×
Data type	Base64-encoded ASCII data 💌	
Certificate file name:	WebsealCert.arm	Browse
Location:	C:\Program Files\Tivoli\PDWeb\www\certs\	
	OK Cancel Help	

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 (*).)

	Key database information	
B-Type: CMS key database file		
ile Name: C:\Program Files\Tivoli\PDWet	Nwww\certs\mypdsrv.kdb	
	Key database content	
Personal Certificates		▼ Receive
* test-webseal-cert		Delete
		View/Edit
		Export/Import
		Recreate Request
	List of personal certificates. Default ind	New Self-Signed

Version 0.8 - 21 September, 2001



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 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 acceptclient-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-ldap = <passwd-ldap-library>
#passwd-uraf = <uraf-authn-library>
#token-cdas = <token-cdas-library>
#token-cdas = <cert-cdas-library>
#toter-cdas = <cert-cdas-library>
#http-request = <http-request-library>
#cdsso = <cdsso-authn-library>
#passwd-strength = <passwd-strength-library>
#cert-attrs = <cred-ext-attrs-library>
passwd-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.)

Key database information		
B-Type: CMS key database file		
le Name: C:\Program Files\Tivoli\PDWeb\www\certs\mypdsrv.kdb		
Key database content		
Signer Certificates	-	Add
Fivoli PKI Demo System CA Certificate		Delete
Fhawte Personal Premium CA		1
Fhawte Personal Freemail CA Fhawte Personal Basic CA		View/Edit
Inawte Personal Basic CA Fhawte Premium Server CA		-
Fhawte Server CA		Extract
/erision Test CA Root Certificate		
RSA Secure Server Certification Authority		
/eriSign Class 1 CA Individual Subscriber-Persona Not Validated		
/eriSign Class 2 CA Individual Subscriber-Persona Not Validated		
/eriSign Class 3 CA Individual Subscriber-Persona Not Validated		
/erisign Class 1 Public Primary Certification Authority		
/erisign Class 2 Public Primary Certification Authority		
/erisign Class 3 Public Primary Certification Authority		

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':

PKI Demo System CA Certificate
1024
X509 V3
01
Valid from August 13, 2001 to August 13, 2031
gest): :A0:DA:EC:C5:D7:68:B1:73:80:59
n: 1.2.840.113549.1.1.5(1.2.840.113549.1.1.5)

- 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

Version 0.8 - 21 September, 2001

corresponding PD user.

- k. Re-start WebSEAL to make these changes take effect.
- I. 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 an 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 reinstalling 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):

BK Key Management	_ 🗆 ×
Key Database File Create View Help	
Key database information	
DB.Type:	
File Name:	
Key database content	
Personal Certificates 🗸	Receive
	Delete
	View/Edit
	Import
	Recreate Request
	New Self-Signed
	Extract Certificate
	t
To start, please select the Key Database File menu to work with a key database	

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.)

Key database type	CMS key database file 🔹	
File Name:	Idapsrvkey.kdb	Browse
Location:	[C1]	
	OK Cancel Help	

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:

Password Prompt	×
Password	l: [*******
Confirm Password	: ·····
Set expiration time?	60 Days
🗹 Stash the j	password to a file?
Password Strength:	
OK Reset	Cancel Help

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

Informatio	n	×
Î	The password has been encrypted and saved in f C:\ldapsrvkey.sth.	ile:
	ОК	

e. Click on '**OK**'; information about the key database just created will be displayed at the top of the panel:

3M Key Management - [C:\ldapsivkey.kdb]	
Database <u>F</u> ile <u>Create</u> <u>View</u> <u>H</u> elp	
Key database information	
Type: CMS key database file	
a Name: C.Udapsrvkey kdb	
Key database content	
igner Certificates	▼ Add
nawle Personal Premium CA	Delete
nawte Personal Freemail CA nawte Personal Basic CA	View/Edit
nawte Premium Server CA nawte Server CA	
rawie server CA erisign Test CA Root Certificate	Extract
SA Secure Server Certification Authority	
eriSign Class 1 CA Individual Subscriber-Persona Not Validated	
eriSign Class 2 CA Individual Subscriber-Persona Not Validated	
eriSign Class 3 CA Individual Subscriber-Persona Not Validated	
erisign Class 1 Public Primary Certification Authority	
erisign Class 2 Public Primary Certification Authority	
erisign Class 3 Public Frimary Certification Authority	
ansign class 3 Fublic Finnary Certification Automity	
requested action has successfully completed!	

- 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)

llogoo provido tho	Following		
lease provide the	ronowing:		
Key Label		LDAP Server]
Version		X509 V3 🔻	
Key Size		1024 🔻	
Common Name		secure2.pisc.uk.ibm.com	
Organization		ibm	
Organization Unit	(optional)		
Locality	(optional)		
State/Province	(optional)		
Zipcode	(optional)		
Country		GB 💌	
Validity Period		365 Days	
Validity Period		365 Days	

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'

BM Key Management - [C:\ldapsrvkey.kdb]	
/ Database File Create View Help	
Key database information	
3-Type: CMS key database file	
le Name: CNidapsrvkey.kdb	
Key database content	
Personal Certificates 🔹	Receive
LDAP Server	Delete
	View/Edit
	Export/Import
	Recreate Request
	New Self-Signed
	Extract Certificate
e requested action has successfully completed!	

- 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 Base64encoded ASCII data and specify a filename and directory (we used

Extract Certificate to a	File	×
Data type	Base64-encoded ASCII data 🔻	
Certificate file name:	LDAPsrvcert.arm	Browse
Location:	[C:1]	
	OK Cancel Help	

k. Click on 'OK'.

- I. 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.

∰ Secure₩ay Directory Server \	#eb Admin: secure2 - Netscape		_ 8 ×
Eile Edit View Go Communicato	r ∐elp		
Back Forward Reload	🔥 🥕 🚵 🍦 😭 🔕 Home Search Netscape Print Security Shop	31 Glop	N
	http://secure2.pisc.uk.ibm.com/81/Idap/cgi-bin/Idacgi.exe?Action=Sta		👻 🌍 What's Related
📋 🚴 Instant Message 🛛 🖳 WebMa	il 🖳 Contact 🖳 People 🖳 Yellow Pages 🖳 Download 👔	🕇 Channels	
Directory Server	SSL settings		• ?-
Introduction	😔 secure2		
▶ ☐ Settings ▼ ☐ Security	K Ready		
▼⊡ SSL	Edit the SSL general settings, then click Update.		
Settings	5 ABA 5		
Certificate revocation	SSL status	C SSL Only	
 Kerberos Replication 		 SSL On 	
Database		C SSL Off	
Current state	Authentication method	 Server Authentication 	
Logs Logoff		C Server and Client Authentication	
E Logon	Secure port	63.6	
	Key database path and file name	c:\ldapsrvkey.kdb	
	Key label		
	A password is only required if there is no password st	ash file for the key database, or if you wish to override the password stash.	
	Key password		
	Confirm password		
	Update Reset		
	Related tasks		
	Encryption - Select the type of SSL encryption. <u>Certificate revocation</u> - Define the LDAP serve	r used for certificate revocation.	
	-		
Applet o	om ibm webexec herald HeraldÅpplet running		

- 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
```

Version 0.8 - 21 September, 2001

```
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
supportedsaslmechanisms=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):

	Key database information	
B-Type:		
le Name:		
	Key database content	
Personal Certificates		Receive
		Delete
		View/Edit
		Import
		Recreate Request
		New Self-Signed

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.)

New	· · · · ·	×
Key database type	CMS key database file 💌	
File Name:	LDAPclikey.kdb	Browse
Location:		
	OK Cancel Help	

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:

assword Prompt	
Password:	*****
Confirm Password:	*****
Set expiration time?	60 Days
🗹 Stash the pa	ssword to a file?
assword Strength:	

- 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:

Key database information B-Type: CMS key database file ile Name: C:LDAPclikey.kdb Key database content Signer Certificates Add Delete Thawte Personal Preemail CA Thawte Personal Brie CA View/Edit	IBM Key Management - [C:\LDAPclikey.kdb]	
Key database information B-Type: CMS key database file ile Name: C1LDAPclikey.kdb Key database content Signer Certificates Add Delete View/Edit Thawte Personal Premium CA Thawte Personal Premium CA Thawte Personal Premium CA Thawte Personal Premium CA Thawte Personal Premium Server CA Thawte Personal Premium Server CA Thawte Server CA Thawte Server CA View/Edit Extract View/Edit Thawte Server CA Thawte Server CA Thawte Server CA View/Edit Extract View/Edit Thawte Server CA Thawte Server CA Thawte Server CA View/Edit Extract View/Edit View/Edi	ey Database File Create View Help	
B-Type: CMS key database file ile Name: C:LDAPClikey kdb Key database content Signer Certificates Add Delete Delete Delete ViewEdit Thawte Personal Premium CA Thawte Personal Basic CA Thawte Personal Basic CA Thawte Personal Basic CA Thawte Server CA Thawte Server CA Thawte Server CA Certificate RSA Secure Server Certification Authority VeriSign Class 1 CA Individual Subscriber-Persona Not Validated VeriSign Class 2 CA Individual Subscriber-Persona Not Validated VeriSign Class 2 Public Primary Certification Authority Verisign Class 2 Public Primary Certification Authority Verisign Class 2 Public Primary Certification Authority		
Ile Name: C1LDAPclikey.kdb Key database content Signer Certificates Add Delete Add Delete View/Edit Thawte Personal Premium CA Thawte Personal Preemail CA Thawte Personal Basic CA Thawte Server CA View/Edit Extract Extract Extract View/Edit Extract	Key database information	
Ile Name: C1LDAPclikey.kdb Key database content Signer Certificates Add Delete Add Delete View/Edit Thawte Personal Premium CA Thawte Personal Preemail CA Thawte Personal Basic CA Thawte Server CA View/Edit Extract Extract Extract View/Edit Extract	DB-Type: CMS key database file	
Key database content Signer Certificates Add Thawte Personal Premium CA Delete Thawte Personal Freemail CA View/Edit Thawte Personal Basic CA View/Edit Thawte Server CA View/Edit Yensign Test CA Root Certificate Extract RSA Secure Server Certification Authority Verisign Class 1 CA Individual Subscriber-Persona Not Validated Verisign Class 2 CA Individual Subscriber-Persona Not Validated Verisign Class 3 CA Individual Subscriber-Persona Not Validated Verisign Class 2 Ca Individual Subscriber-Persona Not Validated Verisign Class 2 Public Primary Certification Authority Verisign Class 2 Public Primary Certification Authority Verisign Class 2 Public Primary Certification Authority		
Signer Certificates Add Thawte Personal Freemail CA Delete Thawte Personal Basic CA View/Edit Thawte Personal Basic CA Thawte Personal State CA Thawte Personal Basic CA Thawte Server CA Yensign Test CA Root Certificate Extract RSA Secure Server Certification Authority Verisign Class 1 CA Individual Subscriber-Persona Not Validated Verisign Class 1 CA Individual Subscriber-Persona Not Validated Verisign Class 3 CA Individual Subscriber-Persona Not Validated Verisign Class 1 Public Primary Certification Authority Verisign Class 3 CA Individual Subscriber-Persona Not Validated Verisign Class 2 Public Primary Certification Authority Verisign Class 3 CA Individual Subscriber-Persona Not Validated	ne wane. C.LDAF Cirkey.Kdb	
Thavte Personal Premium CA Delete Thavte Personal Basic CA View/Edit Thavte Personal Basic CA View/Edit Thavte Personal Basic CA View/Edit Thavte Server CA Extract Yerisign Test CA Root Certificate RSA Secure Server Certification Authority Verisign Class 1 CA Individual Subscriber-Persona Not Validated Verisign Class 2 CA Individual Subscriber-Persona Not Validated Verisign Class 1 Public Primary Certification Authority Verisign Class 2 CA Individual Subscriber-Persona Not Validated Verisign Class 2 Public Primary Certification Authority Verisign Class 3 CA Individual Subscriber-Persona Not Validated	Key database content	
Thawte Personal Freemail CA Thawte Personal Basic CA Thawte Personal Basic CA Thawte Personal Basic CA Thawte Personal Basic CA View/Edit Thawte Server CA Versigin Test CA Root Certificate RSA Secure Server Certification Authority VeriSign Class 1 CA Individual Subscriber-Persona Not Validated VeriSign Class 3 CA Individual Subscriber-Persona Not Validated Verisign Class 3 CA Individual Subscriber-Persona Not Validated Verisign Class 3 Public Primary Certification Authority Verisign Class 2 Public Primary Certification Authority	Signer Certificates 🗸 🗸	Add
Thawle Personal Freemail CA Thawle Personal Basic CA Thawle Server CA Thawle Server CA Thawle Server CA Weinsign Test CA Root Certificate RSA Secure Server Certification Authority VeriSign Class 1 CA Individual Subscriber-Persona Not Validated VeriSign Class 3 CA Individual Subscriber-Persona Not Validated Verisign Class 3 CA Individual Subscriber-Persona Not Validated Verisign Class 3 CA Individual Subscriber-Persona Not Validated Verisign Class 2 Public Primary Certification Authority Verisign Class 2 Public Primary Certification Authority	Thawte Personal Premium CA	Delete
Thawte Premium Server CA Thawte Server CA Verisign Test CA Root Certificate RSA Secure Server Certification Authority VeriSign Class 1 CA Individual Subscriber-Persona Not Validated VeriSign Class 2 CA Individual Subscriber-Persona Not Validated VeriSign Class 1 Chulkindual Subscriber-Persona Not Validated VeriSign Class 1 Public Primary Certification Authority Verisign Class 2 Public Primary Certification Authority Verisign Class 2 Public Primary Certification Authority	Thawte Personal Freemail CA	
Thawte Server CA Verisign Test CA Root Certificate RSA Secure Server Certification Authority VeriSign Class 1 CA Individual Subscriber-Persona Not Validated VeriSign Class 3 CA Individual Subscriber-Persona Not Validated Verisign Class 3 CA Individual Subscriber-Persona Not Validated Verisign Class 1 Public Primary Certification Authority Verisign Class 2 Public Primary Certification Authority	Thawte Personal Basic CA	View/Edit
Verisign Class 1 CA Individual Subscriber-Persona Not Validated VeriSign Class 2 CA Individual Subscriber-Persona Not Validated VeriSign Class 3 CA Individual Subscriber-Persona Not Validated VeriSign Class 3 CA Individual Subscriber-Persona Not Validated VeriSign Class 1 Public Primary Certification Authority Verisign Class 2 Public Primary Certification Authority	Thawte Premium Server CA	
RSA Secure Server Certification Authority VeriSign Class 1 CA Individual Subscriber-Persona Not Validated VeriSign Class 2 CA Individual Subscriber-Persona Not Validated VeriSign Class 3 CA Individual Subscriber-Persona Not Validated Verisign Class 1 Public Primary Certification Authority Verisign Class 2 Public Primary Certification Authority		Extract
VeriSign Class 1 CA Individual Subscriber-Persona Not Validated VeriSign Class 2 CA Individual Subscriber-Persona Not Validated VeriSign Class 3 CA Individual Subscriber-Persona Not Validated Verisign Class 1 Public Primary Certification Authority Verisign Class 2 Public Primary Certification Authority		·
VeriSign Class 2 CA Individual Subscriber-Persona Not Validated VeriSign Class 3 CA Individual Subscriber-Persona Not Validated Verisign Class 1 Public Primary Certification Authority Verisign Class 2 Public Primary Certification Authority		
VeriSign Class 3 CA Individual Subscriber-Persona Not Validated Verisign Class 1 Public Primary Certification Authority Verisign Class 2 Public Primary Certification Authority		
Verisign Class 1 Public Primary Certification Authority Verisign Class 2 Public Primary Certification Authority		
Verisign Class 2 Public Primary Certification Authority		
Verision Class 3 Public Primary Certification Authority		
	vensign crass 3 Public Primary Certification Authority	
	he requested action has successfully completed!	

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)

Data type	Base64-encoded ASCII data 💌	
Certificate file name:	LDAPsrvcert.arm	Browse
Location:	C3	

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:

IBM Key Management - [C:\LDAPclikey.kdb]	
y Database <u>F</u> ile <u>C</u> reate <u>V</u> iew <u>H</u> elp	
Key database information	
B-Type: CMS key database file	
le Name: C:\LDAPclikey.kdb	
Key database content	
Signer Certificates	▼ Add
DAP Server	Delete
hawte Personal Premium CA	Duitte
hawte Personal Freemail CA	View/Edit
'hawte Personal Basic CA	
hawte Premium Server CA	Extract
hawte Server CA	11
'erisign Test CA Root Certificate	
RSA Secure Server Certification Authority	
eriSign Class 1 CA Individual Subscriber-Persona Not Validated	
'eriSign Class 2 CA Individual Subscriber-Persona Not Validated	
eriSign Class 3 CA Individual Subscriber-Persona Not Validated	
erisign Class 1 Public Primary Certification Authority erisign Class 2 Public Primary Certification Authority	
ensign Class 2 Public Primary Certification Authority erisign Class 3 Public Primary Certification Authority	
rensign Grass 5 Flubic Frittany Certification Authonity	
e requested action has successfully completed!	

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:

LDAP Server		
Key Size:	1024	
Certificate Property:		
Version	X509 V3	
Serial Number:	3B:AB:60:87	
Issued to:		
secure2.pisc.uk.i	bm.com	
ibm		
GB		
Issued by:		
secure2.pisc.uk.i	hm com	
ibm	bin.com	
GB		
Validity:	Valid from September 20, 2001 to September 21, 2002	
Fingerprint (MD5 D		
ED:F7:B4:1E:E0:9	5:42:6E:35:E9:21:17:23:F2:C4:FD	
Signature Algorith	m: 1.2.840.113549.1.1.4(1.2.840.113549.1.1.4)	
Set the certificate a	as a trusted root	
	OK	

- 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
supportedsaslmechanisms=CRAM-MD5
supported1dapversion=2
supported1dapversion=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
```

Version 0.8 - 21 September, 2001

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 sceen below.

🚳 SSL Communication with the LDAP Server 🛛 🗙
Enable SSL Communication with the LDAP Server?
SSL Port Number
636
SSL client key file
c:\LDAPclikey.kdb
SSL client certificate label (if required)
SSL client key file password

< Back Next > 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. Tivoli Policy Director V3.8 – Installation Guidelines/Cookbook

Policy Director Configuration Review
Management Server Host: secure2.pisc.uk.ibm.com Listening Port: 7135 Name of the file containing the Management Server's signed certificate: C:\pdcacert.b64 User Registry Selection: Idap LDAP Host Name: secure2.pisc.uk.ibm.com LDAP Port Number: 389 LDAP DN for GSO Database: ou=emea,o=ibm,c=gb Enable SSL Communication with the LDAP Server?: Yes SSL Port Number: 636 SSL client key file: c:\LDAPclikey.kdb SSL client key file password:
< Back Finish Cancel

- 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.)

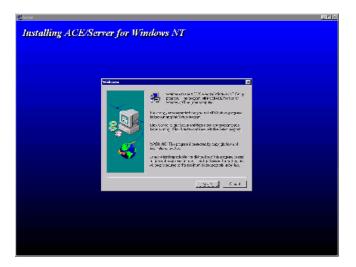
This assumes that assume you are using the ACE/Server package from Security Dynamics which was supplied with the SecureWay Boundary Server (SBS), so you have:

- 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:

Tivoli Policy Director V3.8 - Installation Guidelines/Cookbook



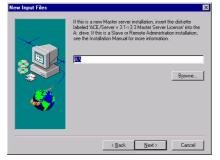
f. Click on 'Next'. A further Welcome screen will be displayed:



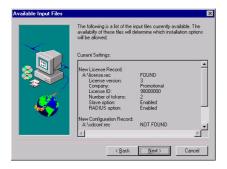
g. Click on 'Next'. The License Agreement screen will be displayed:



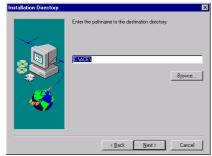
h. Click on 'Yes'. A 'New Input Files' screen will be displayed. Ensure that the diskette labelled "ACE/Server V3.3.1 2 User Promo License" is inserted in the diskette drive specified.



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':



I. 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:

d Client		
Name:		
Network address:		
Site:		Select
Client type: UNIX Client Communication Single-Transact	Server	
Encryption Type: 🔿 SDI 👁 DES		
🗖 Sent Node Secr	ret	
🗂 Open to All Loca	ally Known Users	
🗖 Search Other R	calms for Unknown Users	
Group Activations	User Activations	
Secondary Nodes	Delete Client	
Edit Client Extension Data	Assign/Change Encryption Key	

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:

Name: harperv.welwyn.	.uk.ibm.com	
Network address: <mark>3.180.244.205</mark>		
Site:		Selec
Client type: UNIX Client Communication Single-Transact	Server view view view view view view view view	
Encryption Type: C SDI @ DES		
🗖 SentNode Seco	et	
🗂 Open to All Loca	ally Known Users	
🗖 Search Other Re	alms for Unknown Users	
Group Activations	User Activations	1
Secondary Nodes	Delete Client	1
Edit Client Extension Data	Assign/Change Encryption Key	1

- 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:

	PD Users	
Site:		Select
	Members	Client Activations
-	Delete Group	Edit Group Extension Data
	Edit Access Times	· · · · · · · · · · · · · · · · · · ·

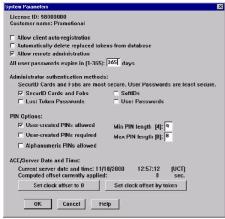
s. Click on 'Client Activations...'. A confirmation message will be displayed:



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':

Group: PD Users Clients	Clients Activated On
arperv.welwyn.uk.ibm.com	harperv.welwyn.uk.ibm.com
Add Client	× Remove Client

- 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:



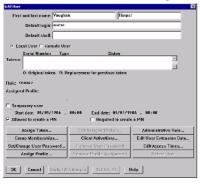
- y. Click on 'Yes'. You will be returned to the ACE/Server Administration screen.
- z. From the manu bar, click on Token -> Import Tokens.... An 'Import Token Filename' panel will be displayed. Insert the diskette containing the SecurID seed values (whose label includes a batch name, a specification 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':

emberships User: Vaughan Harper	×
Available Groups PD Users	Group Memberships PD Users
۲ Join Group	Remove Group
* Filter	Edit Membership Data Edit Group
Exit Help	

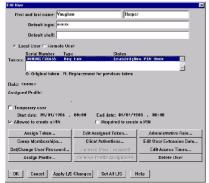
- ff. Click on 'Exit'. The 'Edit User' panel will be displayed again.
- gg. Click on 'Assign Token...'. The 'Select Token' panel will be displayed:

Token			×
Serial Num	ber:		
Tokens	Unassi	gned	
Retrieve se	rial numbe	r from Smart Ca	rd
ОК	Cancel	Help	
	Serial Num Tokens Retrieve se	Serial Number: Tokens Unassi Retrieve serial numbe	Serial Number: Tokens Unassigned Retrieve serial number from Smart Ca

hh. Click on 'Unassigned'. A SecurID Serial Number will be displayed in the 'Select Token' panel:

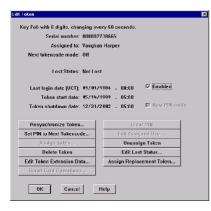


ii. Click on '**OK**'. The 'Edit User' panel will be displayed again, this time with a token specified. Highlight the token:



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:



II. Click on 'Resynchronize Token...'. The 'Resynchronize Token' panel will be displayed. Key the six digit number displayed by the SecurID token:

Resynchronize Token	Þ
Serial Number: 000002738665	
Enter the code displaying on the token, then select OK.	
432111	
OK Cancel Help	

mm. Click on '**OK**. Wait for the display to change, then key the new six digit number displayed by the SecurID token:

Resynchronize Token	×
Serial Number: 000002738665	
Enter the code displaying on the token, then select OK.	
432111	
Wait for the code to change, then enter the new code and select OK	
272982	
OK Cancel Help	

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:

Tokencode
ber: 000002738665
ode displaying on the token.
905520
be the first 4 digits of the next tokencode.
Cancel Help

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 httpsforms-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

Version 0.8 – 21 September, 2001

c) In the [wand] stanza ensure that the <code>verify-clients</code> 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 to 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 <u>Re-access the</u> <u>page using HTTPS</u>. 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:

Tivoli Policy Director V3.8 – Installation Guidelines/Cookbook

Policy Director Login - He	tscape Sets Habi	- 5 ×
	l anno Sacat Magello Si Sinany Sin.	N
💓 Bockmatts 🥀 Less	the Proced/Augury the sign of the bene487	💌 💓 V-Patri Robota
Policy Director	Login	
Sandard Authenticatio		
 Usummu 		
· Fineword		
Coken Authentication	756278	
 FASSUCHE 	Pontost .	
uig n		
>	at set C. av	135 Mar 42 19 V

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:

		Activity report Da	te: 11/27/2000 17:35:48	
		Pa	ge: 2 of 2	
Date	Tine	Current User/Client (Group) Description	Affected User (Site) Server	
1/27/2000	17:22:370	SYSTEN	>/	
1/27/2000	17:22:37L	Admin Server Started	harperv.welwyn.uk.ibm.con	
1/27/2000	17:34:270	usera/harperv.welwyn.uk.ibm.con	000002738665/Vaughan Harp	
1/27/2000	17:34:27L	Node Secret Sent to Diient	harperv.wclwyn.uk.ibm.con	
1/27/2000	17:34:270	usera/harperu.welwyn.uk.ibm.com	000002738665/Vaughan Harp	
1/27/2008	17:34:27L	PASSCODE Accepted	harpers.welwyn.uk.ibm.con	
1/27/2888	17:35:070	Administrator		
1/2//2000	17:35:0/L	Sdadnin Started	harperv.weiwyn.uk.ibm.con	
1/27/2000	17:35:400	Administrator		
1/27/2000	17:35:48L	Printed Activity Report	harperv.welwyn.uk.ibm.com	
Previous	Nes	t Go to Page 2	Exit	

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 <code>pkiUser</code> and <code>PKiCA</code>

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)

Tivoli Policy Director V3.8 – Installation Guidelines/Cookbook

- k. Next run CfgStart -i on the LDAP server.
- I. Once this is complete go back to the TA server and run <code>CfgStart -i</code> again, this will complete the TA configuration.
- m. Once complete TA can be tested in the normal way. One you have issed 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 dirctory

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, pdacld 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 persession cookies (not stored)'

Running IP traces

<u>On AIX</u>

- 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

<u>On Solaris</u>

 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).

<u>On NT</u>

- 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.

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
- secugra -roreground -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/** (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

For Business Partners, there is information on Policy Director on TIPS at 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.

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:

SG24-4986Understanding LDAPSG24-5110LDAP 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