IBM Tivoli Access Manager for e-business Version 3.9 Cookbook

Windows, AIX and Solaris

Vaughan Harper EMEA Technical Evangelist – Access 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 1.1 – 30 September, 2002



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 Access Manager. The information in this publication is not intended as the specification of any programming interfaces that are provided by Tivoli Access Manager, 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, Sean McDonald from the US Tivoli Security Pre-Sales team, 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, Gary Linker from the Level 2 team in Austin, Chris Hockings from IBM Australia and Shali Goradia.

In addition, special thanks to Avery Salmon and Jon Harry from the PIC at IBM Hursley and their team of Oleg Bascurov, Gianluca Gargaro and Jeff Miller for their work on the 3.9 Beta Workshop Hands-On Lab Guide.

Table of Contents

Т	able of Contents	iii
Part I -	Introduction	1
1.	Introduction	1
Part II	- Windows Environment	2
2.	Windows System preparation (operating system, etc)	2
3.	Easy Install	
3.1	Easy Install of the IBM SecureWay Directory	
3.2	Easy Install of Access Manager Management Server	9
3.3	Easy Install of Access Manager WebSEAL	13
4. 4.1	Easy Install process to set up Access Manager components on a remote machine Easy Install of Access Manager WebSEAL	15
5.	Easy Install - Web Portal Manager	20
5.1	Easy Install of Web Portal Manager (PDWPM)	20
6.	Native installation process	27
6.1	GSKit installation (Windows)	27
6.2	LDAP Server installation (Windows)	30
6.3	LDAP Server configuration (Windows)	
6.4	Directory Management Tool steps	48
6.5	Install IBM SecureWay Directory Version 3.2.2 e-fix 2	
6.6	Update the DB2 License key.	
6.7	LDAP Client installation (Windows)	
6.8 6.0	Access Manager Servers Installation (Windows)	
6.10	Install MebSEAL (Windows)	
6.11	Access Manager Configuration (Windows)	
6.12	2 Access Manager RTE + WebSEAL Configuration (Windows)	
6.13	3 Web Portal Manager Installation & Configuration (Windows)	77
6.14	4 Changing Web Portal Manager port numbers (Windows)	
6.15	5 Verify Web Portal Manager operation	94
Part II	I - AIX Environment	98
7.	AIX System Preparation and general AIX Notes	98
8.	LDAP Server installation/configuration (AIX)	100
8.1	Operating system pre-requisites	
8.2	Install the IBM HTTP Server	100
8.3	Install GSKit	102
8.4	Install IBM SecureWay Directory	103
8.5	Configure LDAP	
8.6	Add Access Manager Suffixes	
8./	Directory Management Tool steps	
9.	Access Manager Server installation (AIX)	112
10.	WebSEAL Installation (AIX)	113
11.	Access Manager Configuration (AIX)	115
12.	Web Portal Manager Installation and Configuration (AIX)	121

12.1	Install the Access Manager pre-requisite software	
12.2	Install WebSphere Application Server	
12.3	Install the WebSphere Application Server PTFs	
12.4	Install Web Portal Manager	126
12.5	Configure Web Portal Manager	127
12.6	Set the HTTP Server port numbers	129
12.7	Verify Web Portal Manager operation	
13.	Useful information for Access Manager in the AIX environment	138
LI	DAP commands	
A	ccess Manager commands	
A	ccess Manager Processes	
A	ccess Manager log lifes	
Part IV	- Solaris Environment	
14.	Solaris System Preparation and general Solaris Notes	139
15.	Easy Installation Process for Solaris	139
15.1	IBM SecureWay Directory and Prerequisite Installation and Configuration	140
15.2	Access Manager RTE and Policy Server Installation and Configuration	143
15.3	WebSEAL Install and Configuration	145
15.4	Web Portal Manager Install & Configuration	146
16.	Access Manager Component Configuration & Unconfiguration (Solaris)	148
17.	Solaris – Native installation	149
17.1	LDAP Server installation/configuration (Solaris)	
17.2	Operating system pre-requisites	149
17.3	Install DB2	149
17.4	Install DB2 Fix Pack 5	150
17.5	Update the DB2 License key	
17.6	Install GSK it	
17.7	Install the LDAP Client.	
17.0	Install the LDAD Server	
17.9	Download and Install the IDAP a fix 2	
17.1	Check/set the Solaris kernel configuration parameters	
17.1	2 Configure LDAP	156
17.1	3 Add Access Manager Suffixes	
17.1	4 Directory Management Tool steps	
18.	Access Manager Server installation (Solaris) (Native)	165
19.	WebSEAL Installation (Solaris) (Native)	166
20.	Access Manager Configuration (Solaris) (Native)	167
21.	Useful commands for Access Manager in the Solaris environment	168
LI	DAP	
D	irectory Management Tool steps	
PI)	
Sc	סומרוא	169
Part V -	Generic Product Configuration	
22.	Initial Access Manager Validation	170
23.	Further Access Manager Configuration	175
D	irectory Management Tool	

24.	Query contents – additional notes	
	Ouery contents with Lotus Domino Go Webserver	
	\tilde{Q} uery_contents with Netscape Enterprise Server under AIX	
25	Setting up a WebSFAL server certificate	183
23.	Annroach (a) - Generating a self-signed certificate	183
	Approach (b) - Certificate Signing Request sent to Tivoli PKI	105
	Approach (c) - Certificate Signing Request sent to Entrust CA	
	Additional notes	208
20		200
26.	Setting up client certificate authentication	
27.	Setting up an SSL connection to the LDAP Directory	211
	LDAP Server - create the key database file	
	LDAP Client (Access Manager Server components) - create the key database file	
	LDAP Client (Access Manager Server) - install LDAP Server certificate	
	Configuring PDRTE for SSL communication to LDAP	
28.	Installation of SecurID token support	223
_0.	Problem Determination	233
	Uninstalling	233
	Problem	
30		225
29.	Useful LDAP commands	
30.	Troubleshooting	
	Access Manager won't start	
	Problems once Access Manager has started	
	Page Not Found problems	237
	Running IP traces	
	Other problem determination ideas - AIX	239
Part	VI - 3.9 Beta Workshop Hands-on Labs Guide	
31	Introduction	240
31.	1.1 Style conventions	240 240
3	1.2 Addition information resources	
3	1.3 Machine hostnames and DNS names	
3	14 Lab Environment	241
3	1.5 Default Configurations	242
-	File Locations.	
	IBM Directory Server Configuration Options	
	Active Directory Server Configuration Options	
	Domino Server Configuration Options	
3	1.6 User IDs, Passwords and Ports	
3	1.7 Banker 2001 Users and Roles	
3	1.8 Useful utilities	
32	Installing Policy Director	244
3	2.1 Setup	
33	Configure Policy Director with Your User Registry	246
3	3.1 Configuring PDRTE with IBM Directory Server	246
5	Considerations	246
	Configuration of PDRTE using IBM Directory Server 3.2.2	246
3	3.2 Configuring PDRTE with Active Directory	248
5	Considerations	
	Configuration	
	Configuration	
3	3.3 Configuring PDRTE with Domino	

Procedure	
33.4 Finishing Policy Director Configuration on Your Directory Server	
34. Installing and Configuring Web Portal Manager	255
34.1 Initial Procedure	
34.2 Enable SSL	
35. Verify the Configuration with PDADMIN and WebSEAL	258
35.1 Starting PDAdmin	
Unauthenticated access	
Login as 'sec_master'	
Using IBM Secure Way Directory Server	238
Using Active Directory	
Using Domino	
35.3 Connect to WebSEAL	
36. Configure WebSphere with Your User Registry	
36.1 Objectives	
36.2 Adding Groups and Users to IBM Directory Server	
36.3 Adding Groups and Users to Active Directory	
Considerations.	
Using the Active Directory GUI	
36.4 Adding Groups and Users to Domino Server	
Creating Domino Directory Osers	
Some useful LDAP commands	
36.5 Configuring WebSphere Security with Your User Registry	
Considerations	
Setting up the Registry in WebSphere	
36.6 Mapping Users and Groups to Roles with the WebSphere Admin Console	
Considerations	
36.7 Testing Banker 2001 Security	
Starting the Application	
Other Application Functionality	
Testing Security	
Importing Banker 2001 Users and Groups into Policy Director	
37. Multiple WebSEAL Servers on the Same Machine	
37.1 Configuring a Second WebSEAL Server to Listen on Different Ports Using the Same IP Add	lress as the
Initial WebSEAL Server	
37.2 Configuring a Third WebSEAL Server to Listen on Ports 80 and 443 Using a Different IP Ac	dress than the
Initial WebSEAL Server	
Create a new virtual IP-address.	
37.3 Changing the Configuration of the Primary WebSEAL Instance	278
37.4 Final Question	
20 HTTD 1 1 Summark	270
38. HITP 1.1 Support	
Using TCP Tunnel to monitor WebSEAL	
	202
39. Forced Re-authentication, Constant Session ID and Session Termination	
39.1 Enable Forms-Based Login	
39.3 Constant Session ID	
Configure WebSEAL to Transmit the Session ID to the Junctioned Server	283
Parsing the HTTP Request Header using Banker 2001	

57.4	Configure a Constant Session ID on WebSEAL.	
Re	educe Session-Inactivity Timeout	
Τι	Irn on REAUTH-FOR-INACTIVE	
39.5	Terminating a User Session	
Те	erminate a Specific User Session	
Te	erminate All Sessions of a Particular User on a WebSEAL Server	
40.	Switch User	
40.1	Objectives	
40.2	Scenario	
40.3	Assigning Users to the Groups	
40.4	Enabling the Switch User Functionality on WebSEAL	
40.5	Using the Switch User Function	
41.	Caching data on POST method	
42.	TLS support	
43	Integration of Policy Director and WebSnhere Application Server	294
43 1	Objectives	
43.1 In	Objectives	294 205
III. Do	indi Setup	
re Se	tion the Migration Teel	
Se	sup the Migration 1001	
M	Igrate the wAS Admin Server Application	
le	ell WAS to use PD for authorization	
43.2	Testing PD and WAS Integration	
43.3	Migrate the Banker 2001 Application Security to Policy Directory	
Oł	ojectives	
Pr	ocedure	
Те	esting Banker 2001 Security with Policy Director	
<u> </u>	Form Based Single Sign On	202
	Form Dased Single Sign-On	
44.1	Port 1	
44.1 44.2	Part 1 Part 2	
44.1 44.2 45.	Part 1 Part 2 Installation and Configuration of the Policy Director Web Plug-In for Mic	
44.1 44.2 45. Inform	Part 1 Part 2 Installation and Configuration of the Policy Director Web Plug-In for Mic nation Server (IIS)	
44.1 44.2 45. Inform 45.1	Part 1 Part 2 Installation and Configuration of the Policy Director Web Plug-In for Mic nation Server (IIS)	
44.1 44.2 45. Inform 45.1 45.2	Part 1 Part 2 Installation and Configuration of the Policy Director Web Plug-In for Mic nation Server (IIS) Objectives Prerequisites	302 303 rosoft Internet 305 305 305 305
44.1 44.2 45. Inform 45.1 45.2 45.3	Part 1 Part 2 Installation and Configuration of the Policy Director Web Plug-In for Mic nation Server (IIS) Objectives Prerequisites Installation of Policy Director Web Plug In for IIS	302 303 303 rosoft Internet 305 305 305 305 305
44.1 44.2 45. Inform 45.1 45.2 45.3 45.4	Part 1 Part 2 Installation and Configuration of the Policy Director Web Plug-In for Mic nation Server (IIS) Objectives Prerequisites Installation of Policy Director Web Plug In for IIS Configuring new Virtual Hosts on IIS	302 303 303 rosoft Internet 305 305 305 306 307
44.1 44.2 45. Inform 45.1 45.2 45.3 45.4 Co	Part 1 Part 2 Installation and Configuration of the Policy Director Web Plug-In for Mic nation Server (IIS) Objectives Prerequisites Installation of Policy Director Web Plug In for IIS Configuring new Virtual Hosts on IIS	302 303 303 rosoft Internet 305 305 305 306 307 307 307
44.1 44.2 45. Inform 45.1 45.2 45.3 45.4 CC Pr	Part 1 Part 2 Installation and Configuration of the Policy Director Web Plug-In for Mic. nation Server (IIS) Objectives Prerequisites Installation of Policy Director Web Plug In for IIS Configuring new Virtual Hosts on IIS Donsiderations.	302 303 303 rosoft Internet 305 305 305 306 307 307 307 307
44.1 44.2 45. Inform 45.1 45.2 45.3 45.4 Co Pr 45.5	Part 1 Part 2 Installation and Configuration of the Policy Director Web Plug-In for Mic nation Server (IIS) Objectives Prerequisites Installation of Policy Director Web Plug In for IIS Configuring new Virtual Hosts on IIS Donsiderations. ocedure Configuring the Policy Director Web Plug-In for IIS	302 303 303 rosoft Internet 305 305 305 306 307 307 307 307 307 308
44.1 44.2 45. Inform 45.1 45.2 45.3 45.4 CC Pr 45.5 45.6	Part 1 Part 2 Installation and Configuration of the Policy Director Web Plug-In for Mic nation Server (IIS) Objectives Prerequisites Installation of Policy Director Web Plug In for IIS Configuring new Virtual Hosts on IIS Disiderations ocedure Configuring the Policy Director Web Plug-In for IIS Using Policy Director Web Plug-In for IIS	302 303 303 rosoft Internet 305 305 305 305 306 307 307 307 307 307 307 307
44.1 44.2 45. Inform 45.1 45.2 45.3 45.4 CC Pr 45.5 45.6 Pr	Part 1 Part 2 Installation and Configuration of the Policy Director Web Plug-In for Mic nation Server (IIS) Objectives Prerequisites Installation of Policy Director Web Plug In for IIS Configuring new Virtual Hosts on IIS onsiderations ocedure Configuring the Policy Director Web Plug-In for IIS Using Policy Director WebPI for IIS Ocedure	302 303 303 rosoft Internet 305 305 305 306 307 307 307 307 307 307 307 307 307 307
44.1 44.2 45. Inform 45.1 45.2 45.3 45.4 CC Pr 45.5 45.6 Pr 45.7	Part 1 Part 2 Installation and Configuration of the Policy Director Web Plug-In for Mic nation Server (IIS) Objectives Prerequisites Installation of Policy Director Web Plug In for IIS Configuring new Virtual Hosts on IIS onsiderations ocedure Configuring the Policy Director Web Plug-In for IIS Using Policy Director WebPI for IIS Ocedure	302 303 303 rosoft Internet 305 305 305 306 307 307 307 307 307 307 307 307 307 307
44.1 44.2 45. Inform 45.1 45.2 45.3 45.4 Co Pr 45.5 45.6 Pr 45.7 Co	Part 1 Part 2 Installation and Configuration of the Policy Director Web Plug-In for Mic nation Server (IIS) Objectives Prerequisites Installation of Policy Director Web Plug In for IIS Configuring new Virtual Hosts on IIS onsiderations ocedure Configuring the Policy Director Web Plug-In for IIS Using Policy Director WebPI for IIS Ocedure Unconfiguring Policy Director WebPI for IIS	302 303 303 rosoft Internet 305 305 305 306 307 307 307 307 307 307 307 307 307 307
44.1 44.2 45. Inform 45.1 45.2 45.3 45.4 Co Pr 45.5 45.6 Pr 45.7 Co Pr	Part 1 Part 2 Installation and Configuration of the Policy Director Web Plug-In for Mic nation Server (IIS) Objectives Prerequisites Installation of Policy Director Web Plug In for IIS Configuring new Virtual Hosts on IIS onsiderations ocedure Configuring the Policy Director Web Plug-In for IIS Using Policy Director WebPI for IIS ocedure Unconfiguring Policy Director WebPI for IIS onsiderations	302 302 303 rosoft Internet 305 305 305 306 307 307 307 307 307 307 308 311 311 312 313
44.1 44.2 45. Inform 45.1 45.2 45.3 45.4 CC Pr 45.5 45.6 Pr 45.7 CC Pr 45.8	Port 1	302 303 303 rosoft Internet 305 305 305 306 307 307 307 307 307 307 311 311 312 313 313
44.1 44.2 45. Inform 45.1 45.2 45.3 45.4 Co Pr 45.5 45.6 Pr 45.7 Co Pr 45.8 46.	Part 1	302 303 303 rosoft Internet 305 305 305 306 307 307 307 307 307 307 308 311 311 312 313 313 313 313
44.1 44.2 45. Inform 45.1 45.2 45.3 45.4 Co Pr 45.5 45.6 Pr 45.7 Co Pr 45.8 46. 46.	Part 1	302 303 303 rosoft Internet 305 305 305 306 307 307 307 307 307 308 311 311 312 313 313 313 313 313
44.1 44.2 45. Inform 45.1 45.2 45.3 45.4 CC Pr 45.5 45.6 Pr 45.7 CC Pr 45.8 46. 46.1	Part 1	302 302 303 rosoft Internet 305 305 305 306 307 307 307 307 307 308 311 311 312 313 313 313 313 313
44.1 44.2 45. Inform 45.1 45.2 45.3 45.4 Co Pr 45.5 45.6 Pr 45.7 Co Pr 45.8 46. 46.1	Part 1	302 303 303 rosoft Internet 305 305 305 306 307 307 307 307 308 311 311 312 313 313 313 313 313 313
44.1 44.2 45. Inform 45.1 45.2 45.3 45.4 Co Pr 45.5 45.6 Pr 45.7 Co Pr 45.8 46. 46.1 Ins. Co 46.2	Part 1	302 303 303 rosoft Internet 305 305 305 305 305 305 306 307 307 307 307 307 307 307 307 307 307 307 308 311 312 313 313 313 313 313 314 314
44.1 44.2 45. Inform 45.1 45.2 45.3 45.4 45.4 45.5 45.6 Pr 45.7 CC Pr 45.8 46. 46.1 Ins. CC 46.2	Part 1	302 303 303 rosoft Internet 305 305 305 306 307 307 307 307 308 311 311 312 313 313 313 313 313 313 313
44.1 44.2 45. Inform 45.1 45.2 45.3 45.4 45.4 45.5 45.6 Pr 45.7 CC Pr 45.8 46. 46.1 Ins Cc 46.2 46.3	Part 1	
44.1 44.2 45. Inform 45.1 45.2 45.3 45.4 45.4 45.5 45.6 Pr 45.7 CC Pr 45.8 46.1 Ins Cc 46.2 46.3 Ins Cc	Part 1	302 303 303 rosoft Internet 305 305 305 306 307 307 307 307 307 307 307 307 311 311 312 313 313 313 313 313 313 313

46.4 Installing IBM SecureWay Directory Server 3.2.2	
Configuring IBM SecureWay Directory Server 3.2.2 for PD 3.9	
46.5 Installing Active Directory	
Before You Start Installation	
Installation of Active Directory	
46.6 Installing Domino Server	
Domino Server Configuration Options	
Basic Configuration of Domino Server	
Configuration of Domino Administrator	
Configuring Lotus Domino Server to Run with Policy Director	
Modify Domino LDAP configuration	
Modify Domino HTTP Server Configuration	
Configure the PD Privileged User in Domino	
47. Appendix B WebSphere Installation	
47.1 Prerequisites and Preparations	
47.2 Procedure	
47.3 Configuring and Testing Your WebSphere Installation	
48. Appendix C Manual Installation of PD Web Portal Manager	
48.1 Manually Installing PD WPM into WebSphere	
Considerations	
Procedure	
49. Appendix D Banker 2001 Installation	
49.1 Loading the Banker 2001 Application into Websphere	
Importing the Application	
Starting and Testing the Application	
Part VII - Additional Information	
50. Publications	

Part I - Introduction

1. Introduction

This document should be read in conjunction with the formal product documentation. It is not an overview or description of Access Manager, but its scope is strictly limited to being a hands on guide designed to assist those installing IBM Tivoli Access Manager. 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 Access Manager

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

Part II - Windows Environment

Note: the Access Manager 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.

2. 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 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 6a or higher, or else Windows 2000 **Advanced Server** with Service Pack 2.
- Ensure that you have IP connectivity (for example, attempt to 'ping' another machine).
- It is **much** easier to install Access Manager 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 'Adamter', select 'MS Loopback Adapter', click on 'OK', click on 'OK', click on 'Close'. You will then need to specify an IP address for this adapter. You will probably also need to add an entry in C:\Winnt\system32\drivers\etc\hosts mapping IP address to fully qualified hostname in order to get reverse DNS to work.

3. Easy Install

Version 3.9 of Access Manager 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 Access Manager 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.

Note: These Easy Install scripts work very well on a 'clean' machine with a fresh Windows install on it (no web server, no DB2, no LDAP etc). However if you run into problems (particularly as a result of there being parts of other products remaining on the system) it may well be beneficial to stop using the Easy Install processes and instead go through the individual Native installation processes.

3.1 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 v7.1.5, GSKit, IBM HTTP Server, IBM SecureWayDirectory Client and Server v3.2.2.

Note: The LDAP Easy Install process works only on Windows NT file systems (NTFS) only.

- a. Uninstall any previous versions of the IBM SecureWay Directory, DB2 and IBM HTTP Server.
- b. If it exists, delete the **\ldapdb2** folder. (There appears to be a problem with installing the directory where there is already a database/instance present.)
- c. Ensure that the **db2admin** and **Idapdb2** 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** user id already exists then there appears to be no mechanism for supplying the **db2admin** password, and a DB2 installation error will result.)
- d. If it exists, delete C:\Program Files\IBM HTTP Server\conf\httpd.conf.
- e. Insert the IBM Tivoli Access Manager Base for Windows Version 3.9 CD.
- f. 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.
- g. Easy install starts in a command window:

```
IBM SecureWay Directory Server
Installation and Configuration

Product Status

IBM DB2 ..... Not Installed

IBM HTTP Server ..... Not Installed

IBM Global Security Toolkit ..... Not Installed

IBM SecureWay Directory Client ..... Not Installed

IBM SecureWay Directory Server ..... Not Installed
```

Version 1.1 – 30 September, 2002

Press ENTER to continue...

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

```
IBM DB2 Configuration Options
Option
                                        Value
 1. Administration ID ..... db2admin
 2. Administration Password .....
 3. Installation Directory ..... C:\Program Files\SQLLIB
Enter the Administration Password:
i. Enter the password for the db2admin Windows user that will be created (twice). (We used
 Secure99, if left as the default this would be db2admin).
 IBM DB2 Configuration Options
Option
                                        Value
 1. Administration ID ..... db2admin
 2. Administration Password .....
 3. Installation Directory ..... C:\Program Files\SQLLIB
Enter the Administration Password: *******
Re-enter the password for confirmation: *******
j. The configuration is updated:
 IBM DB2 Configuration Options
Option
                                        Value
 1. Administration ID ..... db2admin
 2. Administration Password ..... ******
 3. Installation Directory ..... C:\Program Files\SQLLIB
Enter the number of the option to modify or Y to continue:
k. Enter 'y' to confirm the displayed settings. The HTTP Server Configuration Options are
 displayed:
 IBM HTTP Server Configuration Options
                    -----
                                        Value
 Option
 1. Administration ID ..... Administrator
 2. Administration Password .....
 3. HTTP Port ..... 80
 4. Installation Directory ..... C:\Program Files\IBM HTTP Server
Enter the Administration Password:
I. Enter the Windows Administrator password, this is what the HTTP Server will use to start as a
```

Windows service. If a Windows administrator user with the user name of 'Administrator' does not exist then select option (1) and change the Administration ID. The options are then redisplayed.

Version 1.1 – 30 September, 2002

Note: if you are going to user a user name other than Administrator, make sure that this user name really does have all the Administrator privileges.

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

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

m. This is a good time to change the HTTP listening port from 80 in order to avoid port conflicts with WebSEAL later on, which by default listens on port 80. Select option '3' and configure another port, we used 81.

n. Press 'y' and 'Enter' to continue. The IBM GSKIT Configuration Options are displayed:

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

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

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

IBM SecureWay Directory Client	
Ontion	Value
1. Installation Directory	C:\Program Files\IBM\LDAP
	01 (110 g1 a 11100 (10.1 (10.1

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

p. Press 'y' and 'Enter' to accept the default installation directory for IBM LDAP Client. The LDAP Server Configuration Options are then displayed. Enter the password to be used for the LDAP Administrator user (cn=root). Type it again to confirm:

IBM SecureWay Directory Server Configuration Options

Option		Value
1. LDA	P Administrator ID (DN)	cn=root
2. LDA	P Administrator Password	
3. LDA	P Server Hostname	secure2
4. Suf:	fix	
5. LDA	? Server Port	389
6. LDA	SSL Keyfile	D:\common\pd ldapkey.kdb
7. LDA	P SSL Key File Password	* * * * * *
8. SSL	Client Certificate Label	PDLDAP
9. Inst	callation Directory	C:\Program Files\IBM\LDAP

Enter the LDAP Administrator Password: *******

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

q. You are prompted to enter the Suffix:

IBM SecureWay Directory Server Configuration	Options
Option	Value
1. LDAP Administrator ID (DN)	. cn=root
2. LDAP Administrator Password	. *****
3. LDAP Server Hostname	. secure2
4. Suffix	
5. LDAP Server Port	. 389

LDAP SSL Keyfile D:\common\pd_ldapkey.kdb
 LDAP SSL Key File Password ******
 SSL Client Certificate Label PDLDAP
 Installation Directory C:\Program Files\IBM\LDAP

Enter the Suffix:

r. Enter the suffix you want to be created for storage of Access Manager users and groups (we used ou=emea,o=ibm,c=gb):

IBM SecureWay Directory Server Configuration Options			
Option 1. LDAP Administrator ID (DN) 2. LDAP Administrator Password 3. LDAP Server Hostname	Value . cn=root . ******** . secure2		
 Suffix	<pre>. ou=emea,o=ibm,c=gb . 389 . D:\common\pd_ldapkey.kdb . ****** . PDLDAP C.\Deperarm Files\IPM\LDAP</pre>		
s. installation streetery			

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

- s. *** CHECK ***Note: Do not attempt to change the installation directory from C:\Program Files\IBM\LDAP - there appears to be a bug in the Easy Install script which means that no matter where you tell EZINSTALL to put LDAP, it will look for slapd32.conf in C:\Program Files\IBM\...\slapd32.conf.
- t. Enter 'y' to confirm the displayed settings. You are warned that the LDAP keystore provided will be copied onto the hard drive and you will see this message:

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

u. 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).

```
IBM SecureWay Directory Server
Installation and Configuration

Product Status

IBM DB2 ..... Not Installed

IBM HTTPD Server ...... Not Installed

IBM Global Security Toolkit 4 ..... Not Installed

IBM SecureWay Directory Client ..... Not Installed

IBM SecureWay Directory Server ..... Not Installed

Installing DB2 ..

To complete the installation/configuration, the system must be restarted

Press ENTER to continue...
```

v. 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 easy install 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 [7.1.5]

IBM HTTPD Server ...... Configured [1.3.19]

IBM Global Security Toolkit 4 ..... Configured [5.0.4.67]

IBM SecureWay Directory Client ..... Configured [3.2.2.0]

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...
```

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

IBM SecureWay Directory Server Installation and Configuration Product Status IBM DB2 Configured [7.1.5] IBM HTTP Server Configured [1.3.19] IBM Global Security Toolkit Configured [5.0.4.67] IBM SecureWay Directory Client Configured [3.2.2.0] IBM SecureWay Directory Server Installed [3.2.2.0] Configuring IBM SecureWay Directory Server... The IBM HTTP Server service is stopping... The IBM HTTP Server service was stopped successfully. The IBM HTTP Server service is starting. The IBM HTTP Server service was started successfully. Starting IBM SecureWay Directory Configuration *** DO NOT CANCEL THIS WINDOW *** *** This could take several minutes *** Cannot open message catalog file ldapadm.cat. 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 ou=emea,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 ou=emea,o=ibm,c=gb... Adding new entry ou=emea,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 Configured [7.1.5] IBM DB2 IBM HTTPD Server Configured [1.3.19] IBM Global Security Toolkit 4 Configured [5.0.4.67] IBM SecureWay Directory Client Configured [3.2.2.0] IBM SecureWay Directory Server Configured [3.2.2.0] Ezinstall completed successfully.

Press ENTER to continue...

x. When the screen above is displayed it means that the IBM 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 easy install.

3.2 Easy Install of Access Manager Management Server

Use the **ezinstall_pdmgr** batch file to install the AM Runtime and AM Policy Server components. This sets up a workstation with the following packages; GSKit, IBM Directory Client v3.2.2, AM Runtime and AM Policy Server. We performed the steps documented here on the same machine as the previous install of the Directory.

a. Insert the IBM Tivoli Access Manager Base for Windows Version 3.9 CD.

- b. Use Windows Explorer to open the drive where the CD image is located. In the root directory of this drive launch the **ezinstall_pdmgr.bat** file by double-clicking on it.
- c. Easy install 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]:

d. Easy Install 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 IBM Tivoli Access Manager Runtime Configuration Options are displayed and you are invited to enter the LDAP Server Hostname:



Enter the LDAP Server Hostname:

e. Enter the LDAP Server Hostname. Since LDAP is installed locally this should be the DNS name of the local host (**secure2.pic.uk.ibm.com** in our case). You will be invited to enter a suffix:

IBM Tivoli Access Manager Runtime Configuration Options	
Option Value	
1. Configure Using This Registry Type ldap	
2. LDAP Server Hostname secure2.pic.uk.ibm.com	
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	

Enter the Suffix:

f. 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 (we used **ou=emea,o=ibm,c=gb**). If you want to use a different suffix you need to make sure that the object already exists in LDAP.

```
IBM Tivoli Access Manager Runtime Configuration Options
-----
Option Value
```



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

g. 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: enter 'n'. The Access Manager Management Server Configuration Options screen is re-displayed:

IBM Tivoli Access Manager Policy Server Configuration Options



Enter the LDAP Administrator Password:

- h. Enter the LDAP Administrator password. This is the password that you set for cn=root during LDAP configuration.
- i. You are then asked to enter the password that will be used for the Access Manager master user, **sec_master**. Enter the password you want and the re-enter for confirmation:



j. You must now decide if other Access Manager machines will be able to download the Access Manager internal CA certificate from the management server. This saves a manual step when configuring remote Access Manager machines but removes the security of having a manual CA Certificate transfer. We chose 'y' for this install to keep things simple, for a demonstration type environment.

Allow other PD Client machines to download the certificate file? [Y \mid N]: Y

k. The installation and configuration begins. IBM GSKIT and the 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 easy install starts with the installation of the AM Runtime. If LDAP were installed on a different machine the easy install would have installed IBM GSKIT and the LDAP Client at this point.

IBM Tivoli Access Manager Policy Server Installation and Configuration

```
ProductStatusIBM Global Security ToolkitConfigured [5.0.4.67]IBM SecureWay Directory ClientConfigured [3.2.2.0]Access Manager RuntimeNot InstalledAccess Manager Policy ServerNot Installed
```

Installing Tivoli SecureWay Policy Director Runtime.

I. The installation will proceed until a re-boot is required:

IBM Tivoli Access Manager Policy Server Installation and Configuration

```
ProductStatusIBM Global Security ToolkitConfigured [5.0.4.67]IBM SecureWay Directory ClientConfigured [3.2.2.0]Access Manager RuntimeInstalled [3.9]Access Manager Policy ServerNot InstalledInstalling IBM Tivoli Access Manger Policy ServerInstalled
```

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

m. Press 'Enter' to re-boot the machine. Once the machine has finished re-booting log into Windows using the same user id as before. The easy install will automatically carry on where it left off with the configuration of Access Manager Runtime. You should see the installation progress as shown below:

IBM Tivoli Access Manager Policy Server Installation and Configuration

Product

Status

```
      IBM Global Security Toolkit
      Configured [5.0.4.67]

      IBM SecureWay Directory Client
      Configured [3.2.2.0]

      Access Manager Runtime
      Configured [3.9]

      Access Manager Policy Server
      Installed [3.9]

      Configuring IBM Tivoli Access Manager Policy Server...

      IBM Tivoli Access Manager Policy Server

      Installation and Configuration

      Product
      Status

      IBM Global Security Toolkit
      Configured [5.0.4.67]

      IBM SecureWay Directory Client
      Configured [3.2.2.0]

      Access Manager Runtime
      Configured [3.2.2.0]

      Access Manager Policy Server
      Configured [3.9]

      Ezinstall completed successfully.
      Press ENTER to continue...
```

n. When the screen above is displayed it means that the Access Manager Policy Server has been successfully installed and configured. Access Manager Runtime is also installed which means that you can use PDADMIN for command-line administration. Press 'ENTER' to exit easy install.

3.3 Easy Install of Access Manager WebSEAL

Use the **ezinstall_pdweb** batch file to install WebSEAL. This sets up a workstation with the following packages; GSKit, IBM Directory client v3.2.2, AMRTE and WebSEAL. Again we installed this on the same machine as the directory and AM Policy Server.

- a. Insert the IBM Tivoli Access Manager Web Security for Windows Version 3.9 CD.
- b. Ensure that the IBM SecureWay Directory V3.2.2 and the Access Manager Policy Server services are started.
- c. Use Windows Explorer to open the drive where the CD image is located. In the root directory of this drive launch the **ezinstall_pdweb.bat** file by double-clicking on it. Easy install 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]:

d. Easy install 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:

Enter the Security Master Password:

e. Enter the password you configured for sec_master during the PD Management Server installation. The installation and configuration begins:

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

Product Status
IBM Global Security Toolkit ..... Configured [5.0.4.67]
```

```
IBM SecureWay Directory Client ..... Configured [3.2.2.0]
Access Manager Runtime ..... Configured [3.9]
IBM Tivoli AM WebSEAL Server .... Not Installed
```

Installing Policy Director WebSEAL Server...

IBM Tivoli Access Manager WebSEAL Server (PDWEB) Installation and Configuration

```
ProductStatusIBM Global Security ToolkitConfigured [5.0.4.67]IBM SecureWay Directory ClientConfigured [3.2.2.0]Access Manager RuntimeConfigured [3.9]IBM Tivoli AM WebSEAL ServerInstalled [3.9]
```

Configuring Access Manager WebSEAL...

IBM Tivoli Access Manager WebSEAL Server (PDWEB)

Installation and Configuration		
Product IBM Global Security Toolkit IBM SecureWay Directory Client Access Manager Runtime IBM Tivoli AM WebSEAL Server	Status Configured Configured Configured Configured	[5.0.4.67] [3.2.2.0] [3.9] [3.9]
ezinstall completed successfully.		
Press ENTER to continue		

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

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). You can now check that Access Manager is working by following the steps described in Section 22 - Initial Access Manager Validation on Page 170 below.

4. Easy Install process to set up Access Manager components on a remote machine

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

4.1 Easy Install of Access Manager WebSEAL

Use the **ezinstall_pdweb** batch file to install WebSEAL. This sets up a workstation with the following packages; GSKit, IBM Directory client v3.2.2, AM Runtime and WebSEAL.

a. Insert the IBM Tivoli Access Manager Web Security for Windows Version 3.9 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. Easy Install starts in a command window:

```
IBM Tivoli Access Manager WebSEAL Server (PDWEB)
 Installation and Configuration
Product
                                            Status
 IBM Global Security Toolkit ..... Not Installed
 IBM SecureWay Directory Client ..... Not Installed
Access Manager Runtime ..... Not Installed
IBM Tivoli AM WebSEAL Server ..... Not Installed
 Press ENTER to continue...
c. This shows the current status of the components required for WebSEAL. Press 'ENTER'. The
 IBM GSKIT Configuration Options are displayed - enter '\mathbf{y}' to accept the default installation
 directory for IBM GSKIT:
 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: \boldsymbol{y}
d. The LDAP Client Configuration Options are then displayed. Enter 'y' to accept the default
 installation directory for IBM LDAP Client:
```

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: \boldsymbol{y}

e. The Access Manager Runtime Configuration Options are then displayed:

IBM Tivoli Access Manager Runtim	e Configuration Options
Option	Value
1. Configure Using This Registr	y Type ldap

IBM Tivoli Access Manager 3.9 - Cookbook

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.pic.uk.ibm.com):

IBM Tivoli Access Manager Runtime Configuration Options

Opt:	ion	Value
1.	Configure Using This Registry Type	ldap
2.	LDAP Server Hostname	secure2.pic.uk.ibm.com
з.	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.	Access Manager Policy Server Hostname	
12.	SSL Server Port for AM Policy Server	7135
13.	Policy Server CA Certificate Filename	

Enter the Suffix:

g. Enter the suffix where you specified the GSO database should be created when setting up the Access Manager Management Server (we choose to use o=ibm,c=gb):

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

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, so enter 'n'.

IBM Tivoli Access Manager Runtime Configuration	Options
Option Va	alue
1. Configure Using This Registry Type	ldap
2. LDAP Server Hostname s	secure2.pic.uk.ibm.com

IBM Tivoli Access Manager 3.9 – Cookbook

3.	LDAP Server Port	389
4.	Suffix	ou=emea,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.	Access Manager Policy Server Hostname	
12.	SSL Server Port for AM Policy Server	7135
13.	Policy Server CA Certificate Filename	

Enter the host name of the Policy Director Management Server:

i. The Access Manager Runtime needs to know where to contact the Policy Server. Enter the full DNS name of the machine where the Access Manager policy server is installed (secure2.pic.uk.ibm.com in our case):

IBM Tivoli Access Manager Runtime Configuration Options
Option Value 1. Configure Using This Registry Type ldap 2. LDAP Server Hostname secure2.pic.uk.ibm.com 3. LDAP Server Port 389 4. Suffix ou=emea,o=ibm,c=gb 5. Enable SSL with LDAP Server n 6. LDAP SSL Keyfile n 7. LDAP SSL Keyfile DN 636 10. Installation Directory C:\Program Files\Tivoli\Policy Director 11. Access Manager Policy Server Hostname secure2.pic.uk.ibm.com 12. SSL Server CA Certificate Filename 7135
If you have enabled Policy Server to allow the download of the certificate files, leave this option blank. Otherwise, specify the pdcacert.b64 file created by the Policy Server configuration. Enter the path to the Access Manager for e-business Certificate File:

j. In order for the Access Manager Runtime to authenticate the other Access Manager servers it connects to it must have a copy of the AM CA Certificate that was generated by the Policy Server when it was configured. This can either be manually copied to the local machine or downloaded as part of the configuration of AM Runtime. If when you configured the Policy Server you said we would allow the AM CA Certificate to be downloaded then you can simply press **ENTER** here to continue:

Opt	ion	Value
1.	Configure Using This Registry Type	ldap
2.	LDAP Server Hostname	secure2.pic.uk.ibm.com
3.	LDAP Server Port	389
4.	Suffix	ou=emea,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.	Access Manager Policy Server Hostname	secure2.pic.uk.ibm.com
12.	SSL Server Port for AM Policy Server	7135
13.	Policy Server CA Certificate Filename	c:\pdcacert.b64

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

k. Enter 'y' to confirm the displayed settings. Next the WebSEAL configuration options are required.



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 easy install will automatically restart.

```
Access Manager WebSEAL Server (PDWEB) Options
Option Value
1. Security Master Password ...... ******
```

Enter the Security Master Password:

p. When prompted enter the password for **sec_master**. You are asked for this password as it is required to complete the configuration and is not stored in the response file for security reasons. Easy install will carry on where it left off with the configuration of Access Manager Runtime:

IBM Tivoli Access Manager WebSEAL Server (PDWEB) Installation and Configuration

```
ProductStatusIBM Global Security ToolkitConfigured [5.0.4.67]IBM SecureWay Directory ClientConfigured [3.2.2.0]Access Manager RuntimeInstalled [3.9]IBM Tivoli AM WebSEAL ServerInstalled [3.9]
```

Configuring IBM Tivoli Access Manager Runtime...

IBM Tivoli Access Manager WebSEAL Server (PDWEB) Installation and Configuration

```
ProductStatusIBM Global Security ToolkitConfigured [5.0.4.67]IBM SecureWay Directory ClientConfigured [3.2.2.0]Access Manager RuntimeConfigured [3.9]IBM Tivoli AM WebSEAL ServerConfigured [3.9]
```

Ezinstall completed successfully.

Press ENTER to continue...

- q. When the screen above is displayed it means that Access Manager WebSEAL has been successfully installed and configured. Press '**ENTER**' to exit easy install.
- r. 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).
- s. Access Manager Runtime has also been installed on the machine so PDADMIN is available for command-line administration from this machine.

5. Easy Install - Web Portal Manager

5.1 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. If there is any possibility that a Web Portal Manager installation has been previously attempted on the machine in question, run regedit. If the following registry key entry exists: HKEY_LOCAL_MACHINE\SOFTWARE\TivoliPolicy Director Web Portal Manager delete it. (As stated in the Release Notes, the presence of this registry key will cause the WPM Easy Installation to fail.)
- b. Insert the IBM Tivoli Access Manager Web Portal Manager for Windows Version 3.9 CD.
- c. 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.
- d. Easy install starts in a command window:

Press ENTER to continue..

e. 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:

f. Type 'y' to continue. The IBM HTTP Server Configuration Options will be displayed:

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

Enter the Administration Password:

g. Enter the Windows Administrator password - this is what the HTTP Server will use to start as a Windows service. If a Windows administrator user with the user name of **Administrator** does not exist then select option (1) and change the Administration ID. The options are then redisplayed.

Note: if you are going to user a user name other than Administrator, make sure that this user name really does have all the Administrator privileges.

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

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

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

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

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

i. Enter 'y' to continue. The Access Manager Runtime Configuration Options are displayed:

IBM Tivoli Access Manager Runtime Configuratic	n Options
Option	Value
1. Configure Using This Registry Type	ldap
2. LDAP Server Hostname	
3. LDAP Server Port	389
4. Suffix	
5. Enable SSL with LDAP Server	
6. LDAP SSL Keyfile	
7. LDAP SSL Keyfile DN	
8. LDAP SSL Key File Password	
9. LDAP Server SSL Port	636
10. Installation Directory	C:\Program Files\Tivoli\Policy Director
11. Access Manager Policy Server Hostname	
12. SSL Server Port for AM Policy Server	7135
13. Policy Server 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.pic.uk.ibm.com** in our case):

IBM	Tivoli Access Manager Runtime Configuration Options
Opt	ion Value
1.	Configure Using This Registry Type ldap
2.	LDAP Server Hostname secure2.pic.uk.ibm.com
З.	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.	Access Manager Policy Server Hostname
12.	SSL Server Port for AM Policy Server 7135

Version 1.1 – 30 September, 2002

13. Policy Server CA Certificate Filename

Enter the Suffix:

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

```
IBM Tivoli Access Manager Runtime Configuration Options
```

Opt:	ion	Value
1.	Configure Using This Registry Type	ldap
2.	LDAP Server Hostname	secure2.pic.uk.ibm.com
3.	LDAP Server Port	389
4.	Suffix	ou=emea,o=ibm,c=gb
5.	Enable SSL with LDAP Server	
6.	LDAP SSL Keyfile	
7.	LDAP SSL Keyfile DN	
8.	LDAP SSL Key File Password	
9.	LDAP Server SSL Port	636
10.	Installation Directory	C:\Program Files\Tivoli\Policy Director
11.	Access Manager Policy Server Hostname	
12.	SSL Server Port for AM Policy Server	7135
13.	Policy Server CA Certificate Filename	

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

I. 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':

IBM Tivoli	. Access	Manager	Runtime	Configuration	Options	

Opti	on	Value
1.	Configure Using This Registry Type	ldap
2.	LDAP Server Hostname	secure2.pic.uk.ibm.com
3.	LDAP Server Port	389
4.	Suffix	ou=emea,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.	Access Manager Policy Server Hostname	
12.	SSL Server Port for AM Policy Server	7135
13.	Policy Server CA Certificate Filename	

Enter the host name of the Policy Director Management Server:

m. PD Runtime needs to know where to contact the Management Server. Enter the full DNS name of the machine where the Access Manager Policy Server is installed (secure2.pic.uk.ibm.com in our case):

IBM	IBM Tivoli Access Manager Runtime Configuration Options			
Opt	ion Value			
1.	Configure Using This Registry Type ldap			
2.	LDAP Server Hostname secure2.pic.uk.ibm.com			
з.	LDAP Server Port			
4.	Suffixou=emea,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			
10.	Installation Directory C:\Program Files\Tivoli\Policy Director			
11.	Access Manager Policy Server Hostname secure2.pic.uk.ibm.com			
12.	SSL Server Port for AM Policy Server 7135			

13. Policy Server CA Certificate Filename

If you have enabled Policy Server to allow the download of the certificate files, leave this option blank. Otherwise, specify the pdcacert.b64 file created by the Policy Server configuration. Enter the path to the Access Manager for e-business Certificate File:

n. In order for AM Runtime to authenticate the other Access Manager servers it connects to it must have a copy of the AM CA Certificate that was generated by the Policy Server when it was configured. This can either be manually copied to the local machine or downloaded as part of the configuration of AM Runtime. This will depend on the choice we made when we were configuring the Policy Server.

IBM	Tivoli Access Manager Runtime Configuration	n Options
Opt	ion	Value
1.	Configure Using This Registry Type	ldap
2.	LDAP Server Hostname	secure2.pic.uk.ibm.com
З.	LDAP Server Port	389
4.	Suffix	ou=emea,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.	Access Manager Policy Server Hostname	secure2.pic.uk.ibm.com
12.	SSL Server Port for AM Policy Server	7135
13.	Policy Server CA Certificate Filename	

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

 e. Enter 'y' to continue. The IBM WebSphere Configuration Options are displayed. Enter the Windows Administrator password. This is what WebSphere will use to start as an Windows service:

IBM WebSphere Configuration Options	
Option	Value
1. Administration ID	. Administrator
2. Administration Password	C.\WebCabere\AppCorter
3. Installation Directory	. C: (websphere Appserver

Enter the Administration Password: *******

p. A summary of entries is shown:

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

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

- q. If a Windows administrator user with the user name of Administrator does not exist then select option (1) and change the Administration ID. The options are then re-displayed. Note: if you are going to user a user name other than Administrator, make sure that this user name really does have all the Administrator privileges.
- 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.

IBM Tivoli Access Manager Web Portal Manager Installation and Configuration

Version 1.1 – 30 September, 2002

IBM Tivoli Access Manager 3.9 – Cookbook

Product Status IBM Global Security Toolkit Not Installed IBM HTTP Server Not Installed IBM SecureWay Directory Client Not Installed Access Manager Runtime Not Installed IBM WebSphere Application Server Not Installed Access Manager Web Portal Manager Not Installed Installing IBM Global Security Toolkit. IBM Tivoli Access Manager Web Portal Manager Installation and Configuration Product Status IBM Global Security Toolkit Configured [5.0.4.67] IBM HTTP Server Configured [1.3.19] IBM SecureWay Directory Client Configured [3.2.2.0] Access Manager Runtime Configured [3.9] IBM WebSphere Application Server Not Installed Access Manager Web Portal Manager Not Installed Installing IBM WebSphere Application Server 4.0. IBM Tivoli Access Manager Web Portal Manager Installation and Configuration Product Status IBM Global Security Toolkit Configured [5.0.4.67] IBM HTTP Server Configured [1.3.19] IBM SecureWay Directory Client Configured [3.2.2.0] Access Manager Runtime Installed [3.9] IBM WebSphere Application Server Configured [4.0] Access Manager Web Portal Manager Not Installed Installing IBM Tivoli Access Manager 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 installation will then continue once you log in. The runtime environment is configured:

IBM Tivoli Access Manager Web Portal Manager Installation and Configuration

```
ProductStatusIBM Global Security ToolkitConfigured [5.0.4.67]IBM HTTP ServerConfigured [1.3.19]IBM SecureWay Directory ClientConfigured [3.2.2.0]Access Manager RuntimeInstalled [3.9]IBM WebSphere Application ServerConfigured [4.0]Access Manager Web Portal ManagerInstalled [3.9]
```

Configuring IBM Tivoli Access Manager Runtime...

Version 1.1 – 30 September, 2002

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: ...

IBM Tivoli Access Manager Web Portal Manager Installation and Configuration

ProductStatusIBM Global Security ToolkitConfigured [5.0.4.67]IBM HTTP ServerConfigured [1.3.19]IBM SecureWay Directory ClientConfigured [3.2.2.0]Access Manager RuntimeConfigured [3.9]IBM WebSphere Application ServerConfigured [4.0]Access Manager Web Portal ManagerConfigured [3.9]

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.pic.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. This process is described in Section 6.14 Changing Web Portal Manager port numbers (Windows) on Page 88 below.
- v. You can verify Web Portal Manager operation as described in Section 6.15 -

Verify Web Portal Manager operation on Page 94 below.

Note: If the Web Portal Manager configuration fails with an error message which says to check if the admin server is started, use Start -> Settings -> Control Panel -> Services (NT), or Start -> Programs -> Administrator Tools -> Services (2000), to ensure that the IBM WS AdminServer is running. If it is not already running, then starting it and then re-running **ezinstall_pdwpm.bat** may help.

6. Native installation process

This section describes the techniques for installing Access Manager and its components without the easy install scripts.

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 Access Manager Servers or Web Portal Manager. If you currently have a version of GSKit installed on your system, verify the version is at **5.0.4.67 or above**. To determine the version you currently have installed, issue the **gskver** command from **C:\Program Files\IBM\gsk5\bin** and check the Product Version that is displayed.

- a. Log in to Windows as a user with administrator privileges.
- b. Insert the IBM Tivoli Access Manager Base for Windows Version 3.9 CD.
- c. Start a command prompt.
- d. From the command prompt, change to the windows\gskit directory on the drive where the CD is located and enter the following command: setup.exe PolicyDirector
- e. The GSKit welcome screen is displayed:



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

choose Destination Lot	auon	^
	Setup will install GSK5 in the following folder.	
	To install to this folder, click Next.	R
-	To install to a different folder, click Browse a folder.	nd select another
	You can choose not to install GSK5 by clicki Setup.	ing Cancel to exit
2	Destination Folder C:\Program Files\ibm\gsk5	Browse
	< <u>B</u> ack	Cancel

g. Click on 'Next'. Files are copied across. Then the 'Setup Complete' dialogue box is displayed:
IBM Tivoli Access Manager 3.9 – Cookbook



h. 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.
- You can find additional information on configuring the IBM Directory in the *IBM SecureWay Directory for Windows NT Installation and Configuration guide* – this is on the **IBM Tivoli Access Manager Base for Windows Version 3.9** CD at \doc\Directory
- a. Uninstall any previous versions of the IBM SecureWay Directory, DB2 and IBM HTTP Server.
- 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 **Idapdb2** 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 it exists, delete C:\Program Files\IBM HTTP Server\conf\httpd.conf.
- e. Insert the IBM Tivoli Access Manager Base for Windows Version 3.9 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 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.)

;	Select the language for t the choices below.	his installation from
	U.S. English	
	ок	Cancel

- g. Select a language and click on 'OK'.
- h. The InstallShield runs and the IBM HTTP Server 1.3.19 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 Administrator user id and password under which IBM HTTP Server will run:



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 Directory V3.2.2 Software License Agreement is displayed:



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.
æ. y	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 GSKit and a web server are already installed:



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

Please select th	e 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.
	< <u>Back Next> Cancel</u>

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 option is deselected (as we have already installed it):



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'. DB2 is installed and files are copied across. (In the event of a failure of the silent DB2 installation, it is worth referring to the installation log file C:\DB2LOG\db2.log.) The 'Readme' panel is displayed and you are invited to view 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?
	<u>Yes</u> <u>N</u> o

- aa. Select 'Yes' or 'No' as you feel appropriate.
- bb. The 'Setup Complete' panel is displayed. Select 'Yes, I want to restart my computer now':

	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.
2	Click finish to complete the Setup.
	C Flack Finish

- cc. Click on 'Finish'.
- dd. When the system restarts, log in again as the administrator.

6.3 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:

Service	Status	Startup	Close
Alerter	Started	Automatic 💽	
ClipBook Server		Manual	Start
COM+Event System		Manual	
Computer Browser	Started	Automatic	Stop
DB2 - DB2	Started	Automatic	Burne
DB2 - DB2DAS00	Started	Automatic	Eause
DB2 Governor		Manual	Continue
DB2 Security Server		Manual	- Helenhunderer
DHCP Client		Disabled	Charlum
Directory Replicator		Manual 💌	
			H <u>W</u> Profiles.
Startup Parameters:			
			Help

b. Use Start → Programs → IBM SecureWay Directory → Directory Configuration. The IBM SecureWay Directory 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: 	
Help ABack	Next Cancel

Version 1.1 – 30 September, 2002

d. Click on 'Next'. Another 'IBM SecureWay Directory Configuration' panel will be displayed:



e. Click on 'Next'. Another 'IBM SecureWay Directory Configuration' panel will be displayed:



f. (Ensure that you do not enable Change Log support as this will cause a performance impact.) Click on '**Next**'; another '**IBM SecureWay 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.



h. Ensure that '**IBM HTTP**' is selected. Click on '**Next**'. You will be prompted about the location of 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		
BM HTTP web server configuration file:			~
C:\Program Files\IBM HTTP Server\conf\httpd.conf	Browse	1	E IN
			3 March
			1
		X	and the second s
		1	
Help	< <u>₿</u> ack	Next •	Cancel

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



j. Review the settings and click on **'Configure'**. The background window will start displaying messages regarding creating and configuring the ldapadb2 database:

Directory Configuration	_ 🗆 🗵
Added account rights to account: Idapdb2.	
Creating database instance: ldapdb2.	
Created database instance: ldapdb2.	
Logging on user: ldapdb2.	
Logged on user: ldapdb2.	
Impersonating user.	
Impersonated user	
Logging on user: Idapdb2.	
Logged on user: Idapdb2.	
Impersonating user.	
Impersonated user.	
Cataloging node: Idapan2.	
Cataloged doubles inapunz.	
Starting ustabase manager for instance. Idaydb2	
Attaching to instance: Idandb2	
Attached to instance: Idaudb2	
Creating database: Idanda	
Created database: Idandb2.	
Getting configuration for database: ldavdb2.	
Got configuration for database: ldapdb2.	
Updating configuration for database: ldapdb2.	
Updated configuration for database: ldapdb2.	
Completed configuration of the database.	

k. A 'Configuration Summary' is then displayed:

IBM SecureWay Directory Configuration	n	
Configuration Summary		
Directory configuration completed w	thout errors.	
of Admin DN update:	Success	
DB2 configuration:	Success	-
Change Log configuration:	Not selected	1 A
I Web server update:	Success	
The web server must be restarted fo Administration: http://secure2.80/idap/index.html	r changes to take effect. Use the following URL to access Serve	er
Help	Start Over	Ok

- I. Click on 'OK'.
- m. By default the IBM HTTP Server listens to port 80, the same as WebSEAL. If you are going to install WebSEAL on the same machine, 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 stop and restart IBM HTTP Server for the changes made by the LDAP configuration and the port number change 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:

(or specify any drive that has space for the database)

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

WHICH WEIC CHU		· / ·
SecureWay Directory Server	Web Admin: secure2 - Netscape	_ & ×
Elle Edit View Go Communicati	a Helb	
Back Forward Reload	A A A A A A A A A A A A A A A A A A A	N
🕺 🆋 Bookmarks 🛭 🙏 Location:	http://secure2.pisc.uk.ibm.com:81/ldap/cgi-bin/ldacgi.exe?Action=Start	💌 🍘 What's Related
🕺 🚴 Instant Message 🛛 🖳 WebMa	ali 🖳 Contact 🖳 People 🖳 Yellow Pages 🖳 Download 📩 Channels	
Conservation and the second		
Directory Server	Logon	?-
Introduction	Xisecure2	
E Logon	K Ready	
	TPM SamueWay Divertary Samuer Administration	TEM.
	initiation	24/110
	Please enter the LDAP administrator ID and password and click Logon.	
	Admin ID cn=root	
	Password *******	
	Logon	
	AN Conversion TDM Conversion 1002 2000 Attractive conversal	
	(c) Copyright film Corporation 1998, 2000. All rights reserved.	
Docum	ent 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 '<u>Add suffixes</u>'. Enter secAuthority=Default in the 'Suffix DN' box. Access Manager requires that you create this suffix which is used to maintain Access Manager metadata. You must add this suffix only once when you first configure the LDAP server.



- s. Click on '**Update**'. The suffix should be added to the list of 'Current server suffixes' and a message should be displayed stating 'The list was successfully added. You must <u>restart the server</u> for this change to take effect'.
- t. Enter a suffix for the Access Manager 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 Access Manager resources subsequently defined must sit below the suffix defined here thus if the country, organization and organizational unit are specified here, all AM resources will have to be held within that organizational unit, whereas if just the country is specified here, all AM 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			_ & X
Lie Fox Xiew Bo Fourierunga	or neep 🚵 🚵	i 🕹	: <u>()</u>	(1)	N
Back Forward Reload	Home Search Netscape	Find Secu	rity Shop	Stop	
Bookmarks & Location	ail 🔯 Contact 🔯 Republic	Valow Paper B	Download	Channels	• Q ₃ p what's helated
	an 🕞 contact 🕞 reopie 🕞	Tollow Tages	a Download	Creatinge	
Bootmarks & Locador Bootmarks & Locador Bootmarks & Locador Bootmarks & Webb Directory Steven Performance Performance Transactions Event notification Suffixes Performance Referrals Socurity Replectation Database Logoff	Imp://recurs2.pisc.uk.hm.com/f1/ai W Contact W People W Suffixes ★ secure2 The list was successful To add a suffix, enter the d Suffix DN our=enea, The table below displays as beneath that suffix, howevee Current server suffixes cn=localhost isecAuthority=Default Note: The determination of wf Update Reset Related tasks: General - Edit the pr Performance - Char Transachone - Edit Schema - Edit the volume 	Idap/cgi/bin/dac; Yelow Pages L Ivy updated, You istinguished na o= ibm, c=gb iffixes defined r the data is n Comment System suffix nether a suffix nether a suffix nether a suffix nether a suffix nether a suffix of the search ransactions se did event notific and remove r alidation setting	is we?Actor=Sit & is we?Actor=Sit & must costart if me of the suf to this server; to this server; tremoved fr Remove? Intains director password enc israts, and cor trings for the p cation setting ferrals for the s and schemes	t Chornels	s to all directory data
all websel	one her unbauer herstel blevelikerel	at manager		II	
[Mphee	company reported and relaid wpp	a starting			- 🐝 🛥 🗤 🕬 🌾 🛛

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:

SecureWay Directory Server V File Edit View Go Communicato	WebAdmin:secure2-Netscap r Helo	e		
Back Forward Reload	Home Search Netscape	Print Seco Idap/ogi-bin/Idac Yellow Pages	i () utiv Shop giexe?Action=Sta	Com t Chomate
Directory Server	Suffixes			• ?-
Threaddana ▼ Settings	X secure2			
General	I he list was successful	ly updated. You	i must <u>restart th</u>	a <u>server</u> for this change to take effect.
 Performance Transactions Event notification 	To add a suffix, enter the d	istinguished n	ame of the suf	ix, then click Update .
Suffixes	Suffix DN			-
Referrals				
Security Replication Database	The table below displays su beneath that suffix, howeve	iffixes defined r the data is r	l to this server tot removed fr	To remove a suffix, select the checkbox and click Update . Removing a suffix eliminates access to all directory data m the directory.
Current state	Current server suffixes	Comment	Remove?	
Logoff	cn=localhost	System suffic	ĸ	
	ou=emea, o=ibm, c=gb			
	secAuthority=Default			
	Note: The determination of wh	ether a suffix c	ontains director	r data can not be made while the serveris stopped.
	<u>General</u> - Edit the p <u>Performance</u> - Chan <u>Transactoms</u> - Edit <u>Event notification</u> - I <u>Referrals</u> - List, add <u>Schema</u> - Edit the va	rt, referral or nge the search ransactions se Edit event noti and remove : alidation settin	password enc limits, and con titings for the p fication setting referrals for th gs and scheme	yption settings nections settings to enhance performance. Tocessing of grouped operations to enable a clernt or early enternate location when the directory tree is modified. Is server: Referrals are an alternate location where directory information may be found. file has loaded at startup.
Applet c	com ibm.webexec.herald.HeraldApple	et running		

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.

<u>File Edit View Go Communi</u>	cator Help	
ack Forward Reloa	d Home Search Netrcape Fint Security Shop Stop	N
🕺 🏒 Bookmarks 🙏 Locati	ion: http://secure2.pisc.uk.ibm.com:81/ldap/cgi-bin/ldacgi.exe?Action=Start	👻 🎧 🔭 What's Related
🧴 🚴 Instant Message 🛛 Web	aMail 🖳 Contact 🖳 People 🖳 Yellow Pages 🖳 Download 📩 Channels	
Contraints → Dearlier Contraints → Dearlier Controluction Controlu	Mail Contact People Yelow Pages Download Channels Mail Contact People Yelow Pages Image: Stop Secure2 The directory server is running. The directory server is currently 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.	© ?-
💣 🗫 🛛 🗛 App	let com.ibm.webexec.herald.HeraldApplet 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. 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 <code>ibm-slapdPwEncryption</code> line to:

ibm-slapdPwEncryption: crypt

If the LDAP Server won't start... make sure Active Directory isn't also listening on port 389

We have seen problems where the DB2 configuration has succeeded, but the LDAP server will not start. Running the LDAP facility indicates that a bind failed with an error code 2.

It turned out that Active Directory was listening on port 389 (the LDAP port), which caused the LDAP configuration to fail. The resolution was to configure LDAP to listen on a port other than 389 (either using the web interface or through editing slapd32.conf.)

6.4 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 LDAP Administrator ID and password which were entered previously (cn=root and Secure99 in our case):

IBM Tivoli Access Manager 3.9 – Cookbook

🍲 IBM SecureWay Directory Management Too	۱ <u>ــــــــــــــــــــــــــــــــــــ</u>	
冒 Idap://localhost.389	Rebind	>
Introduction	Ready IBM	ø
B Status Administration B Rebind	Enter a new bind DN and password for the server Idap://localhost.389	
🖻 😋 Schema 🚽 Diefreshischema	C Anonymous © Authenticated	_
 ⊡ Object classes ⊡ Attributes 	User DN : [cn=root User password : *******	
Matching rules Syntaxes Syntaxes Syntaxes Arcs tree Browse tree Browse tree Search tree Simple search Advanced search Syntaxed search Clear log file 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 Tool			_ 🗆 🗵
ldap://localhost.389	Browse tree		?
Introduction	Ready		IBM.
- D Status - D Administration - D Rebind	The search Image: Sear	Delete ACL	Edit RDN A
Add server Delete server Exit	Idap://localhost:389 ⊞ - en=localhost		

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 Access Manager users and Global Sign-On (GSO) data (ou=emea, o=ibm, c=gb in our case).

If you have specified an organizational unit (as in our case), select Select 'Organizational unit' as

the entry type in the pull down list.

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

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

Add an LD	AP Entry	
Select an En	try type, enter the Parent DN, modify the Entry RDN, then click OF	¢.
Entry type	Organizational unit 💌	
Parent DN:		
Entry RDN.	jou=emea,u=iom,c=go	
	OK Cancel Help	

f. Click on 'OK':

jectClass (Object class):	organizatio	onalUnit	
(DN):	ou≃emea,	o=ibm,c=gb	
ttributes			
ou:	0	emea,o=ibm,c=gb	2
businessCategory:	0		
description:	2		
destinationIndicator:	2		
facsimileTelephoneNumber:	0		
internationalISDNNumber:	0		
Ē.	0		
physicalDeliveryOfficeName:	0		
postalAddress:	0		
postalCode:	0	1	

- 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.

6.5 Install IBM SecureWay Directory Version 3.2.2 e-fix 2

- a. Download the Readme and code for the IBM SecureWay Directory Version 3.2.2 e-fix 2 from http://www.ibm.com/software/network/directory/support/fixes/
- b. Review the contents of the Readme.
- c. Issue an Idapsearch or use the Directory Management Tool to ensure that LDAP is operating correctly.
- d. Use Start → Settings → Control Panel → Services (NT) or Start → Administrator Tools → Services (Windows 2000) to stop the **IBM SecureWay Directory V3.2.2** service.
- e. You may like to back up the LDAP install directory this is C:\Program Files\IBM\LDAP by default.
- f. Unzip 3.2.2-SWD-002-WIN.zip to a temporary directory we used C:\Temp\ldapfix2
- g. Copy the files from the temporary directory to the LDAP install directory the output should look similar to the following:



```
C:\temp\ldapfix2\web\cgi-bin\ldacgi3.exe
C:\temp\ldapfix2\web\readme\buildno.txt
39 File(s) copied
C:\Program Files\IBM\LDAP>
```

- h. Verify that the new file sizes match those specified in the Readme.
- i. Use Start → Settings → Control Panel → Services (NT) or Start → Administrator Tools → Services (Windows 2000) to start the **IBM SecureWay Directory V3.2.2** service.
- j. Issue an Idapsearch or use the Directory Management Tool to ensure that LDAP is operating correctly.

6.6 Update the DB2 License key

- a. Download the DB2 license key file from <u>http://www-internal.tivoli.com/secure/support/downloads/secureway/policy_dir/am3.9/db2lic.html</u> (internal) or <u>http://www.tivoli.com/secure/support/downloads/secureway/policy_dir/am3.9/db2lic.html</u> (external).
- b. Start a command prompt.
- c. Change to the DB2 bin directory this is $C: \SQLLIB\bin$ by default.
- d. Issue the command db2licm *directory*\db2udbpe.lic where *directory* indicates where the DB2 license key file has been placed.
- e. The output should look similar to the following:

```
C:\>cd\sqllib\bin
C:\SQLLIB\bin>db2licm C:\temp\db2udbpe.lic
DBI1402I License added successfully.
```

C:\SQLLIB\bin>

6.7 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. (The LDAP Client is a requisite of the PDRTE.)

- a. Insert the IBM Tivoli Access Manager Base for Windows Version 3.9 CD.
- b. 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:

IBM Tivoli Access Manager 3.9 – Cookbook



c. Select a language and click on '**OK**'. The InstallShield runs and the IBM Directory V3.2.2 Software License Agreement is displayed:

🚚 IBM SecureWay 3.2.2			
IBM SecureWay Directory V3	1.2.2	IAV) A
	Softwarz Lecasz Agreement Softwarz Lecasz Agreement Breast read the accompanying leanse agreement dreativily beforgara, wign strategie the termit Softwarz agreement. The softwarz agreement agreeme		BLE
		IBM	

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



e. 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]

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



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



h. Click on 'Next'. The 'Custom Installation' panel is displayed. Select only the Client component,

Version 1.1 – 30 September, 2002

and deselect all other components:



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



j. Click on 'Next'. The summary screen is displayed: Start copying files for IBM SecureWay Directory Client SDK.



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

Version 1.1 - 30 September, 2002



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



n. Click on 'Finish'.

6.8 Access Manager Servers installation (Windows)

- a. Insert the IBM Tivoli Access Manager Base for Windows Version 3.9 CD.
- b. Using 'My Computer' find the \windows\PolicyDirector\Disk Images\Disk1 directory on the CD, and double click on setup.exe. The 'Choose Setup Language' dialogue box is displayed:



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



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



e. Click on 'Yes'. The 'Select Packages' panel will be displayed. Select the Access Manager packages you require (at a minimum the Access Manager Runtime Environment and Access Manager Policy Server, we chose all the packages here for our install):



f. Click on 'Next'. The Access Manager Runtime Setup panel is displayed:

nose Destination Location		6
Select folder where Setup will install files.		
Setup will install Access Manager Runtime in t	he following folder.	
To install to this folder, click Next. To install to another folder.	a different folder, click Browse and	d select
- Destination Folder		
- Destination Folder C:\Program Files\Tivoli\Policy Director		Blowse
- Destination Folder C:\Program Files\Tivoli\Policy Director IShireId		Biowse

g. Click on 'Next'. The Access Manager Runtime Setup summary screen is displayed:



h. Review the settings and click on 'Next'. The files are copied across and the Access Manager 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'): IBM Tivoli Access Manager 3.9 – Cookbook



i. Click on 'OK'.

6.9 Install Access Manager Runtime Environment (Windows)

This sequence of steps should be followed on a box requiring **connectivity** with any of the Access Manager servers, such as the C Language Authorization API, the pdadmin API or the pdadmin command line interface.

This should not be carried out on boxes are running the Access Manager servers as they will already have the Runtime Environment installed.

- a. Insert the IBM Tivoli Access Manager Base for Windows Version 3.9 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:

IBM Tivoli Access Manager 3.9 - Cookbook



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

InstallShield Wizard			×
Select Packages			
Choose IBM Tivoli Access Manager for e-busine	ess Packages		
Access Manager Runtime Environment Access Manager Policy Server Access Manager Authorization Server Access Manager Application Developer Kit Access Manager Java Runtime Environmen	t		
InstallShield		<u>S</u> elect All	<u>Clear All</u>
	< <u>B</u> ack	<u>N</u> ext >	Cancel

f. Click on 'Next'; the Access Manager Runtime Setup panel is displayed:



g. Click on 'Next'; the Access Manager Runtime Setup summary screen is displayed:



h. Review the settings and click on '**Next**'; the files are copied across and the Access Manager 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.

6.10 Install WebSEAL (Windows)

- a. Insert the IBM Tivoli Access Manager Web Security for Windows Version 3.9 CD.
- b. Using Windows Explorer find the **\Windows\PolicyDirector\Disk Images\Disk 1** directory on the CD and double click on **setup.exe**. The 'Choose Setup Language' panel is displayed:



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

InstallShield Wizard		×
	Welcome to Access Manager for e-business.	
	The InstallShield® Wizard will install Access Manager for e-business on your computer. To continue, click Next.	
	Karack Cancel	

d. Click on 'Next'; the 'License Agreement' is displayed.



e. Click on 'Yes'; the 'Select Packages' panel is displayed. Select the components you want:



f. Click 'Next'. The 'Choose Destination Location' panel is shown:

is the following folder	
in the following folder	
in the following folder.	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
a different folder, click l	Browse and select
	B <u>r</u> owse
	(24) (1) (
) a different folder, click (

g. Click **'Next'**. The 'Select Components' panel is shown for the WebSEAL components. Select the components you require.


h. Click 'Next'. The files are copied across and the InstallShield Wizard Complete panel is displayed:

	InstallShield Wizard Complete Setup has finished installing Access Manager WebSEAL on your computer.
Click	< Back Finish Carcel
Informat	tion 🔀
•	All Access Manager for e-business components have been installed. Installation completed successfully. Click OK to exit.

j. Click **'OK'**. At this point the computer can be re-booted by issuing Start -> Shut Down -> 'Restart the computer'.

WebSEAL InstallShield Installation Failures

We have seen some situations where the InstallShield install has failed (it just died quietly) after displaying the 'Choose Destination Location' panel but before displaying the 'Select Components' panel. We tried the usual things to fix the problem (re-boot, clear out %TEMP% etc) without success.

The workaround we found was, instead of installing from \windows\PolicyDirector\Disk Images\Disk1\setup.exe, to install using \windows\PolicyDirector\Disk Images\Disk1\WebSEAL\Disk Images\Disk 1\setup.exe on the CD. This fixed the problem.

6.11 Access Manager Configuration (Windows)

This section describes how to configure the Access Manager components we installed earlier.

- a. Ensure that the user registry you are using has started in our case the IBM SecureWay Directory. (You can do this by issuing the command ldapsearch -h ldap_server_hostname -D cn=root -w ldap_password -b "" -s base objectclass=*.)
- b. Use Start → Programs → Access Manager for e-business → Configuration. The 'Access Manager for e-business Configuration' panel appears.
- c. The servers need to be configured in the following order: Access Manager Runtime, then Access Manager Policy Server; then either Access Manager Authorization Server and/or Access Manager WebSEAL as required.
- d. Highlight the 'Access Manager Runtime' in the installed packages column:

elect a package in the list then click Config	ure or Unconfigure.	r
		Close
nstalled Packages	Configured	Refresh
ccess Manager Runtime ccess Manager Policy Server	No No	View log
ccess Manager WebsEAL ccess Manager Authorization Server	No	
		Configure
		Unconfigure

e. Click on 'Configure'. You are prompted to select your User Registry. We selected 'LDAP'



f. Click '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.pic.uk.ibm.com, 389, ou=emea,o=ibm,c=gb.

Version 1.1 – 30 September, 2002

LDAP Host Name
secure2.pic.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 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?		
C Yes C No		
SSL Port Number		
636		
SSL client key file		
SSL client certificate label (if required)		
l SSL client key file password		
< Back Next > Cancel		

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

Access Manager Policy Server Host: secure2 User Registry Selection: Idap LDAP Host Name: secure2.pic.uk.ibm.com LDAP Port Number: 389 LDAP DN for GSO Database: o=ibm.c=gb Enable SSL Communication with the LDAP Server: No Kancel	🏠 Access Manager for e-busin	ess Configuration Review		×
Access Manager Policy Server Host: secure2 User Registry Selection: Idap LDAP Host Name: secure2.pic.uk.ibm.com LDAP Port Number: 389 LDAP DN for GSO Database: o=ibm,c=gb Enable SSL Communication with the LDAP Server: No				
secure2 User Registry Selection: Idap LDAP Host Name: secure2.pic.uk.lbm.com LDAP Port Number: 389 LDAP DN for GSO Database: o=ibm.c=gb Enable SSL Communication with the LDAP Server: No Enable SSL Communication with the LDAP Server: No	Access Manager Policy	Server Host:		
Vser Registry Selection: Idap LDAP Host Name: secure2.pic.uk.ibm.com LDAP Port Number: 389 LDAP DN for GSO Database: o=ibm.c=gb Enable SSL Communication with the LDAP Server: No Kommunication with the LDAP Server: No	secure2			
Idap LDAP Host Name: secure2.pic.uk.ibm.com LDAP Port Number: 389 LDAP DN for GSO Database: o=ibm,c=gb Enable SSL Communication with the LDAP Server: No	User Registry Selection:			
LDAP Host Name: secure2.pic.uk.ibm.com LDAP Port Number: 389 LDAP DN for GSO Database: o=ibm,c=gb Enable SSL Communication with the LDAP Server: No Kommunication with the LDAP Server: No	Idap			
secure2.pic.uk.ibm.com LDAP Port Number: 389 LDAP DN for GSO Database: o=ibm,c=gb Enable SSL Communication with the LDAP Server: No Kontection State S	LDAP Host Name:			
A Back Finish Cancel	secure2.pic.uk.ibm.co	n		
ABY LDAP DN for GSO Database: o=ibm,c=gb Enable SSL Communication with the LDAP Server: No 4 Back Finish Cancel	LDAP Port Number:			
c=ibm, c=gb Enable SSL Communication with the LDAP Server: No < Back	J09			
Cancel	o=ibm c=ab	lase.		
< Back Finish Cancel	Enable SSI Communic	tion with the LDAP Server:	No	
< Back Finish Cancel				
< Back Finish Cancel				
< Back Finish Cancel				
< Back Finish Cancel				
< Back Finish Cancel				
< Back Finish Cancel				
< Back Finish Cancel				
< Back Finish Cancel				
< Back Finish Cancel				
< Back Finish Cancel				
< Back Finish Cancel				
< Back Finish Cancel				
< Back Finish Cancel				
< Back Finish Cancel				
< Back Finish Cancel				
< Back Finish Cancel				
Karter Ka Karter Karter Kar	1	2		
	< Back	Finish	Cancel	

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

	- // 1929 W D	Herresh
nstalled Packages ccess Manager Runtime ccess Manager Policy Server ccess Manager WebSEAL ccess Manager Authorization Server	Uonhigured Yes No No No	View log
		Configure
		Unconfigure
		F

j. Next highlight 'Access Manager Policy Server' 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 Login		×
LDAP Administrator	Name	
cn=root		
LDAP Administrator	Password	

OK	Cancel	

k. Click 'OK'. The 'Access Manager for e-business Administrator Definition' panel is displayed.

The Access Manager for e-business Administrator Name is fixed as **sec_master**, specify the password (we used Secure99):

ana	fy the user name and password for the Access ger for e-business Administrator.
	Name
	sec_master
	Password

	Password confirmation

I. Click on **'OK'**. The 'Access Manager Policy Server SSL parameters' panel is displayed. This screen configures the ports that the Policy Server will use for accepting SSL connections from the other AM servers, the pdadmin command line and the Admin Console.

Specify the SSL connection parameters for the Policy Server.	Access Manager
SSL listening port number	7135
SSL Certificate lifetime	365
SSL connection timeout	7200
Enable root CA Certificate download	

- m. (If desired you can also select 'Enable root CA Certificate download'. This simplifies the distribution of the Root CA Certificate to subsequent Access Manager machines, but may introduce security exposures if the network can be compromised during the configuration step. The certificate is used to support SSL communications between the Access Manager components and must be present on all PD servers configured into the secure domain.)
- n. Accept these values and click on 'OK'. A message 'Configuring Access Manager Policy Server' is displayed. Then an 'Information' panel is displayed:



- o. Click on 'OK' to continue.
- p. You are returned to the 'Access Manager for e-business Configuration' panel once again. Select the next component you want to configure, in our case WebSEAL. Highlight 'Access Manager WebSEAL' and click on 'Configure'.
- q. The 'HTTP properties' panel is displayed:

TP properties		
✓ Allow (uns	ecure) TCP HTTP acc	ress
80	Port to use for un	secure HTTP requests
Allow HTTI	PS access Port to use for H1	TTPS requests
443		
	ок	Cancel

r. Accept the values and click on **'OK'**. The 'Access Manager for e-business Administrator Password' panel is displayed; enter the Access Manager for e-business Administrator password (in our case used Secure99):

ess Manager fo	or e-busines	s Administrator Password	
Specify the p e-business #	password f Administrat	or the Access Manag tor (sec_master).	er for
Password			
<u>]</u>			
ОК		Cancel	
	Specify the pe-business of Password	Specify the password f e-business Administrat Password *******	Specify the password for the Access Manage e-business Administrator (sec_master). Password ******* OK Cancel

- s. Click on 'OK'. WebSEAL is then configured.
- t. The 'Access Manager for e-business Configuration' panel is displayed once again. Highlight 'Access Manager Authorization Server' 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 Login	
LDAP Administrato	r Name
cn=root	
LDAP Administrato	r Password

	1

u. Click on **'OK'**. The 'Access Manager for e-business Administrator Password' panel is displayed; enter the Access Manager for e-business Administrator password:

👘 A	ccess Manager for e-busine	ss Administrator Password	×
	Specify the password e-business Administra	for the Access Manager t ator (sec_master).	for
	Password		
	ОК	Cancel	

- v. Click on 'OK'. The Access Manager Authorization Server is then configured.
- w. You are then returned to the 'Access Manager Configuration' panel and if you have followed all the steps you should see that all the installed packages are now configured:

	Lonridured	
ccess Manager Runtime ccess Manager Policy Server ccess Manager WebSEAL ccess Manager Authorization Server	Yes Yes Yes Yes	View log
		Configure
		Unconfigure
		•

- x. This completes the Access Manager configuration. Click on 'Close' to close the panel. You may want to check that the Access Manager services you have installed are started in Windows' Services before doing any testing.
- y. You can now check that Access Manager is working by following the steps described in Section 22 Initial Access Manager Validation on Page 170 below.

6.12 Access Manager RTE + WebSEAL Configuration (Windows)

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

- a. Unless you selected "Enable root CA Certificate download" when configuring the AM Policy Server, copy the file containing the AM CA Certificate file from the AM Policy Server to the WebSEAL machine (C:\Program Files\Tivoli\Policy Director\keytab\pdcacert.b64) by default.
- b. Use Start → Programs → Access Manager → Configuration. The 'Access Manager Configuration' panel appears.
- c. Highlight the 'Access Manager Runtime' in the installed packages column:

stalled Packages	Configured	Refresh
ccess Manager Runtime ccess Manager WebSEAL	No No	View log
		Configure
		Unconfigure

d. Click on 'Configure'. The Access Manager Policy Server Host dialogue box will be displayed. Specify that AM Policy Server is installed on another machine and specify the Host Name of the box running the AM Policy Server:

Access Manager Policy Server Host		×
Specify the location of the Access Manage	er Policy Server	
© Access Manager Policy Server will be	installed on this machine	
Access Manager Policy Server is instant	alled on another machine	
Other host information		
Host Name	secure2.pic.uk.ibm.com	
Listening Port	7135	
Next >	Cancel	

e. Click on 'Next'. You are asked about which user registry you are using:

×
1

f. Select the registry you are using and click '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).

🙀 LDAP	Server 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 > Cano	el
		0
7		

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?	
∩ Yes ເ⊂ No	
SSL Port Number	
636	
SSL client key file	
SSL client certificate label (if required)	
SSL client key file password	

h. Click on 'Next'. You are shown a 'Access Manager Configuration Review' panel:

Access Manager for e-business	Configuration Review		
Access Manager Policy Ser	ver Host:		
Listening Port:			
7135 Name of the file containing C:\Program Files\Tivoli\P	the Policy Server's sig olicy Director\\kevtab\p	ned certificate: dcacert download.b64	
User Registry Selection:			
LDAP Host Name:			
secure2.pic.uk.ibm.com			
389			
LDAP DN for GSO Databas	se:		
Enable SSL Communication	on with the LDAP Server	r: No	
< Back	Finish	Cancel	
	1		

i. After reviewing the values click '**Finish**'. You will see a message 'Configuring Access Manager Runtime'. After a successful configuration, Access Manager Runtime will be marked as configured:

stalled Packages Cor cess Manager Runtime Yes	figured	Hellesh
cess Manager Runtime Yes		
cess Manager WebSEAL No		View log
		Configure
		Unconfigure

- j. You are returned to the 'Access Manager Configuration' panel. Highlight 'Access Manager WebSEAL' and click on 'Configure'.
- k. The 'HTTP properties' panel is displayed:

	, 313
AA3 Port to use for HTTPS requests	
443	

I. Accept the values and click on **'OK'**. The 'Access Manager Administrator Password' panel is displayed; enter the Access Manager Administrator password:



- m. Click on 'OK'; Access Manager WebSEAL is then configured.
- n. You are then returned to the 'Access Manager Configuration' panel. This completes the Access Manager configuration:



- o. Click on 'Close' to close the panel.
- p. You can now check that Access Manager is working by following the steps described in Section
 22 Initial Access Manager Validation on Page 170 below.

6.13 Web Portal Manager Installation & Configuration (Windows)

This section describes how to install the Web Portal Manager (WPM), the Access Manager webbased interface.

- a. Ensure that GSKit 5.0.4.67 or higher has been installed, and IBM HTTP Server with SSL support. (The 'Additional Modules' component in the HTTP Server installation provides the SSL libraries.) If this is a new machine ensure that the AM Runtime and requisites are installed (such as the LDAP client).
- b. Ensure that you have the necessary prerequisites for WebSphere 4.0 Single Server 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 IBM Tivoli Access Manager Web Portal Manager for Windows Version 3.9 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:

Choose Se	tup Language	×
7	Select the language for th the choices below.	is installation from
	English (United States)	
	ОК	Cancel

f. Select a language and click on '**OK**', The IBM WebSphere Application Server Advanced Single Server Edition v4.0 welcome screen is displayed:

WebSphere Application Server 4.0	_ 🗆 ×
IBM WebSphere Application Server	
Advanced Single Somer Edition of 0	
Aavancea single server Laulon v4.0	
WebSphere Application Server 4.0	
ATTENTION. Before you continue, you must that down all Webservers you plan to run with WebSphere	
It is strongly recommended that you exit all Windows programs before summing this Setup program.	
Click Cancel to gut Setup and then close any program you have numing. Click Next to continue with the Setup program.	
WARNING: This program is protected by copyright law and international treaters.	
Unastherized reproduction or distribution of this program or any portion of it, may result in server civil and ciminal penalties, and will be proceeding to the maximum earth possible under law.	
<u>Next></u> Cancel	

g. Click on '**Next**'; the Installation Options dialogue box is displayed. Select 'Custom Installation':

Select the installation option you prefer and then click next.	
C Typical Installation	
Everything you need to support applications intended to run on server single-node configurations; includes IBM HTTP Server, and JDK 1.3.	rs with D.
Custom Installation	
Choose to install specific components of the total install package; spe other supported webservers.	cify the use of
< <u>B</u> ack <u>N</u> ext>	Cancel

h. Click on 'Next'; deselect the 'IBM HTTP Server' which we have already installed:



i. Click 'Next'; you are asked about which webserver you have installed. Select 'IBM HTTP Server':



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



Version 1.1 – 30 September, 2002

k. Click on 'Next'; the 'Select Program Folder dialogue box is displayed:



I. Click on 'Next'; a summary screen is displayed: Install Options Selected



m. Review the settings and click on **'Next'**; the files are copied across, then the **'Setup Complete'** panel is displayed and you are given the option of viewing the README file:



n. Click on 'Finish'; the 'Restarting Windows' dialogue box will be displayed. Select 'Yes, I want

Version 1.1 – 30 September, 2002



- o. Click on 'OK'.
- p. When the system reboots close the 'WebSphere Application Server First Steps' window, and use Windows Services to stop the IBM HTTP Server and IBM HTTP Administration services. Ensure the WebSphere Application Server is not active - you can do this by issuing the following command:

C:\WebSphere\AppServer\bin\stopserver

- q. Still using the IBM Tivoli Access Manager Web Portal Manager for Windows Version 3.9
 CD: copy all the files from the \windows\websphere\ptf402 directory on the CD to a temporary directory on the hard drive.
- r. It is probably worth reviewing the contents of was40_aes_ptf_2.Readme in this directory.
- s. Run install.bat from the temporary directory:

```
C:\ptf402>install.bat
   WebSphere Application Server 4.0, Advanced Edition, Single Server PTF 2
Please shut down the Application Server and any Webservers that might be
running. If not the PTF may not be installed properly.
Please press return to continue.
Enter the directory where the IBM WebSphere Application Server is installed:
c:\WebSphere\AppServer
WASHOME c:\WebSphere\AppServer
JDKHOME c:\WebSphere\AppServer\java
        1 file(s) copied.
"Installing the WebSphere Application Server Advanced Edition Single Server Version 4.0 PTF 2"
2002/05/17 10:48:46 Extractor version: 1.29
2002/05/17 10:48:46
2002/05/17 10:48:46 Input Jar File
                                       : C:/ptf402/was40_aes_ptf_2.jar src=Default
2002/05/17 10:48:46 Start of extraction for C:/ptf402/was40 aes ptf 2.jar
2002/05/17 10:48:46 No target message provided, default enabled.
2002/05/17 10:48:46 Target Directory
                                       : c:\WebSphere\AppServer
2002/05/17 10:48:46 Testing Temporary Directory : C:\TEMP
2002/05/17 10:48:46 Full Temporary Directory : C:\TEMP
2002/05/17 10:48:46 The temporary directory is usable.
2002/05/17 10:48:46 Backup Jar File
                                      : c:\WebSphere\AppServer\was40_aes_ptf_2_backup.jar
2002/05/17 10:48:46 This update applies to the following components:
2002/05/17 10:48:46
                       Client
2002/05/17 10:48:46
                      Server
                      Samples
2002/05/17 10:48:46
2002/05/17 10:48:46
                       Console
2002/05/17 10:48:46
                       Common
2002/05/17 10:48:46
                       Deploytools
                      Plugins
2002/05/17 10:48:46
2002/05/17 10:48:46
                      Samples_Common
2002/05/17 10:48:46
                       Server_Common
2002/05/17 10:48:46
                      Tools_Common
                       J2EEClient
2002/05/17 10:48:46
```

```
2002/05/17 10:48:46
                         JTCClient
2002/05/17 10:48:46
2002/05/17 10:48:46 The following components were detected installed:
2002/05/17 10:48:46
                          Console
2002/05/17 10:48:46
                          Deploytools
2002/05/17 10:48:46
                          J2EEClient
2002/05/17 10:48:46
                          Tools Common
2002/05/17 10:48:46
                         Common
2002/05/17 10:48:46
                          Client
2002/05/17 10:48:46
                        Samples
2002/05/17 10:48:46
                          Server Common
2002/05/17 10:48:46
                          JTCClient
2002/05/17 10:48:46
                          Server
2002/05/17 10:48:46
                          Samples_Common
2002/05/17 10:48:46
                          Plugins
2002/05/17 10:48:46
2002/05/17 10:48:46 Product file type: XML
2002/05/17 10:48:46 Product file [ c:\WebSphere\AppServer/properties/com/ibm/websphere/product.xml
2002/05/17 10:48:47 No prior history events noted.
2002/05/17 10:48:48 Determining files to back up
2002/05/17 10:48:48 scanning
                                  1 of 13273
                                                 0% complete
2002/05/17 10:48:51 scanning 9284 of 13273
                                                69% complete
2002/05/17 10:48:53 scanning 13273 of 13273 100% complete
2002/05/17 10:48:53
                                                42% complete
2002/05/17 10:48:55 Backing Up 466 of 1102
2002/05/17 10:48:59 Backing Up 561 of 1102
                                                50% complete
2002/05/17 10:49:03 Backing Up 583 of 1102
                                                52% complete
2002/05/17 10:49:08 Backing Up 633 of 1102
                                                57% complete
2002/05/17 10:49:12 Backing Up 717 of 1102
                                                65% complete
2002/05/17 10:49:16 Backing Up 922 of 1102
                                                83% complete
2002/05/17 10:49:21 Backing Up 1045 of 1102
                                                94% complete
2002/05/17 10:49:25 Backing Up 1059 of 1102
                                                96% complete
2002/05/17 10:49:29 Backing Up 1067 of 1102
                                                96% complete
2002/05/17 10:49:33 Backing Up 1082 of 1102
                                                98% complete
2002/05/17 10:49:37 Backing Up 1102 of 1102 100% complete
2002/05/17 10:49:37
2002/05/17 10:49:37 Applying entry
                                        1 of 13272
                                                       0% complete
2002/05/17 10:49:41 Applying entry 1131 of 13272
                                                       8% complete
2002/05/17 10:49:46 Applying entry 1999 of 13272
                                                      15% complete
2002/05/17 10:49:50 Applying entry 3206 of 13272
2002/05/17 10:49:55 Applying entry 4621 of 13272
                                                      24% complete
                                                      34% complete
2002/05/17 10:50:00 Applying entry 5883 of 13272
                                                      44% complete
2002/05/17 10:50:04 Applying entry
                                     7228 of 13272
                                                      54% complete
2002/05/17 10:50:08 Applying entry 8802 of 13272
                                                      66% complete
2002/05/17 10:50:12 Applying entry 8960 of 13272
                                                      67% complete
2002/05/17 10:50:17 Applying entry 9278 of 13272
                                                      69% complete
2002/05/17 10:50:22 Applying entry 10078 of 13272
                                                      75% complete
2002/05/17 10:50:27 Applying entry 10190 of 13272
2002/05/17 10:50:34 Applying entry 10521 of 13272
                                                      76% complete
                                                      79% complete
2002/05/17 10:50:38 Applying entry 10699 of 13272
                                                      80% complete
2002/05/17 10:50:43 Applying entry 10860 of 13272
                                                      81% complete
2002/05/17 10:50:47 Applying entry 11074 of 13272
                                                      83% complete
2002/05/17 10:50:52 Applying entry 11465 of 13272 2002/05/17 10:50:56 Applying entry 12524 of 13272
                                                      86% complete
                                                      94% complete
2002/05/17 10:50:57 Applying entry 13272 of 13272 100% complete
2002/05/17 10:50:57 No Re-Sequencing of jar files was noted.
2002/05/17 10:50:57 Processing virtual script CopyEjbDeploy
2002/05/17 10:50:57 Updating c:\WebSphere\AppServer/properties/com/ibm/websphere/product.xml
2002/05/17 10:50:57 Input Jar File
                                      : C:/ptf402/was40_aes_ptf_2.jar
2002/05/17 10:50:57 Target Directory : c:\WebSphere\AppServer
2002/05/17 10:50:57 Backup Jar File : c:\WebSphere\AppServer\was40_aes_ptf_2_backup.jar 2002/05/17 10:50:57 Warnings Issued : 0
2002/05/17 10:50:57 Log File
                                       : c:\WebSphere\AppServer\logs\was40 aes ptf 2.log
2002/05/17 10:50:57
2002/05/17 10:50:57 End of extraction for C:/ptf402/was40 aes ptf 2.jar with no errors.
2002/05/17 10:50:57
2002/05/17 10:50:57 Please view the log for details.
        1 file(s) copied.
        1 file(s) copied.
Upgrading IBM JDK
```

191 File(s) copied 2002/05/17 10:51:18 Extractor version: 1.29 2002/05/17 10:51:18 2002/05/17 10:51:18 Input Jar File : C:/ptf402/jdk_ptf_2.jar src=Default 2002/05/17 10:51:18 Start of extraction for C:/ptf402/jdk_ptf_2.jar 2002/05/17 10:51:18 No target message provided, default enabled. : c:\WebSphere\AppServer\java_ptf_2 2002/05/17 10:51:18 Target Directory 2002/05/17 10:51:18 Testing Temporary Directory : C:\TEMP 2002/05/17 10:51:18 Full Temporary Directory : C:\TEMP 2002/05/17 10:51:18 The temporary directory is usable. 2002/05/17 10:51:18 Backup Jar File : c:\WebSphere\AppServer\jdk_ptf_2_backup.jar 2002/05/17 10:51:18 This update applies to the following components: 2002/05/17 10:51:18 JDK 2002/05/17 10:51:18 JRE 2002/05/17 10:51:18 2002/05/17 10:51:18 The following components were detected installed: JRE 2002/05/17 10:51:18 2002/05/17 10:51:18 JDK 2002/05/17 10:51:18 2002/05/17 10:51:18 No set product file. 2002/05/17 10:51:18 Bypassing duplicate application checking by request. 2002/05/17 10:51:18 Determining files to back up 2002/05/17 10:51:18 scanning 1 of 213 0% complete 2002/05/1710:51:21scanning138of21364%complete2002/05/1710:51:25scanning181of21384%complete 2002/05/17 10:51:25 scanning 213 of 213 100% complete 2002/05/17 10:51:25 2002/05/17 10:51:26 Backing Up 1 of 187 0% complete 2002/05/17 10:51:30 Backing Up 70 of 187 37% complete 2002/05/17 10:51:34 Backing Up 129 of 187 68% complete 2002/05/17 10:51:41 Backing Up 180 of 187 96% complete 2002/05/17 10:51:44 Backing Up 187 of 187 100% complete 2002/05/17 10:51:44 2002/05/17 10:51:44 Applying entry 1 of 212 2002/05/17 10:51:48 Applying entry 89 of 212 1 of 212 0% complete 41% complete 2002/05/17 10:51:53 Applying entry 188 of 212 88% complete 2002/05/17 10:51:53 Applying entry 212 of 212 100% complete 2002/05/17 10:51:53 No Re-Sequencing of jar files was noted. 2002/05/17 10:51:53 Input Jar File : C:/ptf402/jdk_ptf_2.jar 2002/05/17 10:51:53 Target Directory : c:\WebSphere\AppServer\java ptf 2 2002/05/17 10:51:53 Backup Jar File : c:\WebSphere\AppServer\jdk ptf 2 backup.jar 2002/05/17 10:51:53 Warnings Issued : 0 2002/05/17 10:51:53 Log File : c:\WebSphere\AppServer\logs\jdk_ptf_2.log 2002/05/17 10:51:53 2002/05/17 10:51:53 End of extraction for C:/ptf402/jdk ptf 2.jar with no errors. 2002/05/17 10:51:53 2002/05/17 10:51:53 Please view the log for details. Press any key to continue . . . 191 File(s) copied The system cannot find the path specified. 0 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: (Yes/No) Yes Enter the directory where the IBM HTTP Server is installed: c:\Program Files\IBM HTTP Server Upgrading IHS 2002/05/17 10:53:45 Extractor version: 1.29 2002/05/17 10:53:45 2002/05/17 10:53:45 Input Jar File : C:/ptf402/ihs_ptf_2.jar src=Default 2002/05/17 10:53:45 Start of extraction for C:/ptf402/ihs ptf 2.jar 2002/05/17 10:53:45 No target message provided, default enabled. 2002/05/17 10:53:45 Target Directory : c:\Program Files\IBM HTTP Server 2002/05/17 10:53:45 Testing Temporary Directory : C:\TEMP 2002/05/17 10:53:45 Full Temporary Directory : C:\TEMP 2002/05/17 10:53:45 The temporary directory is usable. 2002/05/17 10:53:45 Backup Jar File : c:\WebSphere\AppServer\ihs_ptf_2_backup.jar 2002/05/17 10:53:45 Component checking deactiviated, affected components entry is null. 2002/05/17 10:53:45 No set product file. 2002/05/17 10:53:45 Bypassing duplicate application checking by request.

```
2002/05/17 10:53:45 Determining files to back up
2002/05/17 10:53:45 scanning 1 of 55 1% complete
2002/05/17 10:53:48 scanning 55 of 55 100% complete
2002/05/17 10:53:48
2002/05/17 10:53:48 Backing Up 17 of 29 58% complete
2002/05/17 10:53:49 Backing Up 29 of 29 100% complete
2002/05/17 10:53:49
2002/05/17 10:53:49 Applying entry 1 of 54 1% complete
2002/05/17 10:53:50 Applying entry 54 of 54 100% complete
2002/05/17 10:53:50 No Re-Sequencing of jar files was noted.
2002/05/17 10:53:50 Input Jar File : C:/ptf402/ihs_ptf_2.jar
2002/05/17 10:53:50 Target Directory : c:\Program Files\IBM HTTP Server
2002/05/17 10:53:50 Backup Jar File : c:\WebSphere\AppServer\ihs_ptf_2_backup.jar
2002/05/17 10:53:50 Warnings Issued : 0
2002/05/17 10:53:50 Log File
                                         : c:\WebSphere\AppServer\logs\ihs ptf 2.log
2002/05/17 10:53:50
2002/05/17 10:53:50 End of extraction for C:/ptf402/ihs_ptf_2.jar with no errors.
2002/05/17 10:53:50
2002/05/17 10:53:50 Please view the log for details.
IBM WebSphere Application Server V4.0.2 AEs Fixpack install complete
File not found - \CONF\HTTPD.CONF
The system cannot find the path specified.
```

- C:\ptf402>
- t. You will have a dialogue similar to above. Once this is complete re-boot the computer by issuing Start -> Shut Down -> 'Restart the computer'.
- u. Once the system has restarted and you have logged in again you need to start WebSphere: use Start → Programs → IBM WebSphere → Application Server V4.0 AES → Start Application Server to start WebSphere. You will see a command window open similar to the following:

```
WebSphere Application Server, Advanced Single Server Edition V4.0
Application Server Launcher
Copyright (C) IBM Corporation, 2001
The configuration file was defaulted to:
    C:\WebSphere\AppServer\config\server-cfg.xml
Using the single available node or the localhost node.
Using the single available server.
Will pause after displaying results.
Initiating server launch.
Loaded domain "WebSphere Administrative Domain".
Selected node "harperv".
Selected server "Default Server".
WSPL0065I: Initiated server launch with process id 359.
Time mark: Monday, May 27, 2002 5:55:28 PM GMT+01:00
Waiting for the server to be initialized.
Time mark: Monday, May 27, 2002 5:55:37 PM GMT+01:00
Initialized server.
Waiting for applications to be started.
Time mark: Monday, May 27, 2002 5:56:25 PM GMT+01:00
Started applications.
WSPL00571: The server Default Server is open for e-business.
Please review the server log files for additional information.
Standard output: C:\WebSphere\AppServer/logs/default server stdout.log
Standard error: C:\WebSphere\AppServer/logs/default server stderr.log
Pausing; press the enter key to continue.
```

v. The phrase 'The server Default Server is open for e-business' indicates that the WebSphere Application Server is running. Press the enter key to continue and the window will close.

- w. Still using the **IBM Tivoli Access Manager Web Portal Manager for Windows Version 3.9** CD:
- x. Using 'My Computer' find the **\windows\Policy Director\Disk Images\Disk1** directory on the CD, and double click on **setup.exe**. The 'Choose Setup Language' dialogue box is displayed:



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



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



aa. Click on '**Yes**'. The 'Select Packages' panel will be displayed. Select 'Access Manager Web Portal Manager':



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



- cc. Click on '**OK**' to dismiss the dialogue.
- dd. Use Start → Programs → Access Manager for e-business → Configuration. The 'Access Manager Configuration' panel appears.
- ee. Highlight the 'Access Manager Web Portal Manager' entry in the installed packages column:

Configured	Refresh
Yes No	View log
	Configure
	Unconfigure
	Configured Yes No

- ff. Click on 'Configure'; the Web Portal Manager is then configured.
- gg. You are then returned to the 'Access Manager Configuration' panel:

nstalled Packages Loningured ccess Manager Runtime Yes Ccess Manager Web Portal Manager Yes Configure Unconfigure			Refresh
Configure Unconfigure	talled Packages cess Manager Runtime cess Manager Web Portal Manager	Lontigured Yes Yes	View log
Unconfigure			Configure
			Unconfigure
()			•

hh. Click on 'Close' to close the panel.

6.14 Changing Web Portal Manager port numbers (Windows)

The Web Portal Manager runs as a WebSphere application – a set of Java Server Pages, by default it will listen on ports 80 and 443. If you are running WPM on the same machine that you are using to run WebSEAL and want WebSEAL to own ports 80 and 443, IBM HTTP Server and WebSphere must be re-configured.

a. We earlier edited the HTTP configuration file, httpd.conf, so that IBM HTTP Server would listen on Port 81 for non-SSL traffic. However as a result of the WPM installation and configuration, additional lines are placed at the end of httpd.conf which disallow any non-SSL traffic. (This is a security measure to protect against sniffing administrator traffic.) The additional lines which were placed at the end of our configuration file following WPM installation and configuration were as follows:

```
### BEGIN PDWPM CONFIG ENTRY ###
Listen 443
LoadModule ibm_ssl_module modules/IBMModuleSSL128.dll
SSLEnable
Keyfile "C:\Program Files\Tivoli\Policy Director\\keytab\pdwpm.kdb"
SSLV2Timeout 100
SSLV3Timeout 1000
### END PDWPM CONFIG ENTRY ###
```

b. If you are running WebSEAL on the same machine that you are using to run WPM and want WebSEAL to own ports 80 and 443, IBM HTTP Server and WebSphere must be re-configured as follows:

(a) 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 had already changed this to Port 81 in an earlier step.

(b) Find the Listen line near the end of the file (added by the WPM configuration). Change the reference to 443 to a different port number - we used 4443:

```
### BEGIN PDWPM CONFIG ENTRY ###
Listen 4443
LoadModule ibm_ssl_module modules/IBMModuleSSL128.dll
SSLEnable
Keyfile "C:\Program Files\Tivoli\Policy Director\\keytab\pdwpm.kdb"
SSLV2Timeout 100
SSLV3Timeout 1000
### END PDWPM CONFIG ENTRY ###
```

c. If you want to enable non-SSL traffic (to port 81 in our case), edit httpd.conf, as follows:

```
### BEGIN PDWPM CONFIG ENTRY ###
Listen 4443
LoadModule ibm_ssl_module modules/IBMModuleSSL128.dll
<VirtualHost :4443>
SSLEnable
SSLClientAuth none
DocumentRoot "C:/Program Files/IBM HTTP Server/htdocs"
</VirtualHost>
SSLDisable
```

Version 1.1 – 30 September, 2002

```
Keyfile "C:\Program Files\Tivoli\Policy Director\\keytab\pdwpm.kdb"
SSLV2Timeout 100
SSLV3Timeout 1000
### END PDWPM CONFIG ENTRY ###
```

- d. Use Start -> Settings -> Control Panel -> Services (NT), or Start -> Programs -> Administrator Tools -> Services (2000), to stop and re-start IBM HTTP Server for the changes to take effect.
- 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 IBM HTTP Server splash screen but not the WPM in order for that to work WebSphere must be reconfigured with the new ports.
- f. If it is not already running start WebSphere Application Server by using Start → Programs → IBM WebSphere → Application Server V4.0 AES → Start Application Server.
- g. Use Start → Programs → IBM WebSphere → Application Server V4.0 AES → Administrator's Console (or point a web browser at http://hostname:9090/admin) to start the WebSphere Administrative Console. You will be presented with the WebSphere Application Server Administrative Login page. Enter a name to log in (but it doesn't matter what this name is):

<u>E</u> ile <u>E</u> dit ⊻iew <u>G</u> o <u>C</u>	ommunicator H	elp						
Back Forward	Reload Ho	🚹 🎿 me Search	Netscape	Ennt	Security	() Shop	Stop	N
🛯 🆋 Bookmarks 🙏	Location: http:	//localhost9090	Madmin/					💽 🏠 What's Related
WebSphere App)	lication Ser	ver						IBM. ¹
								Contraction of the
		Login						
		User	D:	Admin	istrator		1	
				Subm	it			
		The u not ne regist to con	ser id does r ed to be a u ry. It is only u figuration da	not requir serid of a sed to tra ta.	re a passwo i user in the ack user-sp	ord, and do local user lecific chan	es ges	A Constant
								Sec 5
								-
	Document: D	one						

h. Click on 'Submit'.

i. In the left-hand panel, click on the '+' sign to the left of Virtual Hosts and then click on the '+' sign to the left of default_host. Then click on 'Aliases'. The panel should look like this:



j. We need to add new aliases, for ports 81 and 4443. First, click on 'New'; a new panel will be displayed. Under 'Properties', add * in the 'Host Name' field and 81 in the 'Port' field:

server-cfa xml			-	1000	a	50 a. (20 a.	P
	Console Home	Comiguration	Preferences	Save	Exπ	Help	
Q WebSphere Administrative Domain - Nodes - Wirtual Hosts - 음 전fatult_host - 유 Aliases	Configuration for aliase as a servict, JSP, or HT default port 80 is used. <u>For more information</u> .	s. An alias is the DNS host nam ML page). For example, it is th =	e and port number used e "myhost:8080" portion o	by a client to forr of http://myhost.8/	n the URL request fo D80/servlet/snoop. W	a Web application res hen no port number is	ource (such specified, the
	E						
∓ Ba admin host	Properties						
· 문음 admin_host 마음 우양 Security 다 (한 Resources	Host Name: * *			The If the Di resour	° address, DNS host i NS host name, used ce (such as a serviet,	ame with domain nar by a client to request a JSP, or HTML page).	ne suffix, or jus Web applicati

k. Click on 'OK'. You are returned to the 'Aliases' page, showing the new entry:

WebSphere Application Serve	r				IBM.
server-cfg.xml	Console Home	Configuration Prefe	rences Save	Exit Help	8.8
WebSphere Administrative Domain Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Modes Mod	Configuration needs to Configuration needs to Play-in configuration n Aliases The list of one or more DN vFormore Information. New Delete	<u>. Is saind</u> <u>neadf to be regenerated</u> 15 allases by which the virtual host is kn	9 0 ;		
	Host Name		Port		
			9080	i i	
	E = *		9443		
			80		
	E 🖻 👱		443		
	D 5 *		81		

- I. Notice the two messages at the top of the right-hand panel. The first says "Configuration needs to be saved" and the second says "Plug-in configuration needs to be regenerated". These operations can be carried out once the second alias has been added.
- m. Click on 'New'; again, a new panel will be displayed. Under 'Properties', add * in the 'Host Name' field and 4443 in the 'Port' field:

Configuration fo as a servlet, JSP default port 80 i:	raliases. An alias is the DNS host name a , or HTML page). For example, it is the "n : used.	nd port number used by a client to form the URL request for a Web application resource (such nyhost 8080° portion of http://myhost.8080/sen/et/snoop, When no port number is specified, the
For more infor	nation	
Properties		
Host Name:	*	The IP address, DNS host name with domain name suffix, or just the DNS host name, used by a dilent to request a Web applicatio resource (such as a servict, JSP, or HTML page).
Port:	4443	A port value can be specified in conjunction with the host name to indicate the port for which the Web server has been configured to accord client request.

n. Click on 'OK'. You are returned to the 'Aliases' page, showing the new entry:

 <u>Configuration needs to be saved</u> <u>Plug-in configuration needs to be regenerated</u>. 					
The list of one or more DNS aliases by which the virtual host is known					
»For more information					
Host Name	Port				
□ 駒 <u>★</u>	9080				
🗖 🕮 <u>*</u> .	9443				
🗆 🖺 <u>*</u>	80				
□ 些 <u>*</u>	443				
	81				
	4443				

o. Click on 'Configuration needs to be saved'. A 'Save Configuration' panel is displayed:

Save Configuration

You made changes to the configuration file: C:WebSphere\AppServer\config\server-ofg.xml . You can either:



- p. Click on 'OK'. You are returned to the WebSphere Application Server Welcome screen.
- q. You now need to re-generate the Plug-in configuration. In practice the only way that we were able to do this was to point the web browser at



- r. Click on 'Generate'. After the operation had completed the browser displayed a message: 'This document contained no data'. However examination of
 - C:\WebSphere\AppServer\config\config/plugin-cfg.xml indicated that this was not a problem and the file had been updated with the new port numbers:

```
<VirtualHostGroup Name="default host">
        <VirtualHost Name="*:9080"/>
        <VirtualHost Name="*:9443"/>
        <VirtualHost Name="*:80"/>
        <VirtualHost Name="*:443"/>
        <VirtualHost Name="*:81"/>
        <VirtualHost Name="*:4443"/>
</VirtualHostGroup>
```

s. Stop and start the application server. We did this by using the command prompt:

C:\>stopserver WebSphere Application Server, Advanced Single Server Edition V4.0 WebSphere Application Server, Advanced Developer Edition V4.0 WebSphere Application Server, Advanced Edition V4.0 Runtime Utility Program Copyright (C) IBM Corporation, 1997-2001 WSRU0025I: Loading configuration from file. WSRU0028I: Using the specified configuration file: C:\WebSphere\AppServer\config\server-cfg.xml WSRU0029I: The diagnostic host name read as localhost. WSRU0030I: The diagnostic port was read as 7000. Stopping server. The server was successfully stopped.

```
C:\>startserver
WebSphere Application Server, Advanced Single Server Edition V4.0
Application Server Launcher
Copyright (C) IBM Corporation, 2001
The configuration file was defaulted to:
    C:\WebSphere\AppServer\config\server-cfg.xml
Using the single available node or the localhost node.
Using the single available server.
Initiating server launch.
Loaded domain "WebSphere Administrative Domain".
Selected node "secure5".
Selected server "Default Server".
WSPL0065I: Initiated server launch with process id 315.
Time mark: Tuesday, May 28, 2002 11:01:35 AM GMT+01:00
Waiting for the server to be initialized.
Time mark: Tuesday, May 28, 2002 11:01:39 AM GMT+01:00
Initialized server.
Waiting for applications to be started.
Time mark: Tuesday, May 28, 2002 11:02:13 AM GMT+01:00
Started applications.
WSPL0057I: The server Default Server is open for e-business.
Please review the server log files for additional information.
Standard output: C:\WebSphere\AppServer/logs/default server stdout.log
Standard error: C:\WebSphere\AppServer/logs/default server stderr.log
C:\>
```

Note the highlighted line: WSPL0057I: The server Default Server is open for ebusiness – this indicates that the application server has started correctly.

Notes on WebSphere Application Server and DB2 Versions

Access Manager is supplied with WebSphere Application Server Advanced Single Server Edition (AEs). Web Portal Manager is supported only with WAS Advanced Single Server Edition, not Advanced Edition (AE). If you try and install WPM with WAS AE the WPM Configuration will fail: you need to use the WAS Console Application Install wizard.

WAS AE Requires DB2 *Enterprise* Edition, whereas DB2 *Personal* Edition is supplied with the version of IBM SecureWay Directory which is shipped with Access Manager.

There is more information on installing WPM with WAS AE on Windows in Section 34 - Installing and Configuring Web Portal Manager on page 255 below.

6.15 Verify Web Portal Manager operation

- a. Ensure that the IBM HTTP Server was restarted after making any updates to httpd.conf.
- b. Start the IBM SecureWay Directory Server.
- c. Start the Access Manager Servers.
- d. Point a web browser at http://hostname:9090/admin. You will again be presented with the WebSphere Application Server Administrative Login page.
- e. Enter a userid and click on 'Submit'. You will be presented with the WebSphere Application Server Administrative Console.
- f. Use Start → Programs → IBM WebSphere → Application Server V4.0 AES → Administrator's Console (or point a web browser at http://hostname:9090/admin) to start the WebSphere Administrative Console. You will be presented with the WebSphere Application Server Administrative Login page. Enter a name to log in (but it doesn't matter what this name is):



- g. Click on 'Submit'. You may be presented with 'Alert: The changes that were made before your session timed out have been saved to a temporary configuration file'. If so, click on 'OK'.
- h. You will be presented with the WebSphere Application Server Administrative Console:



i. You can use this console to verify that WPM is running: in the left-hand panel, click on the '+' sign to the left of Nodes and then click on the '+' sign to the left of your node (in our case secure5):

WebSphere Administrative Domain
 Nodes
 Nodes
 Secure5
 Enterprise Applications

j. Click on 'Enterprise Applications':

```
* Enterprise Applications
```

The J2EE applications (EAR files) installed on the application server

♦For more information...

Start Stop Restart Install Uninstall I	Export DDL
🔲 Name	Archive URL
sampleApp	\${APP_INSTALL_ROOT}/sampleApp.ear
Server Administration Application	\${APP_INSTALL_ROOT}/admin.ear
🗆 🗗 WebSphere Application Server Samples	\${APP_INSTALL_ROOT}\Samples.ear
D petstore_	\${APP_INSTALL_ROOT}\petstore.ear
Policy Director Web Portal Manager	\${APP_INSTALL_ROOT}\pdwpm.ear

- k. The 5 indicates that the application is running.
- I. Point a web browser at https://hostname:port number/pdadmin
- (https://secure5.pic.uk.ibm.com:4443/pdadmin in our case).
- m. You will be presented with various 'Name Check' or other security alert windows accept these warnings. The Web Portal Manager sign-in screen will be displayed.
- n. Enter the Access Manager Administrator userid (sec_master) and password (Secure99 in our case).

	Urhat's F
Rekad Home Sauch Netrocope Print Security Shop Stop skmarks Location Intro-Cost Attractive Print Security Shop Stop with rest Location Print Security Shop Stop with rest Location Print Rekad Print Security Shop Internet Location New&Cool Image: Read Rest New&Cool Read Read Rest Internet Location New&Cool Image: Read Rest New&Cool Read Read Rest Internet Location New&Cool Read Read Rest New New Version 3.9 Image: Rest Image: Rest Image: Rest Image: Rest Internet Image: Rest Image: Rest Image: Rest Image: Rest Internet Image: Rest Image: Rest Image: Rest Image: Rest Internet Image: Rest Image: Rest Image: Rest Image: Rest Internet Image: Rest Image: Rest Image: Rest Image: Rest Internet <t< th=""><th>کی اور کار برای اور اور اور اور اور اور اور اور اور اور</th></t<>	کی اور کار برای اور
Atmarks & Location Inter://secureS.pic.uk.bm.com:4442/pdadmin/aut/thandieLogin.jpp Internet Lockup New&Cool ReaPlayer Throut. Access Manager for e-business Weston 3.9	Under P
Internet Lookup New&Cool ReaPRayer	
Tivel. Access Manager for e-business Weston 3.9	
IBM. Tivel. Access Manager for e-business. Version 3.9	
TYVOL. Access Manager for e-business. Version 3.9	
Tivel. Access Manager for e-business Verson 3.9	
Trvell. Access Manager for e-business. Version 3.9	
Version 3.9	
Licensed Materials - Pronetty of IBM Corp (c) Copyright by IBM Corp. and other(s) 1999, 2002	
All Rights Reserved. See product license for details.	
User ID: sec_master	
Password: Login	



p. From here you can use the Web Portal Manager to administer Access Manager.

General notes: Refer to the Publications Section on page 240 below for information about where to obtain information about **WebSphere Application Server**.

If you hit problems with IBM HTTP Server try looking at the contents of /usr/HTTPServer/logs, particularly /usr/HTTPServer/logs/error_log.

Part III - AIX Environment

Note: Quick installation is also supported using shell scripts for UNIX systems such as AIX and Solaris - these scripts make it easy to install Access Manager by automatically installing required software and prerequisites. The following sections describe the *native* installation processes for AIX.

7. AIX System Preparation and general AIX Notes

- An Access Manager 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. AIX 5.1.0 requires that bos.rte.libpthreads be at level 5.1.0.10 or greater. You can download these patches from the following support site:
 <u>http://www.ibm.com/partnerworld/pwhome.nsf/weblook/home.html</u>
 and clicking on Support & Downloads. (You can check which level is installed by issuing lslpp -1 |grep libpthreads at a command prompt.)
- 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 of Access Manager 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

Version 1.1 – 30 September, 2002

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 <code>MOUNT POINT</code> field, enter a new directory name where you want to mount the CD (in our case /cdrom) and press <code>Enter</code>

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 Access Manager 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 steps	es in filesystem usag	e following the in	stall and configure
Filesystem	512-blocks used	MB used	Inodes used
/	262,000	131	653
/usr	590,000	295	7,873
/var	65,500	33	76
/tmp	164,000	82	17
/home	32,800	16	509

8. LDAP Server installation/configuration (AIX)

Note: You can find additional information on configuring the IBM SecureWay Directory in the *IBM SecureWay Directory Version 3.2.2 for AIX Installation and Configuration Guide* – this is on the **IBM Tivoli Access Manager Base for AIX Version 3.9** CD at /doc/Directory/aparent.pdf. There are other SecureWay Directory product manuals in the same directory.

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

Note: The web server is used to enable browser based administration of the LDAP server. If this is not possible or not desired, see the section entitled *If you are unable to run the LDAP Administrative web server...* on page 108 below.

- a. Log in as root.
- b. Insert the IBM Tivoli Access Manager Base for AIX Version 3.9 CD.
- c. Using smitty, select: Software Installation and Maintenance -> Install and Update Software -> Install and Update from LATEST Available Software

Version 1.1 – 30 September, 2002
- 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 each of the following entries and press F7 to select it:

- http_server.admin
 ALL
- http_server.base ALL
- http_server.man.en_us
 ALL
- http_server.ssl.128
 ALL

g. Then press Enter:

Install and Update	from LATEST Availab	le Software		
Type or select value Press Enter AFTER n	ues in entry fields. making all desired c	hanges.		
			[Entry Fields]	
* INPUT device / d:	irectory for softwar	e	/dev/cd0	>
* SOFTWARE to insta	all		[http server.admin	> +
PREVIEW only? (i	nstall operation wil	l NOT occur)	no	+
COMMIT software	updates?		yes	+
SAVE replaced fi	les?		no	+
AUTOMATICALLY in:	stall requisite soft	ware?	yes	+
EXTEND file syste	ems if space needed?		yes	+
OVERWRITE same of	r newer versions?		no	+
VERIFY install a	nd check file sizes?		no	+
Include correspo	nding LANGUAGE files	ets?	yes	+
DETAILED output?	_		no	+
Process multiple	volumes?		yes	+
E1-Holp	F2-Pofroch	E2-Cancol	E4-Lict	
ri-neip F5-Dagat	F6-Command	FS=Cancel F7-Fdi+	F8-Image	
F9=Shell	F10=Exit	Enter=Do	ro-image	

- h. Press **Enter**. You will be asked if you are sure. Press **Enter** again. The software will be installed. Exit smitty.
- i. By default the IBM HTTP Server listens to port 80, the same as WebSEAL. If you are going to install WebSEAL on the same machine, 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.
- j. Change directory to /usr/HTTPServer/bin
- k. Start the server by entering the following command: ./apachectl start

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

- I. 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
- m. You can verify that the web server is working by pointing a web browser at
 - http://hostname:port number (http://charon.welwyn.uk.ibm.com:81 in our
 - case) this should result in the IBM HTTP Server splash screen being displayed.

8.3 Install GSKit

- a. Still using the IBM Tivoli Access Manager Base for AIX Version 3.9 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 gskmm ALL and press F7 to select it. Then press Enter:

Install and Upo	late from LATEST Avai	lable Software		
Type or select Press Enter AF	values in entry fiel TER making all desire	ds. d changes.		
* INPUT device * SOFTWARE to : PREVIEW only' COMMIT softwa SAVE replaced AUTOMATICALL' EXTEND file s OVERWRITE san VERIFY instal Include correc DETAILED outp Process mult:	<pre>/ directory for soft install ? (install operation are updates? d files? d install requisite s systems if space need me or newer versions? ll and check file siz esponding LANGUAGE fi put? iple volumes?</pre>	ware will NOT occur) oftware? ed? es? lesets?	[Entry Fields] /dev/cd0 [gskmm no yes no yes no no yes no no yes no yes	> + + + + + + + + + + + + + + + + + + +
F1=Help F5=Reset	F2=Refresh F6=Command	F3=Cancel F7=Edit	F4=List F8=Image	
F9=Shell	F10=Exit	Enter=Do	10-1mage	

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

8.4 Install IBM SecureWay Directory

- a. Still using the IBM Tivoli Access Manager Base for AIX Version 3.9 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:

٠	ldap.max_crypto_client	ALL
٠	ldap.max_crypto_server	ALL

f. Then press Enter:

Install and Upda	ate from LATEST Avai	lable Software		
Type or select w Press Enter AFTH	values in entry fiel SR making all desire	ds. d changes.		
 * INPUT device , * SOFTWARE to in PREVIEW only? COMMIT softwar SAVE replaced AUTOMATICALLY EXTEND file sy OVERWRITE same VERIFY install Include corres DETAILED outpu Process multip 	directory for soft stall (install operation re updates? files? install requisite s ystems if space need or newer versions? and check file siz sponding LANGUAGE fi at? ole volumes?	ware will NOT occur) oftware? ed? es? lesets?	[Entry Fields] /dev/cd0 [ldap.max_crypto_clic no yes no yes yes no no yes no yes	> ent> + + + + + + + + + + + +
F1=Help	F2=Refresh	F3=Cancel	F4=List	
F5=Reset F9=Shell	F6=Command F10=Exit	F7=Edit Enter=Do	F8=Image	

g. Press **Enter**. You will be asked if you are sure. Press **Enter** again. The software will be installed. (This also pulls in DB2 if it is not already installed).

8.5 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: Idapcfg –u "cn=root" –p *password* (where *password* is the LDAP Administrator password – we used Secure99) Idapcfg –I /home/Idapdb2 Idapcfg –s ibmhttp –f /usr/HTTPServer/conf/httpd.conf
- d. Restart the IBM HTTP Server: /usr/HTTPServer/bin/apachectl stop /usr/HTTPServer/bin/apachectl start
- e. The output should look similar to the following:

```
# mkdir /home/ldapdb2
# chmod a+rwx /home/ldapdb2
# ldapcfg -u "cn=root" -p Secure99
 Password for administrator DN cn=root has been set.
IBM Directory Configuration complete.
# ldapcfg -1 /home/ldapdb2
 Creating the directory DB2 default database.
 This operation may take a few minutes.
Cannot open message catalog file ldapadm.cat.
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.

Cannot open message catalog file messages

The 'Cannot open message catalog file' messages were displayed because the <code>slapd.cat</code> and <code>ldapadm.cat</code> files had not been installed. These files can be installed by installing the

ldap.html.en_US ALL packages on the IBM Tivoli Access Manager Language Support Version 3.9 CD.

- g. 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
- h. Start the IBM SecureWay Directory Server: /usr/bin/slapd
- i. The output should look similar to the following:

```
# /usr/bin/slapd
Cannot open message catalog file slapd.cat.
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 libDSP.a.
Plugin of type EXTENDEDOP is successfully loaded from libevent.a.
Plugin of type EXTENDEDOP is successfully loaded from libtranext.a.
Plugin of type AUDIT is successfully loaded from libtranext.a.
Plugin of type EXTENDEDOP 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 EXTENDEDOP is successfully loaded from libtranext.a.
Plugin of type DATABASE is successfully loaded from libtranext.a.
Plugin of type Initialized to 389.
Local UNIX socket name initialized to /tmp/s.slapd.
#
```

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

Alternatively, you can use the startup script /cdrom/common/rc.pd_slapd.

I. To determine whether slapd has started, issue: ps -ef|grep slapd

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

8.6 Add Access Manager Suffixes

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



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

🛛 🦋 Bookmarks 🦽 Local 🔄 🖆 IBM 🚇 Internet 📑	tion: http://charon.welwyn.uk.ibm.com:81/ldap/cgi-bin/ldacgi.exe?Action=Start Lookup 🗂 New&Cool 🖳 RealPlayer
Directory Server	Introduction charon
 Settings Security 	You must <u>add suffixes</u> .

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

irectory Server	Suffixes			
Introduction	🗢 charon			
🗅 Settings 🖸 General	K Ready			
Performance	To add a suffix, enter the di	stinguished na	me of the suffix	ς then click Update .
Suffixes	Suffix DN secluthor	rity=Defaul	.t]
Referrals	12			
Referrals Schema Security Replication	The table below displays su	ffixes defined	to this server.	
 Referrals Schema Security Replication Database Current state 	The table below displays su	ffixes defined	to this server.	

- 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 Access Manager users and Global Sign-On (GSO) data. For example ou=emea, o=ibm, c=gb as shown below. All the Access Manager 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.)

The list was successfull	ly updated. You must <mark>restart th</mark>	ie server for t	this change to take	effect.		
Fo add a suffix, enter the d	istinguished name of the suf	fix, then cliq	ck Update.			
C. C. DN						
Suffix DN ou=emea,	o=1pm,c=gp					
Suffix DN ou=emea,	o=10m, c=gp	To remous	e o guffiy, celect t	he checkhow on	d click Undate , Remaring :	a cuff
Suffix DN ou=emea, The table below displays su diminates access to all dire	offixes defined to this server ctory data beneath that suff	. To remove ix, however	e a suffix, select t r the data is not re	he checkbox an moved from the	d click Update . Removing a e directory.	a suffi
Suffix DN ou=emea, The table below displays su eliminates access to all dire	o-inn, c-go iffixes defined to this server ctory data beneath that suff	. To remove ix, however Remove?	e a suffix, select t r the data is not re	he checkbox an emoved from the	d click Update . Removing a e directory.	a suff
Suffix DN ou=emea, The table below displays su liminates access to all dire Current server suffixes cn=localhost	o-ins, c-go iffixes defined to this server. ctory data beneath that suff Comment System suffix	. To remove ix, however Remove?	e a suffix, select t r the data is not re	he checkbox an moved from the	d click Update . Removing a e directory.	a suff

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:

Suffixes				
😏 charon				
The list was successfull	ly updated. You must <mark>restart th</mark>	<u>ne server</u> for 1	this change to take effect.	
o add a suffix enter the di	istinguished name of the suf	ffix then clir	ick Undate	
o doo d bornin, onior ano a	angaonoa nano or mo oa		on opure.	
		_		
Suffix DN				
Suffix DN				
Suffix DN	fores defined to this server	. To remove	re a suffice calact the sheal	hav and alick Undata Remarking a m
Suffix DN	ffixes defined to this server ctory data beneath that suff	r. To remove fix, however	ve a suffix, select the check r the data is not removed fi	box and click Update . Removing a su rom the directory.
Suffix DN	ffixes defined to this server ctory data beneath that suff	r. To remove fix, however	re a suffix, select the check r the data is not removed fi	box and click Update . Removing a su rom the directory.
Suffix DN he table below displays su iminates access to all dire Current server suffixes	ffixes defined to this server ctory data beneath that suff Comment	. To remove fix, however Remove?	re a suffix, select the check r the data is not removed fi	box and click Update . Removing a su rom the directory.
Suffix DN he table below displays su iminates access to all dire Current server suffixes :n=localhost	ffixes defined to this server ctory data beneath that suff Comment System suffix	To remove fix, however Remove?	re a suffix, select the check r the data is not removed fi	box and click Update . Removing a su rom the directory.
Suffix DN	ffixes defined to this server ctory data beneath that suff Comment System suffix Contains no directory data	To remove fix, however Remove?	re a suffix, select the check r the data is not removed fi	box and click U pdate . Removing a su rom the directory.

g. Click on the 'restart the server' link at the top of the page. A message stating 'The directory server is starting' is displayed. This restart process can take several minutes. Once complete a message stating 'The directory server is running' will be displayed:



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

IBM Tivoli Access Manager 3.9 – Cookbook

Directory Server	General settings	
Introduction	😔 charon	
Settings General	K Ready	
Performance Transactions Event notification	Edit the general settings i	for the server, then click Update .
Suffixes	Hostname	charon
Carletenais	Unsecure port	389
Replication	Version	IBM SecureWay Directory 3.2
▶ 🔲 Database ▼ 🛅 Current state	Password encryption	C None
🗌 🖸 Server status	20	C imask
Connections		• crypt
► C Logs		C SHA
Dogoff		
	Update Reset	

- 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 'restart the server' and wait for the server to restart.
- j. The web browser is no longer required and may be closed.

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

There have been installations where (for various reasons) it has not been possible to run a web server to perform the LDAP administrative operations. In that case an alternative approach is to edit the configuration file manually. The file in question is: /usr/ldap/etc/slapd32.conf

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

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

You can specify one-way password encryption by modifying the <code>ibm-slapdPwEncryption</code> line to:

Ibm-slapdPwEncryption: crypt

8.7 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. Click on Authentication: Simple. Enter the Server name, LDAP administrator DN and password (charon.welwyn.uk.ibm.com, cn=root and Secure99 in our case):

🕸 IBM SecureWay Directory Management Tool			-미×
	Add server		?
	Ready		IBM.
	Connect to directory server Server name : Idap:// [Port : [Use SBL : [Certificate name :] Authentication type : User DN : [User password : [Keyclass file name :] Keyclass file password :]	charon welwyn ukibm.com 389 C None C Simple C SASL External C CRAM MD5 cn=root *******	
Add server Delete server Exit		OK Cancel Help	

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



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

Udap://charon.welwyn.uk.ibm.com:389

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):

-	IBM :	SecureWay Directory Management Tool 🛛 🕐 📃	
ldap://localhost:389	F	ebind ?	[
Introduction Server	F	eady IBM。	
Administration Rebind Schema Chject classes Attributes Matching rules		nter a new bind DN and password for the server idap://localhost.389 Anonymous (@ Authenticated ser DN :	· .
Directory tree Director	Ľ	iser password : CK Cancel Help	
Add server Delete server Exit			
		Delete	

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:



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 Access Manager 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.

elect an En	ntry type, enter the Parent D	N, modify the Entry	RDN, then click C	νK.	
Entry type	Organizational unit 💌				
Parent DN:		1			
Entry RDN:	ou=emea,o=ibm,c=gb	1			

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

jectClass (Object class): 🛛 🚦	rganizatio	onalUnit
i (DN): 🛛 🔽	u=emea,	o=ibm,c=gb
ou:	2	emea,o=ibm,c=gb
businessCategory:	0	
description:	0	
destinationIndicator:	0	
facsimileTelephoneNumber:	0	
internationalISDNNumber:	0	
L2	0	
physicalDeliveryOfficeName:	0	
postalAddress:	0	
postalCode:	0	

k. If desired you can enter a description, etc. 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:

1	Idap://charon.welwyn.uk.ibm.com:389	
	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. Access Manager Server installation (AIX)

- a. Log in as root.
- b. Insert the IBM Tivoli Access Manager Base for AIX Version 3.9 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. Move the cursor to PD ALL and press F7 to select it. Then press Enter:

Install and Update	from LATEST Availabl	e Software			
Type or select valu Press Enter AFTER m	es in entry fields. Making all desired ch	anges.			
			[Fnt rv	Fieldel	
* INPUT device / di	rectory for software	1	/dev/cd0	TICIUS	
* SOFTWARE to insta	11		[PD		> +
PREVIEW only? (in	stall operation will	NOT occur)	no		+
COMMIT software u	pdates?		yes		+
SAVE replaced fil	es?		no		+
AUTOMATICALLY ins	tall requisite softw	are?	yes		+
EXTEND file syste	ms if space needed?		yes		+
OVERWRITE same or	newer versions?		no		+
VERIFY install an	d check file sizes?		no		+
Include correspon	ding LANGUAGE filese	ts?	yes		+
DETAILED output?			no		+
Process multiple	volumes?		yes		+
F1=Help	F2=Refresh	F3=Cancel	F4=	=List	
F5=Reset	F6=Command	F7=Edit	F8:	=Image	
F9=Shell	F10=Exit	Enter=Do		-	

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

10. WebSEAL Installation (AIX)

Note: This step will install WebSEAL together with any necessary pre-requisite components (namely Access Manager Runtime, GSKit and LDAP Client) if they are not already installed.

- a. Log in as root.
- b. Insert the IBM Tivoli Access Manager Web Security for AIX Version 3.9 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 each of the following entries and press **F7** to select it:

•	3.9.0.0	Access	Manager	Runtime	
•	PDWeb				ALL
•	gskkm				ALL
•	ldap.cli	ent			ALL
•	ldap.max	_crypto_	client		ALL

Note: If you are installing WebSEAL on the same box as the LDAP Server or the Access Manager Policy Server, then some of these packages may already be installed. (This is shown by the package name being preceded by an '@' sign in the list.)

g. Then press Enter:

Install and Update f	from LATEST Availabl	e Software			
Type or select value Press Enter AFTER ma	es in entry fields. aking all desired ch	langes.			
 * INPUT device / dir * SOFTWARE to instal PREVIEW only? (ins COMMIT software up SAVE replaced file AUTOMATICALLY inst EXTEND file system OVERWRITE same or VERIFY install and Include correspond 	rectory for software ll stall operation will odates? es? tall requisite softw ns if space needed? newer versions? d check file sizes? ding LANGUAGE filese	e NOT occur) ware? ets?	[Entry /dev/cd0 [3.9.0.0 no yes no yes yes no no yes po	Fields] Access Mana	> ge> + + + + + + + + + +
Process multiple v	volumes?		yes		+
F1=Help F5=Reset F9=Shell	F2=Refresh F6=Command F10=Exit	F3=Cancel F7=Edit Enter=Do	F4 F8	=List =Image	

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

11. Access Manager Configuration (AIX)

Note: This section describes how to configure all the Access Manager servers and WebSEAL.

- a. Ensure that the Directory (and any intervening network) is working correctly. (You can do this by issuing the command ldapsearch -h ldap_server_hostname -D cn=root -w ldap password -b "" -s base objectclass=*)
- b. Using smitty, select: Communications Applications and Services -> Access Manager for e-business
- c. You will be presented with the Access Manager for e-business Setup Menu. Type 1 (corresponding to Configure Package):

```
Access Manager for e-business 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 Access Manager for e-business Configuration Menu. Type 1 (corresponding to Access Manager Runtime Configuration):

Access Manager for e-business Configuration Menu 1. Access Manager Runtime Configuration 2. Access Manager Policy Server Configuration 3. Access Manager Authorization Server Configuration 4. Access Manager WebSEAL Configuration x. Return to Access Manager for e-business 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:

```
Access Manager for e-business Configuration Menu

1. Access Manager Runtime Configuration
2. Access Manager Policy Server Configuration
3. Access Manager Authorization Server Configuration
4. Access Manager WebSEAL Configuration
x. Return to Access Manager for e-business Setup Menu
Please select the menu item [x]: 1
Enter the LDAP server hostname: charon.welwyn.uk.ibm.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 Access Manager for e-business Configuration Menu. Type 1 (this time corresponding to Access Manager Policy Server 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 Access Manager 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 Access Manager 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 Access Manager machines, but may introduce security exposures if the network can be compromised during the configuration step.) The output should look similar to the following:

Access Manager for e-business Configuration Menu

1. Access Manager Policy Server Configuration
2. Access Manager Authorization Server Configuration
3. Access Manager WebSEAL Configuration
x. Return to Access Manager for e-business Setup Menu

Please select the menu item [x]: 1
Enter the LDAP administrative user DN [cn=root]:
Enter the LDAP administrative user password: Secure99
Do you want to enable SSL communication between the
Access Manager Policy 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
Access Manager Administrator account.
The administrator login name is sec_master and cannot be changed.

Enter the password for the Access Manager Administrator: Secure99 Re-enter the password for confirmation: Secure99 Enter the SSL server port for Access Manager Policy Server [7135]: Enter the Policy Server SSL certificate lifetime [365]: Selecting the Enable root CA Certificate download option simplifies the configuration of the Runtime on subsequent machines. Enabling this option may introduce a security exposure if a non-trusted host can impersonate the Access Manager Policy Server in the network. Enable root CA Certificate download (y/n) [No]? y * Configuring server Generating Server Certificates, please wait. Creating the SSL certificate. This may take several minutes... The SSL configuration of the Access Manager Policy Server has completed successfully. The Policy Server'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 Access Manager Policy Server v3.9.0 (Build 020412) Copyright (C) IBM Corporation 1994-2002. All Rights Reserved. 2002-05-17-09:24:11.899+00:00I---- 0x1354A0A0 pdmgrd NOTICE ivc general ivmgrd.cpp 710 0x0000001 Server startup 2002-05-17-09:24:11.999+00:00I---- 0x1354A0A0 pdmgrd NOTICE ivc general ivmgrd.cpp 715 0x0000001 Loading configuration This package has been successfully configured. Press <enter> to continue ...

g. Press Enter. You will again be presented with the Access Manager for e-business Configuration Menu. Type 1 (this time corresponding to Access Manager Authorization Server Configuration) and press Enter. When prompted enter the LDAP administrator password (we used Secure99), and the password for the Access Manager 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 Access Manager server and the LDAP server. The configuration process can take several minutes. The output should look similar to the following:

```
Access Manager for e-business Configuration Menu
        1. Access Manager Authorization Server Configuration
        2. Access Manager WebSEAL Configuration
        x. Return to Access Manager for e-business Setup Menu
Please select the menu item [x]: 1
Enter the LDAP administrative user DN [cn=root]:
Enter the LDAP administrative user password: Secure99
Do you want to enable SSL communication between the
Access Manager Policy Server and the LDAP server (y/n) [Yes]? n
Enter the password for the Access Manager 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
Access Manager Authorization Server v3.9.0 (Build 020412)
Copyright (C) IBM Corporation 1994-2002. All Rights Reserved.
2002-05-17-10:54:27.183+00:00I---- 0x1354A0A0 pdacld NOTICE ivc general ivacl
d.cpp 397 0x0000001
Server startup
2002-05-17-10:54:27.247+00:00I---- 0x1354A0A0 pdacld NOTICE ivc general ivacl
d.cpp 402 0x0000001
Loading configuration
This package has been successfully configured.
Press <enter> to continue ...
```

(The first time we attempted to configure the Access Manager Authorization Server, the

configuration failed with a message "Timeout occurred while attempting to read from socket". However after unconfiguring this package, the second attempt at configuring it was successful.)

h. Press Enter. You will again be presented with the Access Manager for e-business Configuration Menu. Type 1 (this time corresponding to Access Manager WebSEAL Configuration). Press Enter. When prompted enter the password for the Access Manager 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 Access Manager server and the LDAP server. The configuration process can take several minutes. The output should look similar to the following:

Access Manager for e-business Configuration Menu 1. Access Manager WebSEAL Configuration x. Return to Access Manager for e-business Setup Menu Please select the menu item [x]: 1 Enter the password for the Access Manager Administrator: Secure99 Do you want to enable SSL communication between the Access Manager Policy 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 Access Manager WebSEAL Version 3.9.0 (Build 020412)

Copyright (C) IBM Corporation 1994-2002. All Rights Reserved.

Press <enter> to continue ...

i. Press Enter. You can now check that Access Manager is working by following the steps described in Section Part V - 22 - Initial Access Manager Validation on Page 170 below.

12. Web Portal Manager Installation and Configuration (AIX)

Note: This step includes the installation of Web Portal Manager together with any necessary prerequisite components (namely WebSphere Application Server, Access Manager Runtime, GSKit and the LDAP Client) if they are not already installed.

12.1 Install the Access Manager pre-requisite software

- a. Log in as root.
- b. Insert the IBM Tivoli Access Manager Web Portal Manager for AIX Version 3.9 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 each of the following entries and press F7 to select it:

•	gskkm	ALL
•	ldap.client	ALL
•	ldap.max_crypto_client	ALL

Note: If you are installing Web Portal Manager on the same box as the LDAP Server or the Access Manager Policy Server, then some or all of these packages may already be installed. (This is shown by the package name being preceded by an '@' sign in the list.)

g. 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	[gskkm	> +
PREVIEW only? (install operation will NOT occur)	no	+
COMMIT software updates?	yes	+
SAVE replaced files?	no	+
AUTOMATICALLY install requisite software?	yes	+
EXTEND file systems if space needed?	yes	+
OVERWRITE same or newer versions?	no	+
VERIFY install and check file sizes?	no	+
Include corresponding LANGUAGE filesets?	yes	+
DETAILED output?	no	+

Process multig	ple volumes?	У	7es	+
F1=Help F5=Reset F9=Shell	F2=Refresh F6=Command F10=Exit	F3=Cancel F7=Edit Enter=Do	F4=List F8=Image	

- h. Press Enter. You will be asked if you are sure. Press Enter again. The software will be installed.
- i. **If IBM HTTP Server is not already installed** then install IBM HTTP Server as described in Section 8.2 *Install the IBM HTTP Server* on Page 100 above.

12.2 Install WebSphere Application Server

- a. Insert /continue to use the IBM Tivoli Access Manager Web Portal Manager for AIX Version 3.9 CD.
- b. Ensure that a mount point for the CD-ROM device is defined and mounted. (We used /cdrom.)
- c. Change directory to /cdrom/usr/sys/inst.images/WebSphere
- d. Enter the command
 ./install.sh -silent -responseFile ./install.script -prereqfile \
 ./prereq.properties
 (this step may take several minutes to run).
- e. The output should look similar to the following:

```
# ./install.sh -silent -responseFile ./install.script -prereqfile
./prereq.properties
Installing Samples
Launching SEAppinstall.sh for Samples.ear
Launching SEAppinstall.sh for petstore.ear
Creating SampleDB
Launching createSampleDB.sh
A copy of the log file is in /tmp/install.log
The install log file is install.log and is stored in the logs directory
Ending the application...
#
```

12.3 Install the WebSphere Application Server PTFs

a. Stop the WebSphere Application Server, HTTP Server and the LDAP server:

```
# /usr/WebSphere/AppServer/bin/stopServer.sh
WebSphere Application Server, Advanced Single Server Edition V4.0
WebSphere Application Server, Advanced Developer Edition V4.0
WebSphere Application Server, Advanced Edition V4.0
Runtime Utility Program
Copyright (C) IBM Corporation, 1997-2001
```

```
WSRU0025I: Loading configuration from file.
WSRU0028I: Using the specified configuration file:
    /usr/WebSphere/AppServer/config/server-cfg.xml
WSRU0029I: The diagnostic host name read as localhost.
WSRU0030I: The diagnostic port was read as 7000.
Stopping server.
WSRV0056E: A connection could not be made to perform the requested operation.
This usually indicates that the target utility server is stopped.
This may indicate that the wrong diagnostic port was used.
WSRU0031E: Command Failure: Stop Server.
WSRU0032E: Transfer failed:
WSRV0057E: Failed to complete transfer with DrAdmin server.
# /usr/HTTPServer/bin/apachectl stop
/usr/HTTPServer/bin/apachectl stop: httpd stopped
# ps -ef |grep slapd
   root 15750 17914
                      1 05:17:52 pts/0 0:00 grep slapd
    ldap 25178
                 1 0 05:03:39 pts/0 0:06 /usr/bin/slapd
# kill 25178
#
```

- b. Change directory to /cdrom/usr/sys/inst.images/WebSphere_PTF2
- c. It is probably worth reviewing the contents of was40_aes_ptf_2.Readme in this directory.
- d. Copy the contents of this directory to a temporary directory:

```
# cd /cdrom/usr/sys/inst.images/WebSphere_PTF2
# mkdir /tmp/was_ptf2
# cp * /tmp/was_ptf2
#
```

e. Change directory to the temporary directory and issue the following command: ./install.sh The output should look similar to the following:

```
# cd /tmp/was ptf2
# ./install.sh
WebSphere Application Server 4.0, Advanced Edition Single Server PTF 2
Please shut down the Application Server and any Webservers that might be running.
If not the PTF may not be installed properly
If you want to install silently, please issue install.sh -silent
silent install
                    =
IHS install
                     =
                        true
J2C Connector install = maybe
Please enter the WebSphere root directory
/usr/WebSphere/AppServer
Installing the WebSphere Application Server 4.0 PTF 2
2002/05/21 06:07:33 Extractor version: 1.29
2002/05/21 06:07:40
2002/05/21 06:07:41 Input Jar File
                                      : /tmp/was_ptf2/was40_aes_ptf_2.jar src=Default
2002/05/21 06:07:44 Start of extraction for /tmp/was_ptf2/was40_aes_ptf_2.jar
2002/05/21 06:07:44 No target message provided, default enabled.
2002/05/21 06:07:44 Target Directory
                                       : /usr/WebSphere/AppServer
2002/05/21 06:07:45 Testing Temporary Directory : /tmp
2002/05/21 06:07:45 Full Temporary Directory : /tmp
2002/05/21 06:07:45 The temporary directory is usable.
2002/05/21 06:07:45 Backup Jar File : /usr/WebSphere/AppServer/was40 ptf 2 backup.jar
2002/05/21 06:07:45 This update applies to the following components:
2002/05/21 06:07:45
                       Client
2002/05/21 06:07:45
                       Server
2002/05/21 06:07:45
                       Samples
2002/05/21 06:07:45
                       Console
2002/05/21 06:07:45
                       Common
2002/05/21 06:07:45
                       Deploytools
2002/05/21 06:07:45
                      Plugins
2002/05/21 06:07:45
                      Samples_Common
```

2002/05/21 06:07:45 Server Common Tools Common 2002/05/21 06:07:45 J2EEClient 2002/05/21 06:07:45 2002/05/21 06:07:45 JTCClient 2002/05/21 06:07:45 2002/05/21 06:07:45 The following components were detected installed: 2002/05/21 06:07:47 Console 2002/05/21 06:07:47 Deploytools 2002/05/21 06:07:47 J2EEClient 2002/05/21 06:07:47 Tools Common 2002/05/21 06:07:47 Common 2002/05/21 06:07:47 Client 2002/05/21 06:07:47 Samples 2002/05/21 06:07:47 Server_Common 2002/05/21 06:07:47 JTCClient 2002/05/21 06:07:47 Server 2002/05/21 06:07:47 Samples Common 2002/05/21 06:07:47 Plugins 2002/05/21 06:07:48 2002/05/21 06:07:48 Product file type: XML 2002/05/21 06:07:49 Product file [/usr/WebSphere/AppServer/properties/com/ibm/websphere/product.xml] 2002/05/21 06:08:38 No prior history events noted. 2002/05/21 06:08:43 Determining files to back up 1 of 13271 2002/05/21 06:08:44 scanning 0% complete 2002/05/21 06:44:26 Applying entry 12921 of 13270 97% complete Launched chmod 711 /usr/WebSphere/AppServer/uninstall ptf 2.sh Cmd ended rc=0 2002/05/21 06:44:38 Applying entry 13270 of 13270 100% complete 2002/05/21 06:44:39 No Re-Sequencing of jar files was noted. 2002/05/21 06:44:39 Processing virtual script CopyEjbDeploy Launched cp /usr/WebSphere/AppServer/bin/ejbdeploy.sh /usr/WebSphere/AppServer/deploytool/itp/ejbdeploy.sh Cmd ended rc=0 2002/05/21 06:44:43 Updating /usr/WebSphere/AppServer/properties/com/ibm/websphere/product.xml 2002/05/21 06:44:45 Input Jar File : /tmp/was_ptf2/was40_aes_ptf_2.jar 2002/05/21 06:44:45 Target Directory : /usr/WebSphere/AppServer 2002/05/21 06:44:45 Backup Jar File : /usr/WebSphere/AppServer/was40 ptf 2 backup.jar 2002/05/21 06:44:45 Warnings Issued : 0 2002/05/21 06:44:45 Log File : /usr/WebSphere/AppServer/logs/was40_ptf_2.log 2002/05/21 06:44:45 2002/05/21 06:44:45 End of extraction for /tmp/was ptf2/was40 aes ptf 2.jar with no errors. 2002/05/21 06:44:45 2002/05/21 06:44:45 Please view the log for details. Installing JDK PTF 2 2002/05/21 06:46:19 Extractor version: 1.29 2002/05/21 06:46:25 2002/05/21 06:46:26 Input Jar File : /tmp/was_ptf2/jdk_ptf_2.jar src=Default 2002/05/21 06:46:27 Start of extraction for /tmp/was_ptf2/jdk_ptf_2.jar 2002/05/21 06:46:27 No target message provided, default enabled. 2002/05/21 06:46:27 Target Directory : /usr/WebSphere/AppServer/java ptf 2 2002/05/21 06:46:27 Testing Temporary Directory : /tmp 2002/05/21 06:46:27 Full Temporary Directory : /tmp 2002/05/21 06:46:27 The temporary directory is usable. 2002/05/21 06:46:27 Backup Jar File : /usr/WebSphere/AppServer/jdk ptf 2 backup.jar 2002/05/21 06:46:27 This update applies to the following components: JDK 2002/05/21 06:46:27 2002/05/21 06:46:27 JRE 2002/05/21 06:46:27 2002/05/21 06:46:27 The following components were detected installed: 2002/05/21 06:46:29 JRE 2002/05/21 06:46:29 JDK 2002/05/21 06:46:29 2002/05/21 06:46:29 No set product file. 2002/05/21 06:46:29 Bypassing duplicate application checking by request. 2002/05/21 06:46:30 Determining files to back up 2002/05/21 06:46:30 scanning 1 of 301 0% complete

```
IBM Tivoli Access Manager 3.9 - Cookbook
```

```
2002/05/21 06:58:17 Applying entry 300 of 300 100% complete
2002/05/21 06:58:17 No Re-Sequencing of jar files was noted.
2002/05/21 06:58:17 Input Jar File
                                      : /tmp/was_ptf2/jdk_ptf_2.jar
2002/05/21 06:58:17 Target Directory : /usr/WebSphere/AppServer/java ptf 2
2002/05/21 06:58:17 Backup Jar File : /usr/WebSphere/AppServer/jdk_ptf_2_backup.jar
2002/05/21 06:58:17 Warnings Issued : 0
                                      : /usr/WebSphere/AppServer/logs/jdk_ptf_2.log
2002/05/21 06:58:17 Log File
2002/05/21 06:58:17
2002/05/21 06:58:17 End of extraction for /tmp/was ptf2/jdk ptf 2.jar with no errors.
2002/05/21 06:58:17
2002/05/21 06:58:17 Please view the log for details.
WARNING: If you install the IBM HTTP Server PTF, the back level of IHS may not work properly with
the new level of GSkit.
Please enter whether you want to install IHS WebServer PTF (y/n)
У
Installing IHS PTF
2002/05/21 07:08:14 Extractor version: 1.29
2002/05/21 07:08:20
2002/05/21 07:08:21 Input Jar File
                                          : /tmp/was_ptf2/ihs_ptf_2.jar src=Default
2002/05/21 07:08:21 Start of extraction for /tmp/was_ptf2/ihs_ptf_2.jar
2002/05/21 07:08:21 No target message provided, default enabled.
2002/05/21 07:08:22 Target Directory : /usr/HTTPServer
2002/05/21 07:08:22 Testing Temporary Directory : /tmp
2002/05/21 07:08:22 Full Temporary Directory : /tmp
2002/05/21 07:08:22 The temporary directory is usable.
2002/05/21 07:08:22 Backup Jar File : /usr/WebSphere/AppServer/ihs_ptf_2_backup.jar
2002/05/21 07:08:22 Component checking deactiviated, affected components entry is null.
2002/05/21 07:08:22 No set product file.
2002/05/21 07:08:22 Bypassing duplicate application checking by request.
2002/05/21 07:08:22 Determining files to back up
2002/05/21 07:08:22 scanning 1 of 41 2% complete
2002/05/21 07:08:47 scanning 6 of 41 14% complete
2002/05/21 07:08:48 scanning 41 of 41 100% complete
2002/05/21 07:08:48
2002/05/21 07:08:56 Backing Up 2 of 15 13% complete
2002/05/21 07:09:29 Backing Up 4 of 15 26% complete
2002/05/21 07:09:37 Backing Up 13 of 15 86% complete
2002/05/21 07:09:37 Backing Up 15 of 15 100% complete
2002/05/21 07:09:37
2002/05/21 07:09:38 Applying entry 1 of 40
                                                2% complete
2002/05/21 07:10:03 Applying entry 6 of 40 15% complete
2002/05/21 07:10:04 Applying entry 40 of 40 100% complete
2002/05/21 07:10:04 No Re-Sequencing of jar files was noted.
2002/05/21 07:10:04 Input Jar File : /tmp/was ptf2/ihs ptf 2.jar
2002/05/21 07:10:04 Target Directory : /usr/HTTPServer
2002/05/21 07:10:05 Backup Jar File : /usr/WebSphere/AppServer/ihs_ptf_2_backup.jar
2002/05/21 07:10:05 Warnings Issued : 0
2002/05/21 07:10:05 Log File : /usr/WebSphere/AppServer/logs/ihs_ptf_2.log
2002/05/21 07:10:05
2002/05/21 07:10:05 End of extraction for /tmp/was_ptf2/ihs_ptf_2.jar with no errors.
2002/05/21 07:10:05
2002/05/21 07:10:05 Please view the log for details.
Installing the gskit package
Installing new version of GSkit.
+------
                   Pre-installation Verification...
+-----
Verifying selections...done
Verifying requisites...done
Results...
WARNINGS
----
 Problems described in this section are not likely to be the source of any
  immediate or serious failures, but further actions may be necessary or
  desired.
 Already Installed
  The number of selected filesets that are either already installed
  or effectively installed through superseding filesets is 1. See
```

```
the summaries at the end of this installation for details.
 NOTE: Base level filesets may be reinstalled using the "Force"
 option (-F flag), or they may be removed, using the deinstall or
 "Remove Software Products" facility (-u flag), and then reinstalled.
 << End of Warning Section >>
FILESET STATISTICS
   1 Selected to be installed, of which:
      1 Already installed (directly or via superseding filesets)
 _ _ _ _
   0 Total to be installed
Pre-installation Failure/Warning Summary
Pre-installation Failure/Warning
Name
                    Level
_____
                    5.0.4.25 Already superseded by 5.0.4.67
askkm.rte
```

12.4 Install Web Portal Manager

- a. Using smitty, select: Software Installation and Maintenance -> Install and Update Software -> Install and Update from LATEST Available Software
- b. Against Input device / directory for software press F4 and select the CD-ROM typically /dev/cd0.
- c. Against SOFTWARE to install press F4. A list of SOFTWARE to install will be displayed.
- d. Move the cursor to each of the following entries and press F7 to select it:
 - 3.9.0.0 Access Manager Runtime
 - 3.9.0.0 Access Manager Web Portal Manager ALL

Note: Again, if you are installing Web Portal Manager on the same box as the LDAP Server or the Access Manager Policy Server, then some or all of these packages may already be installed. (This is shown by the package name being preceded by an '@' sign in the list.)

e. 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
                                                    [3.9.0.0 Access Manage> +
  PREVIEW only? (install operation will NOT occur)
                                                     no
                                                                              +
  COMMIT software updates?
                                                      yes
                                                                              +
  SAVE replaced files?
                                                      no
                                                                              +
  AUTOMATICALLY install requisite software?
                                                     yes
                                                                              +
                                                     yes
  EXTEND file systems if space needed?
                                                                              +
  OVERWRITE same or newer versions?
                                                                              +
                                                      no
```

ALL

VERIFY install and o	check file sizes?		no		+
Include correspondir	ng LANGUAGE filese	ts?	yes		+
DETAILED output?			no		+
Process multiple vol	lumes?		yes		+
FI=Help F2	2=Reiresn	F3=Cancel		F4=L1St	
F5=Reset F6	6=Command	F'/=Edit		F8=1mage	
F9=Shell F1	10=Exit	Enter=Do			

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

12.5 Configure Web Portal Manager

- a. Start the IBM SecureWay Directory Server (/usr/bin/slapd).
- b. Ensure that the Directory (and any intervening network) is working correctly. (You can do this by issuing the command ldapsearch -h ldap_server_hostname -D cn=root -w ldap password -b "" -s base objectclass=*)
- c. Ensure that the Access Manager Policy Server is running (ps -ef|grep pdmgrd).
- d. Using smitty, select: Communications Applications and Services -> Access Manager for e-business
- e. You will be presented with the Access Manager for e-business Setup Menu. Type 1 (corresponding to Configure Package):

```
Access Manager for e-business Setup Menu

1. Configure Package

2. Unconfigure Package

3. Display Configuration Status

x. Exit

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

f. Press Enter. You will be presented with the Access Manager for e-business Configuration Menu. Type 1 (corresponding to Access Manager Runtime Configuration):

Access Manager for e-business Configuration Menu 1. Access Manager Web Portal Manager Configuration x. Return to Access Manager for e-business Setup Menu

Please select the menu item [x]: 1

g. Press Enter. The output should look similar to the following:

```
Access Manager for e-business Configuration Menu
        1. Access Manager Web Portal Manager Configuration
        x. Return to Access Manager for e-business Setup Menu
Please select the menu item [x]: 1
Stopping WebSphere Application Server with command
          /usr/WebSphere/AppServer/bin/stopServer.sh
WebSphere Application Server, Advanced Single Server Edition V4.0
WebSphere Application Server, Advanced Developer Edition V4.0
WebSphere Application Server, Advanced Edition V4.0
Runtime Utility Program
Copyright (C) IBM Corporation, 1997-2001
WSRU0025I: Loading configuration from file.
WSRU0028I: Using the specified configuration file:
    /usr/WebSphere/AppServer/config/server-cfg.xml
WSRU0029I: The diagnostic host name read as localhost.
WSRU0030I: The diagnostic port was read as 7000.
Stopping server.
Failed to open socket
WSRU0054E: Exception: java.net.ConnectException: A remote host refused an attempted connect
operation.
java.net.ConnectException: A remote host refused an attempted connect operation.
        at java.net.PlainSocketImpl.socketConnect(Native Method)
        at java.net.PlainSocketImpl.doConnect(PlainSocketImpl.java:329)
        at java.net.PlainSocketImpl.connectToAddress(PlainSocketImpl.java:141)
        at java.net.PlainSocketImpl.connect(PlainSocketImpl.java:128)
        at java.net.Socket.<init>(Socket.java:285)
        at java.net.Socket.<init>(Socket.java:112)
        at com.ibm.ejs.sm.util.debug.DrClientSocket$1.run(DrClientSocket.java:83)
        at java.security.AccessController.doPrivileged(Native Method)
        at com.ibm.ejs.sm.util.debug.DrClientSocket.prepareSocket(DrClientSocket.java:80)
        at com.ibm.ejs.sm.util.debug.DrClientSocket.prepare(DrClientSocket.java:73)
        at com.ibm.ejs.sm.util.debug.DrSocket.sendThenReceive(DrSocket.java:144)
        at com.ibm.ejs.sm.util.debug.DrClientAccessor.sendThenReceive(DrClientAccessor.java:854)
        at com.ibm.ejs.sm.util.debug.DrClientAccessor.processRequest(DrClientAccessor.java:840)
        at com.ibm.ejs.sm.util.debug.DrClientAccessor.processRequest(DrClientAccessor.java:831)
        at com.ibm.ejs.sm.util.debug.DrClientAccessor.basicStopServer(DrClientAccessor.java:460)
        at com.ibm.ejs.sm.util.debug.DrAdmin.stopServer(DrAdmin.java:1076)
        at com.ibm.ejs.sm.util.debug.DrAdmin.processCommands(DrAdmin.java:658)
        at com.ibm.ejs.sm.util.debug.DrAdmin.process(DrAdmin.java:237)
        at com.ibm.ejs.sm.util.debug.DrAdmin.main(DrAdmin.java:157)
        at java.lang.reflect.Method.invoke(Native Method)
        at com.ibm.ws.bootstrap.WSLauncher.main(WSLauncher.java:158)
WSRU0031E: Command Failure: Stop Server.
WSRU0032E: Transfer failed:
WSRV0057E: Failed to complete transfer with DrAdmin server.
Installing Access Manager Web Portal Manager with command
         /usr/WebSphere/AppServer/bin/SEAppInstall.sh -install
/opt/PolicyDirector/java/export/pdwpm/pdwpm.ear -precompileJsp FALSE -interactive false
IBM WebSphere Application Server Release 4, Aes
J2EE Application Installation Tool, Version 1.0
Copyright IBM Corp., 1997-2001
The -configFile option was not specified. Using /usr/WebSphere/AppServer/config/server-cfg.xml
Loading Server Configuration from /usr/WebSphere/AppServer/config/server-cfg.xml
Server Configuration Loaded Successfully
Loading /opt/PolicyDirector/java/export/pdwpm/pdwpm.ear
```

IBM Tivoli Access Manager 3.9 - Cookbook

```
Getting Expansion Directory for EAR File
Expanding EAR File to /usr/WebSphere/AppServer/installedApps/pdwpm.ear
Installed EAR On Server
Validating Application Bindings..
Finished validating Application Bindings.
Saving EAR File to directory
Saved EAR File to directory Successfully
Backing up Server Configuration to /usr/WebSphere/AppServer/config/server-cfg.xml~
Saving Server Configuration to /usr/WebSphere/AppServer/config/server-cfg.xml
Save Server Config Successful
JSP Pre-compile Skipped.....
Installation Completed Successfully
Starting WebSphere Application Server with command
          /usr/WebSphere/AppServer/bin/startServer.sh -waitAmount 0
WebSphere Application Server, Advanced Single Server Edition V4.0
Application Server Launcher
Copyright (C) IBM Corporation, 2001
The configuration file was defaulted to:
    /usr/WebSphere/AppServer/config/server-cfg.xml
Using the single available node or the localhost node.
Using the single available server.
Will wait indefinitely for launch results.
Initiating server launch.
Loaded domain "WebSphere Administrative Domain".
Selected node "charon".
Selected server "Default Server".
WSPL0065I: Initiated server launch with process id 11950.
Time mark: Tuesday, May 21, 2002 8:05:00 AM CDT
Waiting for the server to be initialized.
Time mark: Tuesday, May 21, 2002 8:06:39 AM CDT
Initialized server.
Waiting for applications to be started.
Time mark: Tuesday, May 21, 2002 8:58:03 AM CDT
Started applications.
WSPL0057I: The server Default Server is open for e-business.
Please review the server log files for additional information.
Standard output: /usr/WebSphere/AppServer/logs/default server stdout.log
Standard error: /usr/WebSphere/AppServer/logs/default_server_stderr.log
Regenerating WebSphere plugin configuration with command
         /usr/WebSphere/AppServer/bin/GenPluginCfg.sh -configFile
/usr/WebSphere/AppServer/config/server-cfg.xml
IBM WebSphere Application Server Advanced Single Server Edition, Release 4.0
Web Server Plugin Configuration Generator
Copyright IBM Corp., 1997-2001
Loading Server Configuration from /usr/WebSphere/AppServer/config/server-cfg.xml
Server Configuration Load Successful
Generating Plugin Configuration from /usr/WebSphere/AppServer/config/server-cfg.xml
Plugin Config Generation Completed Successfully
/usr/HTTPServer/bin/apachectl restart: httpd restarted
Press <enter> to continue ...
```

h. Press Enter.

12.6 Set the HTTP Server port numbers

a. We earlier edited the HTTP configuration file, httpd.conf, so that IBM HTTP Server would

Version 1.1 – 30 September, 2002

listen on Port 81 for non-SSL traffic. However as a result of the WPM installation and configuration, additional lines are placed at the end of httpd.conf which disallow any non-SSL traffic. (This is a security measure to protect against sniffing administrator traffic.) The additional lines which were placed at the end of our configuration file following WPM installation and configuration were as follows:

```
### BEGIN PDWPM CONFIG ENTRY ###
Listen 443
LoadModule ibm_ssl_module libexec/mod_ibm_ssl_128.so
SSLEnable
Keyfile "/var/PolicyDirector/keytab/pdwpm.kdb"
SSLV2Timeout 100
SSLV3Timeout 1000
### END PDWPM CONFIG ENTRY ###
```

b. If you are running WebSEAL on the same machine that you are using to run WPM and want WebSEAL to own ports 80 and 443, IBM HTTP Server and WebSphere must be re-configured as follows:

(a) Edit the HTTP configuration file, httpd.conf, by default found in the

/usr/HTTPServer/conf directory. Locate the port value in the httpd.conf file and change it from Port 80 to a different port number - we had already changed this to Port 81 in an earlier step.

(b) Find the Listen line near the end of the file (added by the WPM configuration). Change the reference to 443 to a different port number - we used 4443:

```
### BEGIN PDWPM CONFIG ENTRY ###
Listen 4443
LoadModule ibm_ssl_module libexec/mod_ibm_ssl_128.so
SSLEnable
Keyfile "/var/PolicyDirector/keytab/pdwpm.kdb"
SSLV2Timeout 100
SSLV3Timeout 1000
#### END PDWPM CONFIG ENTRY ###
```

c. If you want to enable non-SSL traffic (to port 81 in our case), edit httpd.conf, as follows:

```
### BEGIN PDWPM CONFIG ENTRY ###
Listen 4443
LoadModule ibm_ssl_module libexec/mod_ibm_ssl_128.so
<VirtualHost :4443>
SSLEnable
SSLClientAuth none
DocumentRoot /usr/HTTPServer/htdocs/en_US
</VirtualHost>
SSLDisable
Keyfile "/var/PolicyDirector/keytab/pdwpm.kdb"
SSLV2Timeout 100
SSLV3Timeout 1000
### END PDWPM CONFIG ENTRY ###
```

d. Restart the IBM HTTP Server:

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

e. Start WebSphere Application Server by issuing:

/usr/WebSphere/AppServer/bin/startServer.sh -waitAmount 0

Version 1.1 – 30 September, 2002

f. Point a web browser at http://hostname:9090/admin

(http://charon.welwyn.uk.ibm.com:9090/admin in our case). You will be presented with the WebSphere Application Server Administrative Login page. Enter a name to log in (but it doesn't matter what this name is):



- g. Click on 'Submit'.
- h. In the left-hand panel, click on the '+' sign to the left of Virtual Hosts and then click on the '+' sign to the left of default_host. Then click on 'Aliases'. The panel should look like this:

🔆 IBM WebSphere Application Server Admir	histrative Console - Netscap	e.					_ 8 ×
File Edit View Go Communicator Help							
Back Forward Reload Home	🏄 🚵 🛁 Search Netscape Print	🗳 🙆 Security Shop	31 Stop				N
🚺 🦋 Bookmarks Location: http://charor	1.welwyn.uk.ibm.com:9090/admi	in/secure/logon.do				💌 🕐	What's Related
🚺 📫 IBM 🖳 Internet 📩 Lookup 📩 Ne	w&Cool 🖳 RealPlayer						
WebSphere Application Server							IBM.
server-cfg.xml	Console Home	Configuration	Preferences	Save	Exit	Help	00
WebSphere Administrative Domain U Nodes U Virtual Hosts U default_host U default	Aliases The list of one or more DNS +For more information New Delete	aliases by which the virtu	al host is known				
	Host Name			Port			
+ Ag Security				908	0		
🕀 🛅 Resources				944	3		
	□ ± *			80			
	口 助 *			443			
<u>s</u>							
Document: Done						i 🛛 🦀 🦀 🧃	P 🖪 🎸

i. We need to add new aliases, for ports 81 and 4443. First, click on 'New'; a new panel will be displayed. Under 'Properties', add * in the 'Host Name' field and 81 in the 'Port' field:



j. Click on 'OK'. You are returned to the 'Aliases' page, showing the new entry:

erver-cfg.xml	Console Home	Configuration	Preferences	Save	Exit	Help	
WebSphere Administrative Domain	Configuration needs to Plug-in configuration n Plug-in configuration n Plug-in configuration n	: <u>be saved</u> reeds to be regenerated,					
a and a security and a security and a security and a security	The list of one or more Dt	IS aliases by which the virtual h	ost is known				
AS Security	The list of one or more Dr <u>For more information</u> New Delete Host Name	IS aliases by which the virtual h	ost is known	Po	t:		
ag Security	The list of one or more D1 +For more information New Delete Host Name 	IS allases by which the virtual h	ost is known	Po 901	t. 10		
ag security Ag Security ← Resources	The list of one of more Dr •For more information New Delete Host Name • • • • • •	(S aliases by which the virtual h	ost is known	901 901 94	t 10 13		
az ag Ag Security C Resources	The list of one or more D1 +For more information New Delete Host Name B: * B: * B: *	IS all asses by which the virtual h	ost is known	Po 90 94 80	t 10 3		
Ag Security	The list of one or more D • For more information New Delete • Host Name • # • # • # • # • # • # • #	IS allases by which the vidual h	ost is known	Por 901 944 80 443	t 10 13		

- k. Notice the two messages at the top of the right-hand panel. The first says "Configuration needs to be saved" and the second says "Plug-in configuration needs to be regenerated". These operations can be carried out once the second alias has been added.
- I. Click on 'New'; again, a new panel will be displayed. Under 'Properties', add * in the 'Host Name' field and 4443 in the 'Port' field:

Configuration fo as a servlet, JSP default port 80 is <u>For more infor</u>	aliases. An alias is the DNS host name and port r or HTML page). For example, it is the "myhost:80 used. n <mark>ation</mark>	number used by a client to form the URL request for a Web application resource (such 180° portion of http://myhost:8080/servlet/snoop. When no port number is specified, the
Properties		
Host Name:	* *	The IP address, DNS host name with domain name suffix, or just the DNS host name, used by a client to request a Web application resource (such as a serviet, JSP, or HTML page).

m. Click on 'OK'. You are returned to the 'Aliases' page, showing the new entry:

B Configuration needs to be saved		
Aliases		
he list of one or more DNS aliases by which the virtual hos	t is known	
For more information		
New Delete	Port	
	9080	
	9443	
	80	
• B <u>*</u>	443	
□ 點 <u>*</u>	81	
	1778	

n. Click on 'Configuration needs to be saved'. A 'Save Configuration' panel is displayed:

Save Configuration

Save	
Save Configuration File: /usr/WebSphere/AppServer/config/server-cfg.xml	
C Save As Configuration File: //usr/WebSphere/AppServer/config/untitled.xml	

- o. Click on 'OK'. You are returned to the WebSphere Application Server Welcome screen.
- p. You now need to re-generate the Plug-in configuration. In practice the only way that we were able to do this was to point the web browser at

http://hostname:9090/admin/secure/PluginConfig.jsp

(http://charon.welwyn.uk.ibm.com:9090/admin/secure/PluginConfig.jsp in our case):



When settings have changed that affect the communication between an external Web server and the Web container, the plug-in configuration must be regenerated. Click the button below to regenerate the plug-in configuration at this time. Any previous, manual changes to the plug-in configuration file will be lost. <u>For more information</u>...

Generate

q. Click on 'Generate'. After the operation had completed the browser displayed a message: 'This document contained no data'. However examination of

/usr/WebSphere/AppServer/config/plugin-cfg.xml indicated that this was not a problem and the file had been updated with the new port numbers:

r. Stop and start the application server. We did this by using the command prompt:

```
# cd /usr/WebSphere/AppServer/bin
# ./stopServer.sh
WebSphere Application Server, Advanced Single Server Edition V4.0
WebSphere Application Server, Advanced Developer Edition V4.0
WebSphere Application Server, Advanced Edition V4.0
Runtime Utility Program
Copyright (C) IBM Corporation, 1997-2001
WSRU0025I: Loading configuration from file.
WSRU0028I: Using the specified configuration file:
    /usr/WebSphere/AppServer/config/server-cfg.xml
WSRU0029I: The diagnostic host name read as localhost.
WSRU0030I: The diagnostic port was read as 7000.
Stopping server.
The server was successfully stopped.
# /usr/WebSphere/AppServer/bin/startServer.sh -waitAmount 0
WebSphere Application Server, Advanced Single Server Edition V4.0
Application Server Launcher
Copyright (C) IBM Corporation, 2001
The configuration file was defaulted to:
    /usr/WebSphere/AppServer/config/server-cfg.xml
Using the single available node or the localhost node.
Using the single available server.
Will wait indefinitely for launch results.
Initiating server launch.
Loaded domain "WebSphere Administrative Domain".
```

Selected node "charon". Selected server "Default Server". WSPL0065I: Initiated server launch with process id 19874. Time mark: Thursday, May 23, 2002 8:51:16 AM CDT Waiting for the server to be initialized. Time mark: Thursday, May 23, 2002 8:52:28 AM CDT Initialized server. Waiting for applications to be started. Time mark: Thursday, May 23, 2002 9:09:35 AM CDT Started applications. WSPL0057I: The server Default Server is open for e-business. Please review the server log files for additional information. Standard output: /usr/WebSphere/AppServer/logs/default_server_stdout.log Standard error: /usr/WebSphere/AppServer/logs/default_server_stderr.log #

Note the highlighted line: WSPL0057I: The server Default Server is open for ebusiness – this indicates that the application server has started correctly.

Notes on WebSphere Application Server and DB2 Versions

Access Manager is supplied with WebSphere Application Server Advanced Single Server Edition (AEs). Web Portal Manager is supported only with WAS Advanced Single Server Edition, not Advanced Edition (AE). If you try and install WPM with WAS AE the WPM Configuration will fail: you need to use the WAS Console Application Install wizard.

WAS AE Requires DB2 *Enterprise* Edition, whereas DB2 *Personal* Edition is supplied with the version of IBM SecureWay Directory which is shipped with Access Manager.

12.7 Verify Web Portal Manager operation

- a. Ensure that the IBM HTTP Server was restarted after making any updates to httpd.conf.
- b. Start the IBM SecureWay Directory Server (/usr/bin/slapd).
- c. Start the Access Manager Servers (iv start). (You can then display the status of the Access Manager Servers by issuing iv status.)
- d. Point a web browser at http://hostname:9090/admin. You will again be presented with the WebSphere Application Server Administrative Login page.
- e. Enter a userid and click on 'Submit'. You will be presented with the WebSphere Application Server Administrative Console.
- f. You can use this console to verify that WPM is running: in the left-hand panel, click on the '+' sign to the left of Nodes and then click on the '+' sign to the left of your node (in our case charon). Then click on Enterprise Applications:



- g. The Symbol beside Web Portal Manager indicates that the application is running.
- h. Point a web browser at https://hostname:port number/pdadmin (https://charon.welwyn.uk.ibm.com:4443/pdadmin in our case). (Note: you cannot use localhost or * as the host name - you must enter the specific hostname for your machine.)
- i. You will be presented with various 'Name Check' or other security alert windows accept these warnings. The Web Portal Manager sign-in screen will be displayed.
- j. Enter the Access Manager Administrator userid (sec_master) and password (Secure99 in our case):

💥 Access Manag	er Login - Netsi	cape													1	- 8 >
File Edit View (io Communicati	or Help														
🚽 👔	ž 🤹	位	2	m.	4	<u>a</u> .	Ô									N
Back For	vard Reload	Home	Search	Netscape	Print	Security	Shop	Stop						_ @a*) (lasta D	batelo
	s og Lucation	i (mups.//en	alon, weiwy	B Real	.4445/pua	auninzaunzh	anulecogin	sh							W110(31)	relateu
		andb 🔲		Ly freak)	9761											
			[
												.				
												ii •				
			Tiv	Acces	e Manar	ner for e-t	ucinoce									
				Version :	3.9	yei iui e-L	Juanicaa									
			俞							10.	C.F					
			153. 25	12.23	Vag2			Al Tim	and the	13	1					
			002	10	V4Y		l júni ≦		1.2.1	N.S.						
				o o o d				100	1							
				00	-	05		- V -	-	31						
			(itemail)				Land Street									
			Licens	ed Materials -	Property of	of IBM Corp (c) Copyright t	y IBM Corp. a	id other(s)	1999, 200	2.					
			All Hig	nts Reserved.	See produ	ct license for	details.									
				User ID:	sec_m	naster										
				Password		4				10	ain I					
					1	1					<u>.</u>					
A	Docum	ent: Done											=	Julia and		1

k. Click on 'Login':


I. From here you can use the Web Portal Manager to administer Access Manager.

General notes: Refer to the Publications Section on page 240 below for information about where to obtain information about **WebSphere Application Server**.

If you hit problems with IBM HTTP Server try looking at the contents of /usr/HTTPServer/logs, particularly /usr/HTTPServer/logs/error_log.

13. Useful information for Access Manager in the AIX environment

LDAP commands

- 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")

Access Manager commands

a .iv start	Starts pdmgrd, pdacld and webseald
b.iv stop	Stops pdmgrd, pdacld and webseald
C.iv status	Displays status of pdmgrd, pdacld and webseald
d. pdweb start	Starts webseald
e. pdweb stop	Stops webseald
f.pdweb status	Displays status of webseald

Note that pdmgrd will not start if the LDAP Server is not running.

Access Manager 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.

Access Manager log files

- a. /var/PolicyDirector/log/*
- b. /var/pdweb/log/*

AIX commands

- 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

14. 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. Our experience was that in addition to the specific patches required by the Access Manager install (documented in the release notes) that it is advisable to be at a current service level. To this end we applied the latest 'cluster' patch from Sun for Solaris 8 (8_Recommended.zip (71MB)) downloaded from their support site (http://sunsolve.sun.co.uk). The version downloaded included the patches mentioned in the Release Notes dated May 28, 2002.
- 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.

15. Easy Installation Process for Solaris

Access Manager 3.9 provides a quick installation path using shell scripts for UNIX systems such as Solaris. These scripts make it easy to install Access Manager 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, installing all components on a single machine. This is reflected by the components you see reported by each script in turn as we build up the configuration.

15.1 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, GSKit, IBM HTTP Server, IBM SecureWay Directory client and server.

a. Insert the IBM Tivoli Access Manager Base for Solaris Version 3.9 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 Not Installed IBM Global Security Toolkit 5 Not Installed IBM SecureWay Directory Client Not Installed IBM HTTPD Server Not Installed IBM SecureWay Directory Server 3.2 Not Installed

Press ENTER to continue...

- d. The details shown will vary depending on the state of your system. Above you can see the results from our clean system.
- e. Press 'Enter', you will be shown the 'IBM HTTP Server Configuration Options'

Enter the Administration Password:

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

```
IBM HTTP Server Configuration Options
Option
Value
Administration ID
.....root
Administration Password
.....
```

Version 1.1 – 30 September, 2002

3. HTTP Port 80

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

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

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

h. Type 'y' and 'Enter' to begin configuration. Next the IBM SecureWay Directory Configuration Options will be displayed:

```
      IBM SecureWay Directory Server Configuration Options

      Option
      Value

      1. LDAP Administrator ID (DN)
      cn=root

      2. LDAP Administrator Password
      ******

      3. LDAP Host Name
      secureway2

      4. Suffix
      Not Specified

      5. LDAP Server Port
      389

      6. LDAP Server SSL Port
      636

      7. LDAP SSL Keyfile
      /cdrom/pd_solaris_/common/pd_ldapkey.kdb

      8. LDAP SSL Key File Password
      ******

      9. SSL Client Certificate Label
      PDLDAP
```

i. Enter the LDAP Administrator password as prompted (we used Secure99), then re-enter it for confirmation. Next you are the prompted to enter the suffix to be used in the directory, 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.

j. Type **'y'** and **'Enter**' to begin configuration, you will be informed that the SSL Client Keyfile will be 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 ..... Configured [7.1.0.55]

IBM Global Security Toolkit 5 ..... Configured [5.0.4.67]

IBM SecureWay Directory Client ..... Configured [3.2.2.0]

IBM HTTPD Server ..... Configured [1.3.19.0]

IBM SecureWay Directory Server 3.2 ..... Configured [3.2.2.0]

IBM SecureWay Directory Server 3.2

Installation and Configuration is complete.
```

k. This completes the directory and prerequisite installation.

15.2 Access Manager RTE and Policy Server Installation and Configuration

Use the **ezinstall_pdmgr** script to install the AMRTE and AM Policy Server components. This sets up a workstation with the following packages; GSKit, IBM SecureWay Directory client, AMRTE and AM Policy Server.

Before installing the access manager code please ensure you have applied the appropriate Solaris patches for you system as documented to in the latest Access Manager Release Notes (use 'patchadd'). The easy install scripts will check for the presence of these scripts and will fail if they cannot be found.

a. Insert the Tivoli Access Manager Base for Solaris Version 3.9 CD.

- b. At the command prompt type the following:
 - # cd /cdrom/cdrom0
 # ./ezinstall_pdmgr
- c. This will check for any previously installed components and show the following list:

```
IBM Tivoli Access Manager Policy Server
Installation and Configuration
Product Status
IBM Global Security Toolkit 5 ..... Configured [5.0.4.67]
IBM SecureWay Directory Client ..... Configured [3.2.2.0]
Access Manager Runtime .... Not Installed
Access Manager Policy Server .... Not Installed
```

Press ENTER to continue...

- d. The script will check to see the status of the components it is designed to install and configure. As you can see above in our case GSKit and the Directory client where already installed by the previous script (ezinstall_ldap_server).
- e. Press 'Enter' to continue. The Access Manager Runtime Configuration options are displayed as shown below

IBM Tivoli Access Manager Runtime Configuration Options
Option
Value
Configure Using This Registry Type ldap
LDAP Server Hostname Not Specified
LDAP Server Port 389

Enter the LDAP Server Hostname:

f. Enter the fully qualified LDAP Server Hostname as prompted (in our case secureway2.pic.uk.ibm.com) and press 'Enter' IBM Tivoli Access Manager Runtime Configuration Options Option Value 1. Configure Using This Registry Type ldap 2. LDAP Server Hostname secureway2.pic.uk.ibm.com 3. LDAP Server Port 389

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

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

```
IBM Tivoli Access Manager Policy Server Configuration Options
_____
Option
                                     Value
1. LDAP Server Hostname ..... secureway2.pic.uk.ibm.com
2. LDAP Administrator ID (DN) ..... cn=root
3. LDAP Administrator Password ..... ******
4. Security Master Password ..... ******
5. Enable SSL between Policy Server 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 AM Policy Server..... 7135
12. Policy Server SSL Certificate Lifetime ... 365
13. Enable Download of Certificates ..... Not Specified
```

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

- h. 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
- First decide if you want to enable SSL with the LDAP server. We choose not to and typed 'n' and 'Enter'.
- j. You are then prompted for the LDAP Administrator Password (Secure99 in our case)
- k. You are then prompted for the Security Master Password (Secure99 in our case) and asked to reconfirm it.
- I. You are prompted to enter the LDAP DN for the GSO database (o=ibm,c=gb in our case)
- m. You are asked if you want other AM Client machines to download the certificate file (a new feature since 3.8) we answered 'n'. The summary below is now displayed.

```
IBM Tivoli Access Manager Policy Server Configuration Options

Option Value

1. LDAP Server Hostname ...... secureway2.pic.uk.ibm.com

2. LDAP Administrator ID (DN) ..... cn=root

3. LDAP Administrator Password ..... ******

4. Security Master Password ..... ******

5. Enable SSL between Policy Server and LDAP N
```

Version 1.1 – 30 September, 2002

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

n. This completes the minimum required information, you now have the chance to make further changes and begin the configuration. 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.

IBM Tivoli Access Manager Policy Server Installation and Configuration Product Status IBM Global Security Toolkit 5 Configured [5.0.4.67] IBM SecureWay Directory Client Configured [3.2.2.0] Access Manager Runtime Configured [3.9] Access Manager Policy Server Configured [3.9] IBM Tivoli Access Manager Policy Server

Installation and Configuration is complete.

o. This completes the **ezinstall_pdmgr** script. The Access Manager management server should now be installed and working. You can test this out by making use of the '**pdadmin**' interface to administer PD.

15.3 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 v3.2.2, AMRTE and WebSEAL.

a. Insert the IBM Tivoli Access Manager Web Security for Solaris Version 3.9 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:

```
IBM Tivoli Access Manager WebSEAL Server
Installation and Configuration
Product Status
IBM Global Security Toolkit 5 ..... Configured [5.0.4.67]
IBM SecureWay Directory Client ..... Configured [3.2.2.0]
```

Version 1.1 – 30 September, 2002

Access Manager Runtime Configured [3.9] IBM Tivoli Access Manager WebSEAL Server Not Installed

Press ENTER to continue...

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

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

- e. You are asked if you want to enable SSL with the LDAP server (we choose 'n' to keep things simple). Press 'n' and 'Enter'
- 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.

```
IBM Tivoli Access Manager WebSEAL Server
Installation and Configuration
Product Status
IBM Global Security Toolkit 5 ..... Configured [5.0.4.67]
IBM SecureWay Directory Client ..... Configured [3.2.2.0]
Access Manager Runtime ..... Configured [3.9]
IBM Tivoli Access Manager WebSEAL Server .... Configured [Version 3 , Revision 9]
IBM Tivoli Access Manager 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.

15.4 Web Portal Manager Install & Configuration

Use the **ezinstall_pdwpm** script to install the Web Portal Manager (WPM). This sets up a workstation with the following packages; GSKit, IBM SecureWay Directory client v3.2.2, AMRTE, IBM HTTP Server and the WPM itself. Some components may be installed and configured already from previous steps, the script will detect this.

a. Insert the IBM Tivoli Access Manager Web Portal Manager for Solaris Version 3.9 CD.

b. At the command prompt type the following:

cd /cdrom/cdrom0
./ezinstall_pdwpm

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

```
IBM Tivoli Access Manager Web Portal Manager
Installation and Configuration
```

```
Product Status

IBM WebSphere Application Server ...... Not Installed

IBM Global Security Toolkit 5 ..... Configured [5.0.4.67]

IBM SecureWay Directory Client ..... Configured [3.2.2.0]

IBM HTTPD Server ..... Configured [1.3.19.0]

Access Manager Runtime ..... Configured [3.9]

Access Manager Web Portal Manager .... Not Installed

Press ENTER to continue...
```

d. Press 'Enter' to continue; installation of WebSphere Application Server will begin.

During this process we had a number of problems with the easy install script installing WebSphere and then the WebSphere Fixpak.

The initial WebSphere install problem was resolved by reverting to the native installation process. During the native install of WebSphere the install GUI notified us that additional service levels were advised. These were fixes 108940 (which pre-reqs 108714), 108652 &10921 – these were once again downloaded from the SUN support site and applied. We then resumed the easy install script and the install proceeded further. The initial WebSphere install completed ok, the script then failed again during the install of the WebSphere fixpak. We suspect that more fixes may be required to the base Solaris system to proceed further. Unfortunately we did not have time to investigate further for this version of the Cookbook.

16. Access Manager 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 Access Manager 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]:

17. Solaris – Native installation

Note: As described above, easy install scripts are provided for Solaris - these scripts make it easy to install Access Manager by automatically installing required software and prerequisites. The following sections describe the *native* installation processes for Solaris, as there may be situations where the Easy Install scripts are not appropriate or do not work.

17.1 LDAP Server installation/configuration (Solaris)

Note: It is strongly recommended that you read this in conjunction with the *IBM SecureWay Directory Version 3.2.2 for the Solaris Operating Environment Software Installation and Configuration Guide* – this is on the **IBM Tivoli Access Manager Base for Solaris Version 3.9** CD at /doc/Directory/sparent.pdf. There are other SecureWay Directory product manuals in the same directory.

You should also refer to the latest version of the Access Manager Release Notes.

17.2 Operating system pre-requisites

- Apply the latest 'cluster' patch from Sun for Solaris 8 (8_Recommended.zip (71MB)) from their support site (http://sunsolve.sun.co.uk). Ensure that this includes all the patches mentioned in the latest version of the Release Notes.
- Download IBM SecureWay Directory Version 3.2 e-fix 2 (eFix 3.2.2-SWD-002) from <u>http://www.ibm.com/software/network/directory/support/fixes/</u>
- Uninstall any previous LDAP Server or LDAP Client.

17.3 Install DB2

a. Insert the IBM Tivoli Access Manager Base for Solaris Version 3.9 CD.

b. At a command line, type pkgadd -d /cdrom/cdrom0/solaris -a /cdrom/cdrom0/solaris/pddefault \ db2cliv71 db2cucs71 db2rte71 db2crte71 db2engn71 \ db2das71 db2cnvt71 db2cnvk71 db2cnvj71 db2cnvc71 \ db2smpl71 db2conn71 db2cipx71 db2csna71 db2cdrd71 \ db2tspf71 db2elic71 (To avoid typing, you can find this list in /cdrom/cdrom0/ezinstall_ldap_server against DB2 INST LIST.)

c. This should look similar to the following:

```
# pkgadd -d /cdrom/cdrom0/solaris -a /cdrom/cdrom0/solaris/pddefault \
> db2cliv71 db2cucs71 db2rte71 db2crte71 db2engn71 \
> db2das71 db2cnvt71 db2cnvt71 db2cnvj71 db2cnvc71 \
> db2smpl71 db2conr1 db2cipx71 db2csna71 db2cdrd71 \
> db2tspf71 db2elic71
Processing package instance <db2cliv71> from </cdrom/pd_solaris_/solaris>
Client Application Enabler
(sparc) 7.1.0.40
Licensed Materials - Property of IBM
5648-B90
(C) COPYRIGHT International Business Machines Corp. 1993, 1999
....
## Executing postinstall script.
Installation of <db2elic71> was successful.
#
```

17.4 Install DB2 Fix Pack 5

a. Still using the IBM Tivoli Access Manager Base for Solaris Version 3.9 CD.

```
b. At a command line, type
```

cd /cdrom/pd_solaris_/solaris/patches/db2_fixpack_5/delta_install

/cdrom/pd_solaris_/solaris/patches/db2_fixpack_5/delta_install/installallpatch
This should look similar to the following:

```
# cd /cdrom/pd_solaris/solaris/patches/db2 fixpack 5/delta install
# /cdrom/pd_solaris_/solaris/patches/db2_fixpack_5/delta_install/installallpatch
       Do NOT interrupt while installing patch 1720500-005...
INFO:
Installation of <db2cliv71> was successful.
INFO:
      Do NOT interrupt while installing patch 1720500-006...
Installation of <db2conn71> was successful.
      Do NOT interrupt while installing patch 1720500-007...
INFO:
Installation of <db2cdrd71> was successful.
      Do NOT interrupt while installing patch 1720500-008...
INFO:
Installation of <db2cipx71> was successful.
INFO:
      Do NOT interrupt while installing patch 1720500-009...
Installation of <db2crte71> was successful.
INFO: Do NOT interrupt while installing patch 1720500-010...
Installation of <db2csna71> was successful.
INFO:
       Do NOT interrupt while installing patch 1720500-012...
```

```
Installation of <db2das71> was successful.
INFO:
           Do NOT interrupt while installing patch 1720500-013...
Installation of <db2engn71> was successful.
          Do NOT interrupt while installing patch 1720500-014...
INFO
Installation of <db2rte71> was successful.
INFO: Do NOT interrupt while installing patch 1720500-025...
Installation of <db2elic71> was successful.
INFO:
          Do NOT interrupt while installing patch 1720500-059...
Installation of <db2tspf71> was successful.
_____
Summarv
_____
Package
                     Patch ID
                                           Patch Level
                                                                    Result
          _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
                               _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
                                                        -----

        db2tspf71
        1720500-059
        7.1.0.55
        SUCCESS

        db2elic71
        1720500-025
        7.1.0.55
        SUCCESS

        db2rte71
        1720500-014
        7.1.0.55
        SUCCESS

        db2engn71
        1720500-013
        7.1.0.55
        SUCCESS

        db2engn71
        1720500-013
        7.1.0.55
        SUCCESS

        db2das71
        1720500-012
        7.1.0.55
        SUCCESS

        db2csna71
        1720500-010
        7.1.0.55
        SUCCESS

db2crte71
                     1720500-009
                                             7.1.0.55
                                                                    SUCCESS
                     1720500-008
1720500-007
db2cipx71
                                              7.1.0.55
                                                                     SUCCESS
                                                                    SUCCESS
                                             7.1.0.55
db2cdrd71
db2conn71
                                                                    SUCCESS
                     1720500-0067.1.0.551720500-0057.1.0.55
db2cliv71
                                                                      SUCCESS
Log saved in /tmp/db2installallpatch.log.7.1.0.55
#
```

c. If there is not enough disk space available on /var/sadm/patch to save the files to be patched you may need to either free up disk space on /var/sadm/patch or issue the command:

/usr/bin/touch /var/sadm/patch/PATCH_NOSAVE
and re-issue the command to install the patches.

17.5 Update the DB2 License key

- a. Still using the IBM Tivoli Access Manager Base for Solaris Version 3.9 CD.
- b. At a command line, type /opt/IBMdb2/V7.1/adm/db2licm /cdrom/cdrom0/common/db2udbee.lic
- c. This should look similar to the following:

```
# /opt/IBMdb2/V7.1/adm/db2licm /cdrom/cdrom0/common/db2udbee.lic
DBI1402I License added successfully.
#
```

17.6 Install GSKit

Version 1.1 – 30 September, 2002

a. Still using the IBM Tivoli Access Manager Base for Solaris Version 3.9 CD.

b. At a command line, type # pkgadd -d /cdrom/cdrom0/solaris -a /cdrom/cdrom0/solaris/pddefault gsk5bas

c. This should look similar to the following:

```
# pkgadd -d /cdrom/cdrom0/solaris -a /cdrom/cdrom0/solaris/pddefault gsk5bas
Processing package instance <gsk5bas> from </cdrom/pd solaris /solaris>
Certificate and SSL Base Runtime (gsk5bas)
(sparc) 5.0.4.67
IBM
Using </opt> as the package base directory.
## Processing package information.
## Processing system information.
   2 package pathnames are already properly installed.
## Verifying package dependencies.
## Verifying disk space requirements.
Installing Certificate and SSL Base Runtime (gsk5bas) as <gsk5bas>
## Installing part 1 of 1.
/opt/ibm/gsk5/bin/gsk5cmd
/opt/ibm/gsk5/bin/gsk5ikm
/opt/ibm/gsk5/bin/gsk5ver
/usr/lib/libgsk5sys.so <symbolic link>
/usr/lib/libgsk5valn.so <symbolic link>
[ verifying class <none> ]
## Executing postinstall script.
This is an Ultra Series machine.
We are moving appropriate library into place.
Installation of <gsk5bas> was successful.
#
```

17.7 Install the LDAP Client

- a. Still using the IBM Tivoli Access Manager Base for Solaris Version 3.9 CD.
- b. At a command line, type pkgadd -d /cdrom/cdrom0/solaris -a /cdrom/cdrom0/solaris/pddefault IBMldapc

c. This should look similar to the following:

```
# pkgadd -d /cdrom/cdrom0/solaris -a /cdrom/cdrom0/solaris/pddefault IBMldapc
Processing package instance <IBMldapc> from </cdrom/pd_solaris_/solaris>
IBM SecureWay Directory Client
(sparc) 3.2.2.0
5648D1300
IBM SecureWay Directory for Solaris, Version 3.2.2.0
(C) Copyright International Business Machines Corp. 1997,2001.
Copyright (c) 1995,1996 Regents of the University of Michigan.
All rights reserved.
Redistribution and use in source and binary forms are permitted
provided that this notice is preserved and that due credit is given
to the University of Michigan at Ann Arbor. The name of the University
may not be used to endorse or promote products derived from this
```

```
software without specific prior written permission. This software
    is provided ``as is'' without express or implied warranty.
IBM SecureWay Directory client installation directory? (/opt) [?,q]
A non-IBM version of LDAP has been located on your system.
In order to use the command line version of the IBM supplied files,
the existing files (ldapadd, ldapdelete, ldaplist, ldapmodify, ldapmodrdn, ldapsearch
) must be relocated.
Specify the new directory in which to move the files. (/usr/bin/ldapsparc)
 [?,q]
Files will moved to /usr/bin/ldapsparc
## Executing checkinstall script.
Using </opt> as the package base directory.
## Processing package information.
## Processing system information.
WARNING: /usr/bin/ldapadd <no longer a linked file>
WARNING: /usr/bin/ldapdelete <no longer a regular file>
WARNING: /usr/bin/ldapmodify <no longer a regular file>
WARNING: /usr/bin/ldapmodrdn <no longer a regular file>
WARNING: /usr/bin/ldapsearch <no longer a regular file>
## Verifying package dependencies.
## Verifying disk space requirements.
Installing IBM SecureWay Directory Client as <IBMldapc>
## Executing preinstall script.
Adding user ldap
## Installing part 1 of 1.
/etc/dmt.conf <symbolic link>
/etc/ldap.conf
/opt/IBMldapc/bin/dmt
/usr/lib/libldapstatic.a <symbolic link>
/usr/lib/libldif.a <symbolic link>
[ verifying class <none> ]
## Executing postinstall script.
Installation of <IBMldapc> was successful.
#
```

17.8 Install the HTTP Server

Note: The web server is used to enable browser based administration of the LDAP server. If this is not possible or not desired, see the section entitled *If you are unable to run the LDAP Administrative web server or add the Suffixes using the web browser interface...* on page 161 below.

a. Still using the IBM Tivoli Access Manager Base for Solaris Version 3.9 CD.

b. At a command line, type # pkgadd -d /cdrom/cdrom0/solaris -a /cdrom/cdrom0/solaris/pddefault IBMHTTPD IBMHTTPA IBMHSENU IBMHAENU IBMHSLDP IBMHL128 IBMHSSEN

c. This should look similar to the following:

```
# pkgadd -d /cdrom/cdrom0/solaris -a /cdrom/cdrom0/solaris/pddefault IBMHTTPD
IBMHTTPA IBMHSENU IBMHAENU IBMHSLDP IBMHL128 IBMHSSEN
Processing package instance <IBMHTTPD> from </cdrom/pd_solaris_/solaris>
HTTP Server Base Run-Time
(sparc) 1.3.19.0
```

Version 1.1 – 30 September, 2002

```
Licensed Materials - Property of IBM
5648-B78
. . .
. . .
Installation of <IBMHSSEN> was successful.
#
```

- d. By default the IBM HTTP Server listens to port 80, the same as WebSEAL. If you are going to install WebSEAL on the same machine, to avoid port conflicts edit the HTTP configuration file /opt/IBMHTTPD/conf/httpd.conf. Locate the Port value and change it from Port 80 to a different port number we used Port 81.
- e. Start the server by entering the following command: /opt/IBMHTTPD/bin/apachectl start

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

If you get an error message similar to the following:

[alert] httpd: Could not determine the server's fully qualified domain name, using 146.84.122.224 for ServerName

you can correct this by editing /opt/IBMHTTPD/conf/httpd.conf and specifying the fully qualified domain name against the ServerName entry.

f. You can verify that the web server is working by pointing a web browser at http://hostname:port number (http://cross-site-1.uk.tivoli.com:81 in our case) – this should result in the IBM HTTP Server splash screen being displayed.

17.9 Install the LDAP Server

- a. Still using the IBM Tivoli Access Manager Base for Solaris Version 3.9 CD.
- b. At a command line, type pkgadd -d /cdrom/cdrom0/solaris -a /cdrom/cdrom0/solaris/pddefault IBMldaps

c. This should look similar to the following:

```
# pkgadd -d /cdrom/cdrom0/solaris -a /cdrom/cdrom0/solaris/pddefault
IBMldaps
Processing package instance <IBMldaps> from
</cdrom/pd_solaris_/solaris>
IBM SecureWay Directory Server
(sparc) 3.2.2.0
5648D1300
IBM SecureWay Directory for Solaris, Version 3.2.2.0
(C) Copyright International Business Machines Corp. 1997,2001.
Copyright (c) 1995,1996 Regents of the University of Michigan.
All rights reserved.
```

Redistribution and use in source and binary forms are permitted provided that this notice is preserved and that due credit is given to the University of Michigan at Ann Arbor. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission. This software is provided ``as is'' without express or implied warranty. IBM SecureWay Directory server installation directory? (/opt) [?,q] ## Executing checkinstall script. Using </opt> as the package base directory. ## Processing package information. ## Processing system information. 25 package pathnames are already properly installed. ## Verifying package dependencies. ## Verifying disk space requirements. Installing IBM SecureWay Directory Server as <IBMldaps> ## Executing preinstall script. ## Installing part 1 of 1. /etc/ldapschema <symbolic link> /etc/slapd.conf <symbolic link> /var/ldap/SvrStarting.out /var/ldap/SvrStopping.out [verifying class <none>] ## Executing postinstall script. Installation of <IBMldaps> was successful. #

17.10 Download and Install the LDAP e-fix 2

- a. Download IBM SecureWay Directory Version 3.2 e-fix 2 (eFix 3.2.2-SWD-002) from http://www.ibm.com/software/network/directory/support/fixes/
- b. Install the fix as described in the README.

17.11 Check/set the Solaris kernel configuration parameters

a. Set the Solaris kernel configuration parameters, as described in the **Troubleshooting** chapter in the *IBM SecureWay Directory Version 3.2.2 for the Solaris Operating Environment Software Installation and Configuration Guide* – this is on the **IBM Tivoli Access Manager Base for Solaris Version 3.9** CD at /doc/Directory/sparent.pdf. (You can determine the amount of physical memory by issuing prtconf |grep "Memory size".)

b. Issue the reboot command if you changed /etc/system.

17.12 Configure LDAP

- a. At this point it is strongly suggested that you run df to ensure that you have sufficient space in your /export/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 /export/home directory does not already exist, create it by issuing: mkdir /export/home/ldapdb2 chmod a+rwx /export/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 -1 /export/home/ldapdb2 ldapcfg -s ibmhttp -f /opt/IBMHTTPD/conf/httpd.conf
- d. Restart the IBM HTTP Server: /opt/IBMHTTPD/bin/apachectl stop /opt/IBMHTTPD/bin/apachectl start
- e. The output should look similar to the following: [sol29-ldapconfig.op] + [sol30-ldapconfig2.op]

```
# mkdir /home/ldapdb2
# chmod a+rwx /home/ldapdb2
# ldapcfg -u "cn=root" -p Secure99
 Password for administrator DN cn=root has been set.
IBM Directory Configuration complete.
# ldapcfg -l /home/ldapdb2
 Creating the directory DB2 default database.
 This operation may take a few minutes.
Cannot open message catalog file ldapadm.cat.
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:root,ldapdb2
- g. Start the IBM SecureWay Directory Server: /usr/bin/slapd
- h. The output should look similar to the following:

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

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

aupu.2.onee./ubi/bin/biupu //dev/combole 2/di #ndcobcule ibin/bbz belvice

Alternatively, you can use the startup script /cdrom/cdrom0/common/rc.pd_slapd.

k. To determine whether slapd has started, issue: ps -ef|grep slapd

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

17.13 Add Access Manager Suffixes

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



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



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

Directory Server		*****		
Introduction	Sumixes			
Settings General	K Ready			
Performance Transactions Event notification	To add a suffix, enter the d	istinguished na	me of the suff	ix, then click Update
Suffixes Referrals	Suffix DN seclutho	rity=Defau]	t	
🕨 🛄 Sunema	The table below displays su	ffixes defined	to this server.	
Construction				
Security Carlot Replication Database Current state	Current server suffixes	Comment	Remove?	

Click on 'Update'. We found, for some reason, that we received a message stating The DN you entered contains a syntax error, check the values you entered and try again. We therefore followed the procedure described in the section entitled *If you are unable to run the LDAP Administrative web server or add the Suffixes using the web browser interface...* on page 161 below.

SecureWay Directory	y Server Web Admin: cross-site-1 - Netscape	_8
ile Edit View Go Corr Back Forward I	mmunicator Help 3 At en Search Netscape Print Security Shop Stop	N
📲 Bookmarks 🔬	Location: http://cross-site-1.uk.tivoli.com.81.ldap/cgi-bin/ldacgi.exe?Action=Start	👘 "What's Related
🖆 IBM 🖳 Internet	🖆 Lookup 📺 New&Cool 📓 RealPlayer	
Directory Server	Suffixes	0
Introduction	🔗 cross-site-1	
Settings	📢 # The DN you entered contains a syntax error, check the values you entered and try again	
 Performance Transactions Event notification 	To add a suffix, enter the distinguished name of the suffix, then click Update .	
Suffixes Referrals Schema	Suffix DN secAuthority=Default	
C Security	The table below displays suffixes defined to this server	
Current state	Current server suffixes Comment Remove?	
Logs	cn=localhost System suffix	
	Update Reset	
	Related tasks: • General - Edit the port, referral or password encryption settings. • Performance - Change the search limits, and connections settings to enhance performance. • Transactions - Edit rensactions settings for the processing of grouped operations. • Event notification - Edit event notification settings to enable a client to receive notification when the directory tree • Referrals - List, add, and remove referrals for this server. Referrals are an alternate location where directory infor be found • Schema - Edit the validation settings and schema file list loaded at startup.	is modified. rmation may
	Document: Done	<u>ي</u> الم

- d. Alternatively, 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 Access Manager users and Global Sign-On (GSO) data. For example ou=emea, o=ibm, c=gb as shown below. All the Access Manager 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.)

Suffixes charon			0
┥ The list was successful	ly updated. You must <u>restart th</u>	<u>ne server</u> for	this change to take effect.
To add a suffix, enter the d	istinguished name of the sul	fix, then cli	ck Update.
Suffix DN ou=emea, The table below displays su eliminates access to all dire	o=ibm, c=gb ffixes defined to this server ctory data beneath that suff	To remov	e a suffix, select the checkbox and click Update . Removing a suffix the data is not removed from the directory.
Current server suffixes	Comment	Remove?	
cn=localhost	System suffix		
secAuthority=Default	Contains no directory data	Г	
Update Reset	•		

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:

😔 charon							
The list was successfull	y updated. You must <u>restart th</u>	n <u>e server</u> for t	r this change to ta	ake effect.			
Fo add a suffix, enter the di	istinguished name of the suf	fix, then clic	lick Update.				
		_					
Suffix DN							
Suffix DN							
Suffix DN	ffixes defined to this server	. To remove	ve a suffix, sele	ct the chec	kbox and cli	ck Update . R	temoving a suf
Suffix DN	ffixes defined to this server ctory data beneath that suff	. To remove ĩx, however	ve a suffix, sele er the data is no	ct the chec t removed	kbox and cli from the dir	ck Update . R ectory.	temoving a suf
Suffix DN	ffixes defined to this server ctory data beneath that suff Comment	To remove ix, however Remove?	ve a suffix, sele er the data is no 7	ct the chec t removed	kbox and cli from the dir	ck Update . R ectory.	temoving a suf
Suffix DN	ffixes defined to this server ctory data beneath that suff Comment System suffix	. To remove ix, however Remove?	ve a suffix, sele er the data is no ?	ct the chec t removed	kbox and cli from the dir	ck Update . R ectory.	temoving a suf
Suffix DN	ffixes defined to this server ctory data beneath that suff Comment System suffix Contains no directory data	To remove ix, however Remove?	ve a suffix, sele er the data is no ?	ct the chec t removed	kbox and cli from the diri	ck Update . R ectory.	Lemoving a suf

g. Click on the 'restart the server' link at the top of the page. A message stating 'The directory server is starting' is displayed. This restart process can take several minutes. Once complete a message stating 'The directory server is running' will be displayed:



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

Directory Server	General settings	
Introduction	😔 charon	
General	📢 Ready	
Performance Transactions Event notification	Edit the general settings t	for the server, then click Update .
Suffixes	Hostname	charon
 C Schema Security 	Unsecure port	389
Replication Database	Version	IBM SecureWay Directory 3.2
Current state	Password encryption	C None
🖸 Server status	000	C imask
Connections		• crypt
 Callostop Logs Logoff 		C SHA
	Update Reset	

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 or add the Suffixes using the web browser interface...

There have been installations where (for various reasons) it has not been possible to run a web server to perform the LDAP administrative operations, or else error messages have been received when adding the Suffixes using the web interface. In that case an alternative approach is to edit the configuration file manually. The file in question is: /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: ou=emea, o=ibm, c=gb
```

You can specify one-way password encryption by modifying the <code>ibm-slapdPwEncryption</code> line to:

```
Ibm-slapdPwEncryption: crypt
```

17.14 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. Click on Authentication: Simple. Enter the Server name, LDAP administrator DN and password (cross-site-1.uk.tivoli.com, cn=root and Secure99 in our case):

VIBM SecureWay Directory Management Tool			
	Add server		?
	Ready		IBM.
	Connect to directory serve Server name : Idap:// Port : Use SSL : Certificate name : Authentication type : User DN : User password : Keyclass file name : Keyclass file password :	er [cross-site-1.uk.tivoli.com] 388 C None C Simple C SASL External C CRAM MD5. [cn=root] ********	
Add server Delete server Exit		OK Cancel Help	

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 To	pol
📓 Idap://cross-site-1.uk.tivoli.com.389	Introduction
Calintroduction È⊷Cali Server	Ready
Properties Status 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:

- dap://cross-site-1.uk.tivoli.com:389
- 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):

Image: International State Rebind 2 Image: International State Properties ISBM State State ISBM Administration Ready ISBM Belowd ISBM ISBM State State ISBM State ISBM ISBM State <	lE	M SecureWay Directory Management Tool	• 🗆		•
Immoducion Ready IBMa Server Properties IBMa Sector Administration Ready Berker Sector IBMa Control Cases Anonymous Authenticated Direct Cases User ON: Control Cases Direct Cases User ON: Control Cases Direct Vec Sector User ON: Direct Vec Sector Control Cases Direct Vec Control Cases User ON: Direct Vec Control Cases Control Cases	/localhost:389	Rebind	?		
Administration Schema Description Schema Chycet dases Annowmous Annowmous </td <td>uction river Properties Status</td> <td>Ready</td> <td>IBM.</td> <td></td> <td></td>	uction river Properties Status	Ready	IBM.		
Cler Classes Anonymous @ Authendicated User DN: cn=rooc Syntaxes Drecory tree Drecory tree Syntaxes Syntaxes Drecory tree Syntaxes	Administration Rebind thema	Enter a new bind DN and password for the server Idap://localhost.389			
User DN: <u>Cn-roc</u> Directory tree Sector tree Saroth tree Saroth tree CK Cancel Help Concel	Refresh schema Object classes Attributes	Anonymous Authenticated			
Image: Search tree OK Cancel Help Search tree D Senich tree D Senich tree D Advanced search D View log file D View log file	Matching rules Syntaxes irectory tree	User DN : <u>cn=root</u> User password : <u>*********</u>			
E a Smple savch E a Smple savch E to file E a View for file B Olear log file	Browse tree Refresh tree	CK Cancel Help			
La View do file La Clear log file	- D Simple search - D Advanced search				
	g file View log file Clear log file				
Add server Delete server Exit	rver Delete server Exit			ĺ	

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:



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 Access Manager 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.

elect an En	try type, enter the Parent DN, r	modify the Entry R	DN, then click (DK.	
Entry type	Organizational unit 💌				
Parent DN:					
Entry RDN:	ou=emea,o=ibm,c=gb				

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

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

k. If desired you can enter a description, etc. 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:

dap://cross-	site-1.uk.tivoli.com:389	
- 本 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.

18. Access Manager Server installation (Solaris) (Native)

- a. Install GSKit (if not already installed) as described in Section 17.6 on page 151 above.
- b. Install The LDAP Client (if not already installed) as described in Section 17.7 on page 152 above.
- c. Install the Solaris Patches (the latest 'cluster' patch from Sun for Solaris 8 (8_Recommended.zip (71MB)) from their support site (<u>http://sunsolve.sun.co.uk</u>).) Ensure that this includes all the patches mentioned in the latest version of the Release Notes.
- d. Still using the IBM Tivoli Access Manager Base for Solaris Version 3.9 CD.
- e. At a command line, type
 - pkgadd -d /cdrom/cdrom0/solaris -a /cdrom/cdrom0/solaris/pddefault \
 PDRTE PDMgr PDAuthADK PDAcld PDJrte

19. WebSEAL Installation (Solaris) (Native)

- a. Insert the IBM Tivoli Access Manager Web Security for Solaris Version 3.9 CD.
- b. Install GSKit (if not already installed) as described in Section 17.6 on page 151 above.
- c. Install the LDAP Client (if not already installed) as described in Section 17.7 on page 152 above.
- d. Install the Solaris Patches (the latest 'cluster' patch from Sun for Solaris 8 (8_Recommended.zip (71MB)) from their support site (<u>http://sunsolve.sun.co.uk</u>).) Ensure that this includes all the patches mentioned in the latest version of the Release Notes.
- e. If the Policy Director Run Time Environment is not already installed, at a command line, type pkgadd -d /cdrom/cdrom0/solaris -a /cdrom/cdrom0/solaris/pddefault \ PDRTE
- f. At a command line, type
- pkgadd -d /cdrom/cdrom0/solaris -a /cdrom/cdrom0/solaris/pddefault \
 PDWeb

20. Access Manager Configuration (Solaris) (Native)

- a. Ensure that the Directory (and any intervening network) is working correctly. (You can do this by issuing the command ldapsearch -h ldap_server_hostname -D cn=root -w ldap password -b "" -s base objectclass=*)
- b. At the command line, type pdconfig.
- c. The procedure will then be similar to that described in Section 11 Access Manager Configuration (AIX) on page 115 above.
- d. You can now check that Access Manager is working by following the steps described in Section 22 Initial Access Manager Validation on Page 170 below.

21. Useful commands for Access Manager in the Solaris environment

LDAP

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

Directory Management Tool steps

- a. Start the Directory Management Tool. You can do one of the following:
- run the Directory Management Tool on the same AIX box as that on which the directory is located;
- run the Directory Management Tool on a remote system and point it at the AIX box on which the directory is located.
- b. To start the Directory Management Tool on a Solaris XWindows system, type dmt& at the command line.
- c. *If you are accessing the directory from a remote system*, as the Directory Management Tool is starting an error message may be displayed indicating 'An error occurred connecting to server "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 (cross-site-1.uk.tivoli.com, cn=root and Secure99 in our case):

& IBM SecureWay Directory Management Tool				
	Add server	?		
	Ready	IBM.		
	Connect to directory servi Server name : Idap:// Port : Use SSL : Certificate name : Authentication type :: User DN : User password : Keyclass file name : Keyclass file password :	er [charon.emea.tivoli.com] 389 C None C Simple C SASL External C CRAM MD5 C Kerberos [rn=root] *******		
Add server Delete server Exit		OK Cancel Help		

PD

a. /etc/iv start	Starts the PD Servers
b. /etc/iv stop	Stops the PD Servers
c. /etc/iv status	Displays status of PD Servers
d. /etc/pdweb start	Starts WebSEAL
e. /etc/pdweb stop	Stops WebSEAL
f. /etc/pdweb status	Displays status of WebSEAL

Solaris

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

Part V - Generic Product Configuration

22. Initial Access Manager 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):



New Site Certificate			
Certificate for: Signed by: Encryption:	Tivoli Systems Tivoli Systems Medium Grade (DES-CBC with 64-bit secret key)	More Info	
The signer of th who they say th would be for sor you and this we	e Certificate promises you that the holder ey are. The encryption level is an indicati neone to eavesdrop on any information ex o site.	of this Certificate is on of how difficult it changed between	
	<back< td=""><td>Next> Cancel</td></back<>	Next> Cancel	

🔆 New Site Certificate - Netscape
🕒 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=""> Cancel</back>



🔆 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.
<back cancel<="" finish="" td=""></back>
🔆 Certificate Name Check - Netscape

The certificate t contain the corr may be trying to the certificate s with, please car Here is the Certi	hat the site 'charon.emea.tivoli.com' has presented does not ect site name. It is possible, though unlikely, that someone intercept your communication with this site. If you suspect hown below does not belong to the site you are connecting icel the connection and notify the site administrator. ficate that is being presented:
Certificate for: Signed by: Encryption:	IBM IBM Highest Grade (RC4 with 128-bit secret key) More Info
	Cancel Continue

c. You can then log in to the browser Basic Authentication prompt with User Name sec_master and the Access Manager Administrator password (Secure99 in our case):


- d. (Note that the User Name is not case sensitive, but the Password *is* case sensitive.)
- e. Click on '**OK**' you should then be presented with the Access Manager 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:

IBM Tivoli Access Manager 3.9 – Cookbook



Site:	securez.pic.uk.ibm.com
Realm	Access Manager for e-business
<u>U</u> ser Name	sec_master
Password	XXXXXXXX
🔲 <u>S</u> ave this	password in your password list
	OK Cano

? ×

23. Further Access Manager 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 Access Manager banner as before.
- c. Verify that pointing the browser at http://hostname:81/and/or http://hostname:82/ results in the other web server(s) responding.
- d. Ensure that the LDAP Server is started.
- e. You can use the pdadmin command line interface to create a user as follows:

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

- f. Note that the relevant elements of the DN (ou=emea, o=ibm, c=gb in our case) must be consistent with the suffixes previously specified. The password must be consistent with the password rules passw0rd and password1 are consistent with the default password rules, which require at least one numeric character.
- g. You can show the characteristics of the WebSEAL server(s) as follows:

```
pdadmin> server list
  webseald-harperv
  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 junctioned web server is not operating.
- k. The junctions and the characteristics of the junctions can be listed as follows:

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

Version 1.1 – 30 September, 2002

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

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

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

```
Allow Windows-style URLs: no
Total requests : 1
pdadmin>
```

- m. Note: when using query_contents with IIS, you need to specify -q /cgibin/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 Access Manager Web Portal Manager to be used for managing web server contents.

For IBM HTTP Server, do the following:

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

- 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.

WWW Service Properties for harperv Service Directories Longing Advanced
ICP Port. 82
Connection Timeout: 900 seconds Maximum Connections: 100000
Anonymous Logon
Usemame: IUSR_HARPERV
Password:
Password Authentication
Allow Anonymous
☑ Basic (Clear Text)
Windows NT Challenge/Response
Comment:
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 :

Directory:	C:\InetPub\www.r	oot\ogi-pin		Browse.	
C Home Direc	tory 🕍				
— ● ⊻irtual Direc	tory				
Aļias:	/cgi-bin				
	NEMEDICENED				
Virtu <u>a</u> l Servi	91				
	P Address:				
Access					
	ture SSL chennel Miel	Execute			
Enable Clie	nt Certificates 🛛 🗖				
		OK	Cance	l <u>H</u> elp	1
Click o	n 'OK':	arperv			
Click O www.Service Service Dire	n ' OK ': Properties for he ctories Logging / 4	arperv Advanced	Alias	Address	Err
Service Dire	n 'OK': Properties for here ctories Logging / 4 Public Advantage	arperv Advanced	Alias	Address	En
Click O www.service Service Dire Directo Chine Chine	n 'OK': Properties for here ctories Logging / 2 Publyservices Publyservices	arperv Advanced	Alias <home> /Scripts /cripts</home>	Address	Er
Click O www.service Service Dire Directo C.Vine C.Vine C.Vine	n 'OK': Properties for h ctories Logging / ry tPub\wwwroot tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub\scripts tPub tPub\scripts tPub tPub tPub tPub tPub tPub tPub tPub	arperv Indvanced in	Alias <home> /Scripts /cgi-bin /iisadmin</home>	Address	Er
Service Dire Directo CNne CNne CNne CNne CNne CNne CNne	n 'OK': Properties for h Cories Logging # Publywwwroot Publyscripts 4Publywwwroot/cgib NNT/System32/unet	arperv sdvanced sdvanced sdvanced	Alias <home> /Scripts /cgi-bin /iisadmin</home>	Address	Er
Click O	n 'OK': Properties for h ctories Logging / A Publysweroot Publyseripts Publyseripts Publyseriot(spibly) NNT\System32\inet	arperv Advanced in srv\iisadmin	Alias <home> /Scripts /cgi-bin /iisadmin</home>	Address	En
Click O www.service Service Dire Directo CMne CMne CMne CMne CMne	n 'OK': Properties Logging # ry Pub\www.cot HPub\scripts PUb\www.cot\cgib NNT\System32\inet	arperv Advanced	Alias <home> /Scripts /cgi-bin /iisadmin</home>	Address	Err
Click O www.Service Service Dire Directo C.Vine C.Vine C.Vine C.Vine	n 'OK': Properties for h ctories Logging / Publywwwroot Publywwroot Publywwroot Publywwroot Publywwroot NNT System 32 Vinet	arperv Advanced	<mark>Alias</mark> <home> /Scripts /ogi-bin /iisadmin</home>	Address	(Err
Service Dire Service Dire CVIne CVIne CVIne CVIne CVIne	n 'OK': Properties for h ctories Logging & Publywwroot Publywwroot Publywwroot Publywwroot Publywwroot Publywwroot Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charlen Charl	in stviisadmin	Alias «Home» /Scripts /cgi-bin /isadmin	Address	Err
Click O www.service Service Dire Directo	n 'OK': Properties for h ctories Logging / A PU HPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPublxenits PPubl	in stviisadmin dd	Alias (Home> /Scripts /ogi-bin /iisadmin	Address	Ern
Click O WWW Service Service Dire Directo Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline Cline C	n 'OK': Propetties for h ctories Logging / A Publywwwroot Publywwwroot Publywwwroot Publywwwroot Publywwwroot Publywwwroot Cgith NNT System 32 Vinet A A Ie Default Document	arperv Advanced in srv\iisadmin dd	Alias <home> /Scripts /cgi-bin /iisadmin <u>R</u>emove</home>	Address	Err
Click O www.service Service Dire Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine	n 'OK': Properties for hi ctories Lagging / A ry Pub/www.root Pub/www.root/cgi-b NNT/System32/inet A be Default Document coument: Def	arperv kdvanced in srvViisadmin dd	Alias <home> /Scripts /ogi-bin /iisadmin Eemove</home>	Address	En
Click O WW Service Service Dire CVIce CVIce CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICe CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CVICE CV	n 'OK': Properties for h ctories Logging / A Publywwroot APublywwroot APublyweroot/cgi-b Publywwroot/cgi-b Publywwroot/cgi-b RNT/System32/inet A e Default Document ocument: Def	atperv xdvanced in srv/iisadmin dd	Alias <home> /Scriptbin /iisadmin <u>Remove</u></home>	Address	Err
Service Dire Service Dire Directo CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CVine CV	You Constant Con	aiperv kdvanced in srv\iisadmin dd ault.htm d	Alias <home> /Scripts /isadmin /isadmin</home>	Address	Es
Click O www.service Service Dire Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chine Chi	You Constant Con	atperv sdvanced in sr\lisadmin dd	Atias <home> /Scipts /isadmin /isadmin</home>	Address	Err

I) Click on '**OK**.

k)

- m) Click on Properties -> Stop Service in Internet Service Manager to stop IIS.
- n) Click on Properties -> Start Service to re-start IIS.
- o) Ideally obtain a copy of query_contents.exe written specifically to cope with the virtual directories which IIS and Netscape support.

copy query_contents.exe to c:\InetPub\wwwroot\cgi-bin\.
copy query_contents.cfg to c:\winnt\.;
edit query contents.cfg to contain the following:

[server]
docroot=C:\InetPub\wwwroot
[directories]
/iisadmin=c:\winnt\system32\ietsrv\iisadmin

p) Failing that, copy the WebSEAL query_contents.* files from the Access Manager directory to the appropriate directories:

COPY c:\Program Files\Tivoli\PDWeb\www\lib\query_contents\query_contents.exe

```
to c:\InetPub\wwwroot\cgi-bin\.
COPY c:\Program Files\Tivoli\PDWeb\www\lib\query_contents\query_contents.cfg
to c:\winnt\.;
        edit c:\winnt\query_contents.cfg to specify
docroot=c:\inetpub\wwwroot
```

q. Test query_contents.exe from a DOS window:

```
C:\>c:\inetpub\wwwroot\cgi-bin\query_contents.exe dirlist=/
Content-type: text/plain
100
cgi-bin//
default.htm
samples//
iisadmin//
C:\>
```

- r. (The line containing iisadmin will not be present when using the default query_contents.exe.)
- s. Test query_contents.exe from the browser:



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

t. 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 line to start the Directory Management Tool.
- Either click on Add Server, then enter the server name, the LDAP Administrator User DN and password, or else click on Rebind, click on Authenticated, and enter the LDAP Administrator User DN and password (cn=root, Secure99 in our case).
- Click on Directory tree -> Browse tree.

IBM Tivoli Access Manager 3.9 – Cookbook

- Click on the '+' sign beside your organization entry (ou=emea, o=ibm, c=gb in our case).
- The user should be listed (cn=testuser in our case).

24. 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 <code>QUERY_STRING</code>. For example, type the following at a command prompt:

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

25. 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:

- a. generating a self-signed certificate;
- b. sending a Certificate Signing Request to a Tivoli PKI system;
- c. 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 Access Manager WebSEAL. In UNIX issue pdweb stop.)
- c. Start the iKeyman utility: In Windows use 'My Computer' or 'Windows Explorer' find the C:\Program Files\IBM\gsk5\bin directory and double click on gsk5ikm.exe. On UNIX type /usr/bin/gsk5ikm& (You may first need to type export JAVA_HOME=/usr/jdk_base) The IBM Key Management window appears:

IBM Key Management	
eyDatabase File Create View Help	
Key database informa DB-Type: IIIe Name:	dion -
Key database conte	nt
Personal Certificates	Receive
	Delete
	View/Edit
	Import
	Recreate Request
	New Self-Signed
	Extract Certificate
nersonal 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:



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

Î.	The password has been encrypted and saved in file: C:\Program Files\Tivoli\PDWeb\www\certs\mypdsrv.sth
	ОК

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

Key database information		
rey unables mithination		
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
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 3 CA Individual Subscriber-Persona Not Validated		
Verisign Class 1 Public Primary Certification Authority		
Verisign Class 2 Public Primary Certification Authority		

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.)

Keylahel		test-webseal-cert
Ney Laber		
version		X509 V3 V
fey 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
		Networks and Reported

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

BM Key Management - [C:\Program Files\Tivoli\PD\Veb\www\certs\mypdsrv.kdb] Database File Create View Help	
Key database information	
Type: CMS key database file	
Name: C:Program Files/Tivol/PDWeb/www/certs/mypdsrv.kdb	
Key database content	
er sonal Certificates 🔹 👻	Receive
lest-webseal-cert	Delete
	View/Edit
	Export/Import
	Recreate Request
List of personal certificates. Default indicated v	vith *
	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>

- n. Start WebSEAL. (In Windows, start Access Manager WebSEAL. In UNIX issue pdweb start)
- Ensure that all the Access Manager services/process have started. If they do not all start, look in the log for the corresponding service/process.
- p. Verify that Access Manager 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 Access Manager WebSEAL. In UNIX issue pdweb stop.)
- c. Start the iKeyman utility: In Windows use 'My Computer' or 'Windows Explorer' find the C:\Program Files\IBM\gsk5\bin directory and double click on gsk5ikm.exe. On UNIX type /usr/bin/gsk5ikm& (You may first need to type export JAVA HOME=/usr/jdk base) 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 • View/Edit..

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 Self-Signed.

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:

IBM Tivoli Access Manager 3.9 – Cookbook

Password:	*****
Confirm Password:	****
Set expiration time?	60 Days
🗹 Stash the pa	ssword to a file?
issword 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 content Key database content idigner Certificates Add hawte Personal Premium CA hawte Personal Premium CA hawte Personal Premium CA hawte Personal Basic CA hawte Personal Basic CA hawte Personal Basic CA hawte Server CA extract SA Secure Server Certificate arisign Class 1 CA Individual Subscriber-Persona Not Validated arisign Class 3 CA Individual Subscriber-Persona Not Validated arisign Class 3 CA Individual Subscriber-Persona Not Validated arisign Class 1 L Public Primary Certification Authority	B-Type: CMS key database file		
iigner Certificates Add hawke Personal Freemail CA Delete hawke Personal Freemail CA Delete hawke Personal Basic CA View.Ædit hawke Server CA View.Ædit hawke Server CA Extract SA Secure Server Certification Authority Filisign Class 1 CA Individual Subscriber-Persona Not Validated sriSign Class 1 CA Individual Subscriber-Persona Not Validated Stract sriSign Class 1 CA Individual Subscriber-Persona Not Validated Stract	New Marrie: C. 4-rogram - nest nonin- by edwywydderstrypdsty, Kob Key database content		
hawte Personal Premium CA hawte Personal Freemail CA hawte Personal Basic CA hawte Personal Basic CA hawte Personal Basic CA hawte Server CA andre Server CA andre Server CA andre Server CA SA Secure Server Certificate SA Secure Server Certification Authority erisign Class 2 CA Individual Subscriber-Persona Not Validated eriSign Class 3 CA Individual Subscriber-Persona Not Validated erisign Class 3 CA Individual Subscriber-Persona Not Validated erisign Class 1 L Public Primary Certification Authority erisign Class 1 L Public Primary Certification Authority	Signer Certificates	•	Add
hawde Personal Freemail CA hawde Personal Basic CA hawde Personal Basic CA hawde Permium Server CA nawde Server CA Trisign Test CA Root Certificate SA Secure Server Certification Authority ariSign Class 1 CA Individual Subscriber-Persona Not Validated ariSign Class 3 CA Individual Subscriber-Persona Not Validated ariSign Class 1 Lpublic Pinawa Certification Authority	Fhawte Personal Premium CA		Delete
hawle Server CA arisign Test CA Root Certificate SA Secure Server Certification Authority ariSign Class 1 CA Individual Subscriber-Persona Not Validated ariSign Class 3 CA Individual Subscriber-Persona Not Validated ariSign Class 3 CA Individual Subscriber-Persona Not Validated ariSign Class 1 Lublic Primary Certification Authority	Thawte Personal Freemail CA Fhawte Personal Basic CA Thawte Personal Basic CA		View/Edit
erisign Class 1 CA Root Certificate SA Secure Server Certification Authority riSign Class 1 CA Individual Subscriber-Persona Not Validated riSign Class 2 CA Individual Subscriber-Persona Not Validated riSign Class 3 CA Individual Subscriber-Persona Not Validated riSign Class 1 Lublic Finance Certification Authority	Fhawte Server CA		Extract
en Secure Server Certaincation Automn enSign Class 1 CA Individual Subscriber-Persona Not Validated enSign Class 3 CA Individual Subscriber-Persona Not Validated enSign Class 3 CA Individual Subscriber-Persona Not Validated ensign Class 1 Public Primary Certification Authority	/erisign Test CA Root Certificate		1
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	veriSion Class 1 CA Individual Subscriber-Persona Not Validated		
eriSign Class 3 CA Individual Subscriber-Persona Not Validated	/eriSign Class 2 CA Individual Subscriber-Persona Not Validated		
erision Class 1 Public Primary Certification Authority	/eriSign Class 3 CA Individual Subscriber-Persona Not Validated		
and gri ender i i dener innarij e eneredateri denerij	/erisign Class 1 Public Primary Certification Authority		
erisign Class 2 Public Primary Certification Authority	/erision Class 2 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.)

IBM Tivoli Access Manager 3.9 – Cookbook

Court shall		test uphasel sort	
vey Label		lest-webseal-cen	
Key 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
			11

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

Informatio	n
Î	A new certificate request has been successfully created in the file: C3Program FilesTfixoINPDWebtwwwkcertstmypdswcertreq.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:

Credential Central
And any strate output of the second sec
Before enrolling for any certificate, you must first <u>install our server's Certificate Authority</u> (CA) certificate in your browser. This certificate enables your browser to connect to the enrollment facility in a secure, authenticated session.
After the CA certificate is installed in your browser, you can enroll for a certificate or request certificate preregistration. If eligible, you can renew, revoke, or suspend an existing browser certificate. From this page, you can also check the status of a pending request.
1. Select the Enrollment Type:
 Browser Certificate for Netscape Communicator or Navigator 4.05 or later, and Microsoft Internet Explorer 5.0 or later.
 Server or Device Certificate. Typically requested only by system administrators, enrollment for these requires a server or device that generates a PKCS #10 certificate request and accepts a raw or PKCS #7 certificate saved in Base64-encoded or binary format.
 Certificate Preregistration to preregister an applicant for a certificate. After the certificate preregistration request is approved, the Trust Authonity Client (or other PKIX compatible client) can be used to download the certificate.
Select an option from the Action list. Renew, Revoke, and Suspend apply only to browser certificates.
3. Click OK to continue.
Certificate Enrollment
Enrollment Type: Server or Device Certificate 💌
Action: Enroll CK

- 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 Cerl	rtificate Enrollment Form - Netscape	_ 8 ×
$\underline{F}ile \underline{E}dit \underline{V}iew \underline{G}o \underline{C}omn$	municator <u>H</u> elp	
Back Forward Re	诸 🏠 🧀 🤖 🐴 🔞 👔	Ν
💈 ॳ Bookmarks 🙏 Lo	.ocation: https://demota.dfw.ibm.com/YourDomain/PKCS107Cert_ErrolLjsp	🔹 🍘 What's Related
	Tivoli PKI	<u>*</u>
	Server and Device Certificate	
	To request a certificate for a server or device that generates a PKCS #10 certificate request and accepts a raw or PKCS #7 certificate in response:	_
	 Complete both parts of the enrollment form All fields are case-sensitive. Click Submit Enrollment Request. 	
	After you submit the form, you will receive instructions for checking the status of your request. If your request is approved, your certificate will be displayed on-screen. Copy and save the certificate response to a file, and then follow your server's instructions to install the certificate.	
	Registration Information	
	Select the type of certificate you need (see description). Select the 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 aver the CA certificate to a file and installing the server or the device prior to installing the server or device certificate.	x
S	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:

	۲K	J	
V130		Server and Device Co	ertificat
To request a certificate for a serv and accepts a raw or PKCS #7	ver or de certificat	vice that generates a PKCS #10 certificate rec ie in response:	quest
1. Complete both parts of th	e enrolln	nent form. All fields are case-sensitive.	
2. Click Submit Enrollmen	t Reque	st.	
After you submit the form, you w request. If your request is appro- save the certificate response to a certificate.	viii recen ved, you i file, and	re mistucions for checking the status of your r certificate will be displayed on-screen. Copy then follow your server's instructions to install	and the
Registration Information			
Select the type of certificate you nee description).	d (see	Type of Certificate: (Required) Web Server Authentication (1-Year)	
If this is the first time that you are requesting server or device enrolliner need to save the CA certificate to a fi install it in your server or the device ; installing the server or device certific	nt, you ile and prior to ate.	Save CA Certificate to File	
Type your first name or given name a optionally, your middle name or initia	and, il.	First Name: (Required) Vaughan	
Type your last name, family name, or sumame.		Last Name: (Required) Harper	
Type your e-mail address, including sign (@) and any periods (). This e- address is required by some certificat types, such as those used for secure	the at nail te e-mail	E-mail Address: (Optional)	
Select this option to receive an e-mai notification when your request has b finalized.	l ieen	E-mail Notification (Optional)	
Type a Challenge Question and a Re that are special to you and easy to	sponse	Challenge Question: (Optional)	
remember. If you are asked the same Challenge Question when you check enrollment status, you must respond the same Challenge Response.	your with	Challenge Response: (Optional)	_
· ·			3
Certificate Request Informati	ion		
Copy and pasts here the content of the PKCS #10 certificate equest (see sample) that was generated by the server or device for which you are equesting a certificate. If you are equesting a certificate request to a file, open the file in a test editor nuch as Notepad, and then copy and patter the certificate request here.	HIIB VQQD A4GN CSZK KtVI 0ÅAW 8NXt 13XN NZJ1 	# D CERTIFICATE REQUEST OFGAUAG #EGGIN NEV CERTIFICATE RECUEST TCEGVUEADBCNQswCCTVVQCCEVJRQJEPHAD KLOVXWCZXLALALDHAHGBSISLAGSSANDAU ADCELOREGOCZICZIVMCCNMCHAUPHT77C0439R ADCELOREGOCZICZIVMCCNMGHUTCTCCVGGLALBAURSH DOVXWCZINACAGEBOADTESLAGSVADCU DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVASPOCT DOVXWCZINACAGEBOADTESLAGVAST DOVXWCZINACAGEBOADTESLAGVAST DOVXWCZINACAGE	G t b b V N
The data you enter below will overrid field blank if you already entered the	le the dat: : data in y	a contained in the PKCS #10 for the same field. Leav our PKCS #10 request and do not wish to override it	re the t.
Type a name to identify this certificate. Typically this is the hostname of your server or device. This field is required if the FKCS #10 certificate request does not contain the Common Name.	Comm	on Name: (Optimal)	
Type the legally registered name of your organization.	Organ	ization Name: (Optional)	
Type the name of your division or department, such as Human Resources or Software Development.	Organ	izational Unit: (Optimal)	
Type the street address of your organization.	Street	Address: (Optional)	
Type the city or municipality where your organization is located, such as Chicago or Paris.	Locali	y: (Optional)	
Type the state or province where your organization is located. Do not abbreviate. For example, use	State o	r Province: (Optional)	
New York instead of NY.	Count	y: (Optional)	-
New York instead of NY. Select the country where your organization is located.	Use t	he one set in PKCS #10	

- 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 en	urollment request has been appr	roved and your certificate is as follows:
11101 3478 34740 47000 42000 42000 42000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 40000 4000000	DCC Am2 gAv I B Ag I C A 2 I wDQY J VW B A D FV I v4 XI gT 3 J HV 5 per (6 A 2 B Ay IV 5 A HI T F A I H I H M O H J S J B J U X H H 4 H T F A I H H M O H J S J B J U X H H 4 H T F A I H H M O H J S J B J U X H H 4 H T F A I H H M O H J S J S J U X H 4 H T F A I H H M O H J S J S J S J S J S J S J S J S J S J S J S J	Ko ZINVCNAQEFBQAWYDELMAKGA1UEBhNCVVNXG mFOA89uHRqwfqTDVQQLEw9UGNVdGCBGLKAb3 FIGAbxcnloESBD(TAF4'040TX31'UXHR4HTF wCQTDVQGEw1HG)ETHBECGm3Jomf5xkARKT AZ 1bTESHRAGCGm3Jomf5xkARKTANVFNF RowFQYKCZIniZFyLGOGGRHMGFycGVyGJBPHA GLEW9GLVAGEBGLKAb3JgHKx1JAgBQNVBAH bJS5jb2Cuq2BsUQCYR6ZTNvCNAQEBBQADqYOA 9511100KhjaGQuQCppeefCYGyEF7FALJHqt2 fai3+1D06go1BS/GFPD0c053DcAHgq1UNRH4 FEvG8DMB7Do1TNAUSSA/ABHSACTAHHAUC EDAKBgqrBgEFBCcDATAGBGNVHSAECTAHHAUC S80ewFVYDVGJBAwcCAIRORSMAb5GUPCVYK kZEqh71LJubWjQYPc4SCp9BGm62C0SRgD1rHE
To insta server a instructi machine server's	Il this certificate to your server, md click Save Certificate to 1 ons provided by your server's is also your server, you should instructions to install the certific	, first select the certificate format required by your Disk. Then import the file to your server by following certificate and key management program. If this d still save the file as a backup and then follow your cate.
Certifica	ite File Format:	
C B C B C B C B C B C B C B	ase64-Encoded PKCS #7 Certificatu ase64-Encoded PKCS #7 Certificatu ase64-Encoded Raw Certificate for ase64-Encoded Raw Certificate for inary PKCS #7 Certificate inary Raw Certificate	e for PC (CRLF) e for UNIX (LF only) <u>PC (CRLF)</u> UNIX (LF only)
	Construction of Dist.	Detuge to Opposited Control

- 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:

Key database content Signer Certificates Add Delete Thawte Personal Premium CA Thawte Personal Premium CA Thawte Personal Preemail CA Thawte Personal Basic CA Thawte Personal Basic CA Thawte Server CA View/Edit Extract View/Edit Extract View/Edit View/Edit Extract View/Edit Thawte Server Ca View/Edit	Key database information B-Type: CMS key database file	
Signer Certificates	ile Name: C:\Program Files\Tivoli\PDWeb\www\certs\mypdsrv.kdb Key database content	
Thawte Personal Premium CA Thawte Personal Breemail CA Thawte Personal Basic CA Thawte Personal Basic CA Thawte Personal Basic CA Thawte Server CA Verisign Test CA Root Certificate RSA Secure Server CA Verisign Class 1 CA Individual Subscriber-Persona Not Validated VeriSign Class 2 CA Individual Subscriber-Persona Not Validated VeriSign Class 3 Public Primary Certification Authority Verisign Class 3 Public Primary Certification Authority Verisign Class 3 Public Primary Certification Authority	Signer Certificates	▼ Add
Inavite Personal Basic CA Thavite Personal Basic CA Thave Personal Basic CA Thave Personal Basic CA Thave Server CA View/Edit Extract Extract Extract View/Edit. Extract	Thavte Personal Premium CA	Delete
Thavite 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 3 CA Individual Subscriber-Persona Not Validated Verisign Class 1 Public Primary Certification Authority Verisign Class 3 Public Primary Certification Authority Verisign Class 3 Public Primary Certification Authority	Thavite Personal Basic CA Thavite Personal Basic CA Thavite Personal Basic CA	View/Edit
RBA 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 3 CA Unblic Primary Certification Authority Verisign Class 3 Public Primary Certification Authority Verisign Class 3 Public Primary Certification Authority	Verisign Test CA Root Certificate	Extract
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	RSA Secure Server Centification Authontly 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 3 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 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	oli\PDWeb\www\certs\CACertRaw.b64 in	our case
Data type	Base64-encoded ASCII data 🔻	
Certificate file name:	CACertRaw.b64	Browse
Location:	C:\Program Files\Tivol\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: C1Program Files\TivoliPDWeb\wwwAcerts\mypdsv.kdb Key database content Signer Certificates Voli PKI Demo System CA Certificate	▼ Add
B-Type: CMS key database tile Ie Name: C1Program Files\TivoliRPDWeb\www\certs\trypdsrv.kdb Key database content Signer Certificates Tvoli PKI Demo System CA Certificate	▼ Add
Ie Name: C:\Program Files\Tivoli\PDWeb\www\certs\mypdsn:kdb Key database content Signer Certificates Tvoli PKI Demo System CA Certificate	▼ Add
Key database content Signer Certificates Tvoli PKI Demo System CA Certificate	➡ Add
Signer Certificates Ivoli PKI Demo System CA Certificate	▼ Add
Tivoli PKI Demo System CA Certificate	
	Delete
Thawte Personal Premium CA	1
Thawte Personal Freemail CA	View/Ed
Thawte Personal Basic CA	
Fhawte Premium Server CA	Extract
Thawte Server CA	1
/erisign Test CA Root Certificate	
RSA Secure Server Certification Authority	
/eriSign Class 1 CA Individual Subscriber-Persona Not Validated	
(ariQian Clace 2 C8 Individual Rubeeriber Bereena Not) (alidated	
enaigh class 2 CA individual ausscribel-Persona Not validated	
/eriSign Class 2 CA Individual Subscriber-Persona Not Validated	
Verligin Class 3 OA Individual Subscriber-Persona Not Validated Verligin Class 1 OA Individual Subscriber-Persona Not Validated Verligin Class 1 Public Primary Certification Authority	
VerlSign Class 3 CA Individual Subscriber-Persona Not Validated /erisign Class 1 Public Primary Certification Authority /erisign Class 2 Public Primary Certification Authority	

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

Key database information	
Type: CMS key database file	
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
	non con cagnetia
	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	

Version 1.1 – 30 September, 2002

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 (*).)

M Key Management - USYProgram Filest I rookYPDWebtwwwtcertstmypdsrv.kdb) Database File Create View Help	
Key database information Type: CMS key database file Name: C19percem ElectTwoldEDWabbaseAcadelmanders kith	
Key database content	
ersonal Certificates 🔹	Receive
test-webseal-cert	Delete
	View/Edit
	Export/Import
List of personal certificates. Default indicated w	Recreate Request
	New Self-Signed
	1

	Error Message X A database validation error occurred. OK	
Note : If you receive an Error	Message indicating 'A database	validation error occurred', this is
likely to be because GSKit wil	I allow the reception only of Person	onal 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	t this error message.

- cc. The IBM Key Management utility is no longer required and may be closed.
- dd. Back up webseald.conf (Windows: in C:\Program Files\Tivoli\PDWeb\etc; UNIX: in /opt/pdweb/etc).

ee. Edit webseald.conf:

modify the webseal-cert-keyfile line to point to the key database file (mypdsrv.kdb in our case);

modify the webseal-cert-keyfile-stash line to point to the key database password stash
file (mypdsrv.sth in our case);

specify the key label by introducing a line in the [ssl] stanza of the following form: webseal-cert-keyfile-label = test-webseal-cert

ff. On UNIX, after creating the key database file, change the file ownership of the key database file and stash file to **ivmgr**. Use the appropriate operating system command for changing file ownership:

chown ivmgr <keyfile>

chown ivmgr <stashfile>

- gg. Start WebSEAL. (In Windows, start Access Manager WebSEAL. In UNIX issue pdweb start)
- hh. Ensure that all the Access Manager services/process have started. If they do not all start, look in the log for the corresponding service/process.
- ii. Verify that Access Manager 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 Access Manager WebSEAL. In UNIX issue pdweb stop.)
- c. Start the iKeyman utility:

In Windows use 'My Computer' or 'Windows Explorer' find the C:\Program Files\IBM\gsk5\bin directory and double click on gsk5ikm.exe. On UNIX type /usr/bin/gsk5ikm&

IBM Key Management y Database File Create View Help	
Key database info	rmation
B-Type:	
le Name:	
Key database c	entent
ersonal Certificates	Receive
	Delete
	Delete ViewEdit
	Delete View.Em Import
	Delete View/Edit Import Recreate Request
	Delete View.Edit] Import Recreate Request
	Delete View.Edit Import Rocreate Request
	Delete ViewEint Import Recreate Request
	Delete View/Edit] Import Rocreate Request New Self-Signed

(You may first need to type export JAVA_HOME=/usr/jdk_base) The IBM Key Management window appears:

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		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:

IBM Tivoli Access Manager 3.9 – Cookbook

Pa	assword:	*****		
Confirm Pa	assword:	******		
🗌 Set expiratio	n time?	60	Days	
⊮ St	ash the pa	ssword to a	file?	
☑ St	ash the pa th:	ssword to a	ı file?	
≥ St ssword Streng	ash the pa th:	ssword to a	ı file?	
≥ St assword Streng	ash the pa th:	ssword to a	n file?	<u>}</u>

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:

Ile Name: C\Program Files\Tivoli\PDWeb\www\certs\trypdsv.kdb Key database content Signer Certificates Add Thawte Personal Premium CA Thawte Personal Breemail CA Thawte Personal Breemail CA Thawte Personal Bracic CA Thawte Personal Bracic CA Chawte Server CA Thawte Server CA Chawte Server CA Chards Server CA	B-Type: CMS key database file		
Key database content Signer Certificates Add Dhawte Personal Premium CA Delete Thawte Personal Basic CA Thawte Personal Basic CA Thawte Premium Server CA Thawte Server CA Versign Test CA Root Certificate Extract RSA Secure Server Certification Authority Extract Versign Class 1 CA Individual Subscriber-Persona Not Validated /erisign Class 3 CA Individual Subscriber-Persona Not Validated Versign Class 3 CA Individual Subscriber-Persona Not Validated /erisign Class 3 CA Individual Subscriber-Persona Not Validated Versign Class 3 CA Individual Subscriber-Persona Not Validated /erisign Class 3 CA Individual Subscriber-Persona Not Validated Versign Class 3 Public Primary Certification Authority /erisign Class 3 Ca Unitie Primary Certification Authority	Ile Name: C:\Program Files\Tivoli\PDWeb\www\certs\mypdsrv.kdb		
Signer Certificates Add Thawte Personal Premium CA Thawte Personal Freemail CA Thawte Personal Basic CA Thawte Personal Basic CA Thawte Premium Server CA Thawte Server CA View/Edit Delete View/Edit View/Edit Finame Server CA Extract Versign Class 1 CA Root Certificate Extract RSA Secure Server Certification Authority Extract Versign Class 2 CA Individual Subscriber-Persona Not Validated /erisign Class 3 CA Individual Subscriber-Persona Not Validated /erisign Class 3 CA Individual Subscriber-Persona Not Validated /erisign Class 3 CA Individual Subscriber-Persona Not Validated /erisign Class 3 CA Individual Subscriber-Persona Not Validated /erisign Class 3 CA Individual Subscriber-Persona Not Validated /erisign Class 3 Public Primary Certification Authority /erisign Class 3 Chilbir Primary Certification Authority	Key database content		
Thavte Personal Premium CA Thavte Personal Premium CA Thavte Personal Breemail CA Thavte Personal Basic CA Thavte Personal Basic CA Thavte Personal Basic CA Thavte Server CA Thavte Server CA View/Edit Extract Extract Extract Extract	Signer Certificates		Add
Interve Personal Basic CA Thavke Personal Basic CA Thavke Premium Server CA Thavke Server CA View/Edit SA 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	Thawte Personal Premium CA		Delete
Thawle Server CA Verisign Test CA Root Certificate SSA 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 3 Public Primary Certification Authority Verisign Class 3 Public Primary Certification Authority	Inawle Personal Basic CA Thawle Personal Basic CA Thawle Permium Server CA		View/Edit
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 /erisign Class 2 Public Primary Certification Authority	Thawle Server CA Verisign Test CA Root Certificate RSA Secure Server Certification Authority VeriSign Class 1 CA Individual Subscriber-Persona Not Validated	[Extract
Verisign Class 2 Public Primary Certification Authority Verision Class 3 Public Primary Certification Authority	/eriSign Class 2 CA Individual Subscriber-Persona Not Validated /eriSign Class 3 CA Individual Subscriber-Persona Not Validated /erisian Class 1 Public Primary Certification Authority		
renoigh olass of able finitual of Adlicity	Verisign Class 2 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.)

IBM Tivoli Access Manager 3.9 – Cookbook

		les et al a second			
vey Label		test-wei	oseal-cen		
(ey Size		1024	-		
Common Name		harperv	welwyn.uk.ib	m.com	
Organization		Tivoli			
Organization Unit (optional)				
ocality (optional)				
State/Province (optional)				
lipcode (optional)				
Country		GB 💌	-		
-			-10		
Enter the name of a	file in whi	ch to sto	re the certifi	cate request:	
C:\Program Files\Ti	ivoli\PDWe	biwww.c	erts\mypdsrv	certreq.arm	Browse
					14

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:

<u>File E</u> dit ⊻iew <u>G</u> o <u>C</u> on	nmunicator <u>H</u> elp		
Back Forward I	🖪 🏦 🗻 🚵 🕯 Reload Home Search Netscape Print Sei	🖍 🙆 📲 curity Shap Stop	N
🛛 🌿 Bookmarks 🙏	Netsite: http://freecerts.entrust.com/webcerts/index.htm		💌 🌍 🖤 What's Related
CONTACT US VISIT WWW.EN Powered by Enbury' In REQUEST A KEB REQUEST REQUEST REQUEST A KEB REQUEST REQ	In the second s	Retrieve the <u>CA Contribute</u> Read more about Web Security Etimar: Web certificates are insued by <u>EntrandWideEconnectual Consecurity Etimare Consecurity Consecurity Consecurity </u>	
	Such as Java Appress Simply click on a request located on the sidebart to get started. What is a Certificate? A certificate an also include when information in extense comments: A*CA* is most for Certification address party (such as a beine flow of bein information in extense comments: A*CA* is most for Certification address (or address of the comments) of the comments of you want to read more about web security, please read What is a PKI? The commendencing method is provide unbloked	ds a public key and an identify, one such as permissions and is an internal entry of totade third manages digital confidence.	-
	services is known 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
CONTACT US	RUST.COM WEB VPN SET
powered by Entrust [®] Inc	
REQUEST A WEB	Step 1 - Accept and Fill out the Application
REQUEST A WEB SERVER CERTIFICATE	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_harper@uk.ibm.com
	Phone:
	You are interested in Freecerts for the purpose of: *
	Learning
	Minich Mah sanyar ara yau using?
	Uther 🔄
	ATTENTION:
	PLEASE READ THIS IMPORTANT INFORMATION ABOUT THE FREE CERTIFICATE ISSUED BY THE ENTRUST CERTIFICATE DEMO CA
	BY CLICKING ON "YES" AND OR BY USING THE FREE CERTIFICATE YOU AGREE AND ACMINIVEDGE THAT THE CERTIFICATE ISSUED TO YOUR BY THE ENTRUIST CERTIFICATE BANG CAI'S FRONDED AND SHALL & EUSED TO YOUR BY THE ENTRUIST CERTIFICATE RESOLUTION YOUR BY THE ENTRUIST CERTIFICATE FREE CERTIFICATES BUILDED TO YOUR BY COMMERCIAL AUROPOSE. SECHT FREE CERTIFICATES BUILDED TO YOUR BY FOR BY BUILDED TO YOUR BY FREE CERTIFICATES BUILDED TO YOUR BY FREE CERTIFICATES AND YOUR FURTHER RECORDILE THAT THE CERTIFICATES AND TO YOUR BEEN TO YOUR BY FOR BY
	Do you accept the terms and conditions as set out above. *
	Proceed to Step 2
	r required fields.
	WEB VPN SET
The certificates issued to you commercial purposes. You sho certificate requests are approv	on these web sites are intended for demonstration purposes only. They must not be used for uoid also be aware that we do not verify the identity of persons who request certificates. All ed automatically.
@2000 Entrust®, Inc. All Right	5 Reserved.
SET is a trademark of the SET	Secure Electronic Transaction, LLC.

m. Click on 'Proceed to Step 2'. Specify the server name (in other words the DNS name of the WebSEAL machine). **Note**: this must match the name specified above when the Certificate Request was generated.

赛 Web - Netscape	_ 8 ×
Elle Edit View Go Communicator Help	
Back Forward Reload Home Search Netscape First Security Shop Stop	N
👔 🏹 🖞 Bookmarks 🦼 Netsite: http://freecerts.entrust.com/cgi-bin/register.pl	👻 📢 What's Related
CERTIFICATES	
CONTACT US WER VPN/ SET	
VISIT WWW.ENTRUST.COM	
powered by Entrust*Inc.	
WEB Step 2 - Server Name	
REQUEST A WEB	
Please enter your server name as it shows up in the URL of the web server	
REDUEST A WEB SERVER CERTIFICATE secure server will be https://www.myserver.com/, then enter the server name	
as www.myserver.com.	
SECURE WEB SERVER	
ABOUT THIS	
DEMO Proceed to Step 3	
WEB VPN SET	
The certificates issued to you on these web sites are intended for demonstration purposes only. They must not be used for commercial numbers You should also be aware that we do not verify the identify of nersone who request certificates. All	
certificate requests are approved automatically.	
02000 Entrust0, Inc. All Rights Reserved.	
SET is a trademark of the SET Secure Electronic Transaction, LLC.	
Document: Done	

- 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
CONTACT US	UST.COM WEB VPN SET
powered by Entrust [®] Inc.	
WEB	Step 3 - Retrieve Certificate
REQUEST A WEB BROWSER CERTIFICATE REQUEST A WEB SERVER CERTIFICATE CONNECT TO QUR 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: 8010-31910-T082 Ref Number: 08008059
	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.
	MIIBg1TCBowlBAD62NDawCD7VDV020BellxHDEFMAd041UEChM6V022c V02DEU-v7XuRZV2LchlM6186H184g9/m0122MIIGHAN045812E0 Ad0AHAD6180XBg02DFEIx40xg023V028MIIGHAN04583 Ad0AHAD6180XBg02DFEIx40xg023V028MIIGHAN04583 Ad0AHAD6180XBg02DFEIx40xg023V028MIIGHAN04583 Ad0AHAD6180XBg02FEIX400804 Ad0AHAD61804 Ad0AHAD6180
	Submit Request Reset
e certificates issued to you o	n there was citize are intended for demonstration surgers only. They must not be used for
mmercial purposes. You sho tificate requests are approve	al da so be aware that we do not verify the identity of persons who request certificates. All d automatically.
999 Entrust Technologies. A	Il Rights Reserved.
T 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 1.1 – 30 September, 2002

IBM Tivoli Access Manager 3.9 - Cookbook

CERTIFICATES
CONTACT US WEB VPN SET
powered by Entrust Inc.
Veb Step 4 - Server Certificate Retrieval
HOWSET CENTRICATION This is your Server certificate (in raw DER). Copy the entire certificate into your
REQUEST A WEB / CIIDDOARD. If it is going to be installed into Microsoft intermet information Server, only copy SERVER CERTIFICITE / Mark is between the lines "BEGIN CERTIFICATE" and "PEND CERTIFICATE". If you are
using Netscape Enterprise Server, you should copy everything (i.e., including the CONNECT 10 QUE
secure your server using this certificate, please consult your server documentation.
ABOUTHSBEGIN CERTIFICATE
HITEISCLAFIGAVIBAGILANGSKAJANBOKAJANIGVUBAUUPADUPAUPAUPAUPAUPAUPAUPAUPAUPAUPAUPAUPAUPAU
GHA HAGATWA BUZA DWA BUZZ ZU UZAWHACHADEWA ZA TI XU DA VAGANDEWI TA TI NU TA VAGANDEWI TA VAGANDEWI TA TI NU TA VAGANDEWI TA VAGANDEWI TA VAGANDEWI TA VAGANDEWI TA TI NU TA VAGANDEWI
orvuoniesygonej lekupavagy takpizagy vydeinasyntakovanavani levuol ExvyennyydXND i dly i bložsozVNO bi z krytkar tekupava i byvisi levesh
KCAGAIIDEANYZ-GFY-GCVY-di 5 3ZW s'eW dadle and U EL MINET/CENEANBE/chai 6 Gev 0B A OREA 10 DEANBAU/C-GFV HOT U MS are 50 d all a 1967 S C A C TINE 107 1706 A DEANAND
ntgiFL01i+Udde9ULRq169-c+Rj03307=hR+CkT85u100000c7UBarKY=5300PPu Cc14347211+Ud273Ulz420WURDGYucce4UNH1vgYarCe4URF31u0CB00c7UBarKY=5300PPu
AVEAAaGCAagwagGkMasGAIUdDwQEAwIFcDAFBGIVURAEIDAigA9WDAXHD_yN]Ey NDayOFGDEIYUDDEWOTIATIIDODAWIABBI.ahkgBhyAEACAGEBBANCBAAWIDVIYIZI
AYb4Q=jECBC&WHnhOdHA6Ly6yHDQuHTAxtjEÿOC40Hy9jC2EtV240Hz8KB=jahk9B hvhCAQMEERY7X2nzD%07Q4DLnV4Z19hV3Npb249YZh1V2t5ZZZVYZPO&99JJJZD
Ukw9Y249Q1JMMTQ1JnN1cmlhbD0wdAYDVROfBG0wazBpoGegZaRjMGExCzAJBgNV BAYTA1VTMRAwDgYDVQQKEwdFbnRydXN0MS8wLQYDVQQLEyZFbnRydXN0IFBLSSBE
ZWi vbaNicarf0aW9uIENicarBoZaljYXRlczEFYAdOGAlUEArMOQJJMTOIMB8GAlUd IwQYMBaAFKZANIXIG4)+fikaka+soDBHCvoliHB0GAlUdBgQUEBEcgSUEKFRNQnSxR
pkIry2rxjkHRTAJB9HVHRHBjAHHEkGCSGGSID52(QBAAQHMAADBFY0LjADA900 HA0CSGgGTBJ0DBBDQUAAGBADEyuJ07H+68k56222yHGBpuv7pYpsBpVX3cxyL
nicUszi/ni/v4doi1004NU/SHSDOMUliGD/q90tkmgicHSUMWDE10nJlPG257 fdogcireBstoinHVFENBON75149jeOlEwv081VCLSrynKiaH929zcSNa-6U
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
n ne venumaans avera wy vu vu ne wes wes aver intended to' demonstration pulpoise ony. I ney must net be used for commercial pulpose. You should also be aware that we do not verify the identify of persons who request certificates. All certificate requests are approved automatically.
@1999 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
CONTACT US WER VPN SET
VISIT WWW.ENTRUST.COM
powered by Entrust* Inc.
2" 7"
WEN Step 5 - CA Certificate Retrieval (PEM encoding)
REQUEST A WEB
BROWSER CERTIFICATE This is the Certification Authority (CA) certificate. Copy the entire certificate into your
REQUEST A WER / 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
SECURE WESSEVER
BEGIN CERTIFICATE
ABOUT ND MILDRacCArcgavIBAgIENgvf5jANBgkghkiG9v0BADUFADBQNQswCQYDVQQGEwJV
UzeUMA4GA1UECHHRW5UCnVzdDEWCUGA1UECKHRW5UCnVzdCEUSUKGK5VtD25z
NDM5WjBQHQswCQYDVQQGEwJVUzEQMA4GA1ÜEChMHRV50cnVzdDevMC0GA1UECxMm
RWSUcnVzdCBQS0UgRGV4b25zdH3hdG1vb1BDzZ3U6wZpV2F0ZXMwgZ0vDQV1K6Z1 hronNofBP0Abpv2mMTCH2cDR1zmV0cBPFEDix_trt_11MUY29TDF5cTDrx3Vic4c3
st+yPVQk51rHh11MbCppgxcT6AxQ3So7Q1hayBoKGX97TW411F/VCicKyw8PyGyC
UeAVRD5i+sDpWhzZGuTLobIfamIW9alT6QbxeV/Lm4niNtnnqCfHz3ir3Rvu642m
Gok/TBH/QswCQTVQQGE4/JUZEQMA/GA/UBCMHRHSGI/DH/GGA/UECXMm
RW50cmVzdCB050kgRGVtb25zdHJhdG1vb1B0ZLV08VZpV2F0ZXMxDTAIDgWVBAMT
BERSIDEWKWIDVRUGBCQWIGAPAINSODASHJOWRUGBZIAGQWYMDAADKYNIEANICY
MB0GA1UdDgQWBBSmZ4TS++ifu35m5JvrKavR6FqNYjAMBgNVHRMEBTADAQH/MBkG
CSqGSIb2fQdBaAQMMAobBFY0IjADAqSQMA0CSqGSIb3DQEBBQUAA4GBAD7WW/C M7ReFE3HDabBdLsEvHcBbrCC2Bd1DopscdijBVUImensUGaraAGBefc7a153HD
+NgAVzqirK9qqhBmKZv3F51odd7ZwEHEb+ruJr8djqV1rdFtvf+A9zbOa6F+tsQh
MbdJKIUNqr3s19Mr5bpLW76DRrcgUqiXLoPr
WEB VPN SET
The perificates issued to you on these such sites are intended for demonstration numbers only. They must not be used for
commercial purposes. You should also be aware that we do not verify the identity of persons who request certificates. All
certificate requests are approved automatically.
Ø1999 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				
OB-Type: CMS key database file				
ile Name: C.\Program Files\Tivoli\PDWeb\www\certs\mypdsrv.kdb				
Key database content				
Signer Certificatés	▼ Add			
Thawte Personal Premium CA	Delete			
Thawte Personal Freemail CA	-			
Thawte Personal Basic CA	View/Edit			
Thawle Fremium Server CA				
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):

Browse

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:

IB-Type: CMS key database file Ile Name: C:Program Files\Tivoli\PDWeb\www\certs\mypdsrv.kdb Key database content	
B-Type: CMS key database file le Name: C:Program Files\Tivol\PDWeb\www\certs\mypdsrv.kdb Key database content	
ile Name: C:Program Files\Tivoli\PDWeb\wwwlcerts\mypdsrv.kdb Key database content	
Key database content	
Signer Certificates	▼ Add
Entrust Public CA Certificate	Delete
Integrion Certification Authority Root	
BM World Registry Certification Authority	View/Edit
Thawte Personal Premium CA	
Thawte Personal Freemail CA	Extract
Thawte Personal Basic CA	-
Thawte Premium Server CA	
Inawte Server CA	
PEN Boouve Control Control Authority	
Varisian Class 1 Public Primary Cartification Authority	
Verision Class 2 Public Primary Certification Automity	
tensign ender a reality in many control of the during	
Verision Class 3 Public Primary Certification Authority	

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

DM Key Management - [C. shogram hies shronshowed webswew scens singposity.kub]	ي ا
Database File Create View Help	
Key database information	
3-Type: CMS key database file	
e Name: C:\Program Files\Tivoli\PDWeb\www\certs\mypdsrv.kdb	
Key database content	
Versonal Certificates 🔹	Receive
	Delete
	View/Edit
	Import
	Recreate Request
	New Self-Signed
	Extract Certificate
	Cardinal Print Charles and Print 1999

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	2			
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 informati	ion -
B.Twee: CMS key database file	
le Name: C:Program Files\Tivoli\PDWeb\www.certs\mvodsrv.kdb	
Key database conten	t
Personal Certificates	▼ Receive
* test-webseal-cert	Delete
	ViewÆdit
	Export/Import
	Recreate Request
List of personal certifi	cates. Default indicated with *
	New Self-Signed

Version 1.1 – 30 September, 2002



aa.

- bb. The IBM Key Management utility is no longer required and may be closed.
- cc. Back up webseald.conf (Windows: in C:\Program Files\Tivoli\PDWeb\etc; UNIX: in /opt/pdweb/etc).
- dd. 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
```

- ee. 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>
- ff. Start WebSEAL. (In Windows, start Access Manager WebSEAL. In UNIX issue pdweb start)
- gg. Ensure that all the Access Manager services/process have started. If they do not all start, look in the log for the corresponding service/process.
- hh. Verify that Access Manager 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.
- d. In addition, refer to the section entitled 'Global Server ID Certificates Do Not Work Correctly' in the *Tivoli Access Manager Release Notes* regarding changing the ordering of the Cipher list.
26. Setting up client certificate authentication

(Client certificates can be obtained for demonstration use only from the Tivoli PKI demonstration site at http://demota.dfw.ibm.com/YourDomain/index.jsp. This site is accessible over the Internet.)

- a. Set up a WebSEAL Server certificate as described in the previous chapter.
- b. Edit webseald.conf (in C:\Program Files\Tivoli\PDWeb\etc\ Windows or /opt/pdweb/etc/ UNIX): within the [certificate] stanza, there is a statement accept-client-certs = never Change it to accept-client-certs = optional or accept-client-certs = required
- c. Also in the webseald.conf, within the [authentication-mechanisms] stanza set cert-ssl = sslauthn.dll (Windows) or cert-ssl = libsslauthn.a (AIX) or cert-ssl = libsslauthn.so (Solaris) as described in the Access Manager WebSEAL Administrator's Guide.
- 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.)

	Add
CMS key database file CMS key database file CAProgram FilestTivolitPDWebtwwwtcertstmypdsrv.kdb Key database content Signer Certificates Ivoli PKI Demo System CA Certificate	Add
ie Name: C:\Program Files\Twoli\PDWeb\www.certs\mypdsrv.kdb Key database content Signer Certificates Ivoli PKI Demo System CA Certificate	▼ Add
Key database content Signer Certificatés Ivoli PKI Demo System CA Certificate	▼ Add
Signer Certificates ivoli PKI Demo System CA Certificate	▼ Add
ivoli PKI Demo System CA Certificate	
	Delete
hawte Personal Premium CA	Dubto
hawte Personal Freemail CA	ViewEdit
hawte Personal Basic CA	
hawte Premium Server CA	Extract
hawte Server CA	Laudoun
erisign Test CA Root Certificate	
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 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 'View/Edit...':

IBM Tivoli Access Manager 3.9 – Cookbook

Tivoli PKI Demo System CA Certificate		
Key Size:	1024	
Version	X509 V3	
Serial Number:	01	
Issued to:		
TPKI37 PIC GB		
Issued by: TPKI37 PIC GB		
Validity: Fingerprint (MD5 D 04:F6:0F:E1:05:02 Signature Algorithm	Valid from August 13, 2001 to August 13, 2031 igest): :AOLA:EC:C5:D7:68:B1:73:80:59 : 1 2 940 113549 1 1 5(1 2 940 113549 1 1 5)	
eigneini o ringoritini		
Set the certificate a	is a trusted root	

- 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 Access Manager WebSEAL Administrator's Guide.
- j. Ensure that the DN specified within the Client Certificate matches the LDAP DN defined for the corresponding PD user.
- k. Re-start WebSEAL to make these changes take effect.
- I. Once this is all set up you should now be able to point your browser to a protected resource and use your certificate to authenticate.

27. Setting up an SSL connection to the LDAP Directory

Note: This section needs to be revised for Access Manager 3.9.

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 (Access Manager Server)
- Install LDAP Server certificate at the LDAP Client (Access Manager 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 Access Manager 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 Access Manager Servers to use an SSL connection to the LDAP Directory.

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 gsk5ikm.exe in the C:\Program Files\IBM\gsk5\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 (gsk5ikm):



c. 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:	CN	

d. 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:

IBM Tivoli Access Manager 3.9 – Cookbook

Password Prompt		2
Passw	rord: ********	
Confirm Passw	rord: *******	
Set expiration tim	1 e? 60	Days
🗹 Stash t	he password to	a file?
Password Strength:		
	<u> </u>	
OK Re:	set Cance	Help

e. 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 file C:\Idapsrvkey.sth.	¢.
	ОК	

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

BM Key Management - [C:\ldapsrvkey.kdb]	
y Database <u>Fi</u> le <u>C</u> reate <u>V</u> iew <u>H</u> elp	
Key database information	
R.Twne: CMS key database file	
In Names Cilideners/sector	
e wane, ic.adapsivite; kup	
Key database content	
Signer Certificates	← Add
hawte Personal Premium CA	Delete
name la solira realitati con Travte Personal Basic CA Travte Personal Basic CA	View/Edit
hawte Server CA	
/erisign Test CA Root Certificate	Extract
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	
a requested action has successfully completed!	

- g. Next create a self-signed certificate for the LDAP Server. Click on Create -> New Self-Signed Certificate.
- h. 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)

lease provide the	Tollowing:		
Key Label		LDAP Server	
/ersion		X509 V3 🔻	
(ey Size		1024 🔻	
Common Name		secure2.pisc.uk.ibm.com	
Organization		ibm	
Organization Unit	(optional)		
ocality	(optional)		
State/Province	(optional)		
Zipcode	(optional)		
Country		GB 💌	
/alidity Period		365 Days	

i. 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]	
key Database File _ Create _ View _ Help	
Key database information	
3-Type: CMS key database file	
e Name: C Udapsrvkev kdb	
Key database content	
	_
'ersonal Certificates	Keceive
LDAP Server	Delete
	View/Edit
	Export/Import
	Recreate Request
	New Self-Signed
	Extract Certificate
e requested action has successfully completed	

- j. 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.
- k. 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	Þ
Data type	Base64-encoded ASCII data 🔻	
Certificate file name:	LDAPsrvcert.arm	Browse
Location:	C:)	
	OK Cancel Help	

I. Click on 'OK'.

- m. Copy the .arm file you have just created to the LDAP Client machine (in other words the Access Manager Server component machine, for instance the WebSEAL machine).
- n. On the LDAP server machine, point a web browser at http://servername:port number/ldap and log on as the administrator.
- o. Clicking on Security → SSL → Settings, you will be presented with the LDAP SSL options.

💥 SecureWay Directory Server \	⊮eb Admin: secure2 - Netscape		- 5 ×
<u>Eile Edit View Go Communicato</u>	r <u>H</u> elp		
Back Forward Reload	🔥 🥂 🚵 🍦 📽 🙆 Home Search Netscape Print Security Shop	21 Stop	N
🕴 ॳ Bookmarks 🌛 Location:	http://secure2.pisc.uk.ibm.com:81/ldap/cgi-bin/ldacgi.exe?Action=Sta	rt.	💌 🍞 What's Related
🧴 🚴 Instant Message 🛛 🖳 WebMa	il 🖳 Contact 🚇 People 🖳 Yellow Pages 🖳 Download 📋	j Channels	
Directory Server	SSI settings		0 2
Introduction	A carura?		• •
Settings	Ready		
Security			
Settings	Edit the SSL general settings, then click Update .		
Encryption	COT	0.001.0-1-	
Kerberos	SSE status	C SSL Only	
Replication		C SSL Off	
Database		127 M 14 200 000 00	
Current state	Authentication method	• Server Authentication	
🖸 Logoff		C Server and Client Authentication	
	Secure port	63.6	
	Key database path and file name	c.\ldansrykey kdb	
		of trades they have	
	Key label		
	A password is only required if there is no password sta	ish file for the key database, or if you wish to override the password stash.	
	Kay naseword		
	ney passion		
	Confirm password		
	Update Reset		
	Related tasks:		
	Engrantion Calect the type of SCI committee		
	Certificate revocation - Define the LDAP server	used for certificate revocation.	
	5		
<u>.</u>			
Applet o	com ibm webexec herald. HeraldApplet running		

- p. 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).
- q. Click on 'Update'.
- r. Click on 'restart the server' to restart the LDAP server and allow this change to take effect.
- s. To test that SSL has been enabled, run the following command from a command line at the LDAP server:

```
ldapsearch -h servername -Z -K keyfile -P password -b "" -s base
objectclass=*
```

The results should look similar to the following:

```
C:\>ldapsearch -h secure2 -Z -K "c:\ldapsrvkey.kdb" -P Secure99 -b "" -s base
objectclass=*
Namingcontexts=CN=SCHEMA
Namingcontexts=OU=EMEA,O=IBM,C=GB
Namingcontexts=SECAUTHORITY=DEFAULT
Namingcontexts=CN=LOCALHOST
Subschemasubentry=cn=schema
Supportedextension=1.3.18.0.2.12.1
supportedextension=1.3.18.0.2.12.3
supportedextension=1.3.18.0.2.12.5
```

```
supportedextension=1.3.18.0.2.12.6
supportedcontrol=2.16.840.1.113730.3.4.2
supportedcontrol=1.3.18.0.2.10.5
secureport=636
security=ssl
port=389
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 (Access Manager Server components) - create the key database file

a. On the LDAP Client machine, start the IBM Key Management tool (gsk5ikm):



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:	[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:

IBM Tivoli Access Manager 3.9 – Cookbook

Dacemord	******
rassworu.	
Confirm Password:	******
Set expiration time?	60 Days
🗹 Stash the pa	ssword to a file?
Password Strength:	
2-2-3	
and the second se	
Course Course C	and Change De

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

LDAP Client (Access Manager Server) - install LDAP Server certificate

a. Ensure you are viewing the 'Signer Certificates' from the drop-down menu:

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.Tyme: CMS key database file	
IRE NAME: CULDAPCIREY.KOD	
Key database content	
Signer Certificates 🗸 🗸	Add
Thawte Personal Premium CA	Delete
hawte Personal Freemail CA	
'hawte Personal Basic CA	View/Edit
Thawte Premium Server CA	
Fhawte Server CA	Extract
/erisign Test CA Root Certificate	
RSA Secure Server Certification Authority	
/ensign Class 1 CA Individual Subscriber-Persona Not Validated	
/ensign Class 2 CA Individual Subscriber-Persona Not Validated	
/arigin Class 3 CA Individual Subscribert ersona Not Validated	
/erisign class 7 Public Primary Certification Authority	
/erisign Class 3 Public Primary Certification Authority	
]
e 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)

Add CA's Certificate In	im a File	
Data type	Base64-encoded ASCII data 🔻	
Certificate file name:	LDAPsrvcert.arm	Browse
Location:	<u>C1</u>	
	OK Cancel Help	

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]	_ 0
ey Database <u>F</u> ile <u>C</u> reate <u>Vi</u> ew <u>H</u> elp	
Key database information	
OB-Type: CMS key database file	
ile Name: C'll DABclikev kdb	
ile Name, Josephi Ciney, Nab	
Key database content	
Signer Certificates 🔹	Add
LDAP Server	Delete
Thawte Personal Premium CA	
Fhawte Personal Freemail CA	View/Edit
Thawte Personal Basic CA	
Fhawte Premium Server CA	Extract
hawte Server CA	II
/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	
Verisign Class 3 CA Individual Substituter-Persona Nutivalidated	
ensign Class F Fubilit Finnary Certification Authority	
/erisign Class 2 Fublic Primary Certification Authority	
reneigh eines a'r dailer rinnary centineallen Adarenty	
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	
Ver Circle	1004
Rey Size: Cortificato Dronorty	. 1024
Version	X509 V3
Serial Number:	3B:AB:60:87
Issued to:	
secure2.pisc.uk.i ibm GB	lbm.com
issued by: secure2.pisc.uk.i ibm GB	ibm.com
Validity: Fingerprint (MD5 D ED:F7:B4:1E:E0:9 Signature Algorith	Valid from September 20, 2001 to September 21, 2002 ligest): 5:42:6E:35:E9:21:17:23:F2:C4:FD m: 1.2.840.113549.1.1.4(1.2.840.113549.1.1.4)

- 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
supportedldapversion=3
ibmdirectoryversion=3.2.1
ibm-ldapservicename=secure2.pisc.uk.ibm.com
ibm-adminid=CN=ROOT
ibm-servertype=master
```

Version 1.1 – 30 September, 2002

ibm-supportedacimechanisms=1.3.18.0.2.26.2

Configuring PDRTE for SSL communication to LDAP

If you wish to use SSL communication between PD components such as WebSEAL and LDAP then you will need to make this decision as you configure the PDRTE. This will mean a couple of different choices than those described in the earlier chapters.

When configuring PDRTE you will see the sceen below.	
is SSL Communication with the LDAP Server	×
Enable SSL Communication with the LDAP Server?	
© Yes C No	
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.

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:	

Cancel	

- b. Click 'Finish', the PDRTE is configured.
- c. You can then continue and configure any remaining PD servers that you need that will then communicate via this PDRTE to LDAP.

28. Installation of SecurID token support

Note: This section needs to be revised for Access Manager 3.9.

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 Access Manager is installed - this is an unlikely situation in real world, but it is useful for demonstration purposes. (Refer to the Policy Director red book for a description of how to install the ACE/Server on a machine remote from WebSEAL.)

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

- CD-ROM with the ACE/Server 3.3.1
- CD-ROM with the ACE/Agent CD 4.3 (not used in this installation)
- Diskette with the ACE/Server license code
- Diskette with the tokens record (token Seed Kit), and
- Two SecurID tokens

This also assumes that you have a working Policy Director 3.6 running on NT.

a. Log in as a Windows NT administrator.

- b. If there is any possibility of the ACE/Server having been previously installed on the machine, delete the file C:\WINNT\system32\securid. (This file contains a secret which is used for the cryptographic protection of communication between the ACE client and server.) You might also want to ensure that the \ace directory is deleted (to remove any existing ACE/Server configuration data).
- c. Insert the ACE/Server V3.3.1 CD-ROM into the CD drive.
- d. Insert the diskette labelled "ACE/Server V3.3.1 2 User Promo License" into the diskette drive.
- e. Using 'My Computer' find the \aceserv nt_i386 directory on the CD, and double click on setup.exe. An ACE/Server window displays, followed by the Welcome screen:



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



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



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



i. Click on 'Next'. The 'Available Input Files' screen will be displayed:

IBM Tivoli Access Manager 3.9 – Cookbook



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:

ri Liberd		
Name:		
Network address:		
Site:		Select
Client type: UNIX Client Communication Single-Transact	Server	
Encryption Type: 🔿 SDI 👁 DES		
🗖 SentNode Secr	et	
🗂 Open to All Loca	ally Known Users	
🗖 Search Other Fa	ealms for Unknown Users	
Group Activations	User Activations	l I
Secondary Nodes	Delete Client	
	Assign/Change Encryption Key	1

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: 9.180.244.205		
Site:		Selec
Client type: UNIX Client Communication Single-Transact	Server view view view view view view view view	
Encryption Type: C SDI @ DES		
🗖 Sent Node 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:

ime: PD Users	
Site:	Selec
Members	Client Activations
Delete Group	Edit Group Extension Data
Edit Access Times	
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':

Client Activations	×
Group: PD Users	
Client: harperv.welwyn.uk.ibm.com	Clients Activated On harperv.welwyn.uk.ibm.com
Add Client Filter	Remove Client Edit Client
Exit Help	

- 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':

Jser: Vaughan Harper	-1
Available Groups PD Users	Group Memberships PD Users
	× ×
Join Group	Remove Group Edit Membershin Data
1	

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



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



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



jj. Find the actual SecurID token whose serial number matches that displayed.

kk. Click on 'Edit Assigned Token...'. The 'Edit Token' panel will be displayed:

ey Fob with 6 digits, changing ev	rery 60 seconds.
Serial number: 000002	738665
Assigned to: Vaugha	an Harper
Next tokencode mode: Off	
Lost Status: Not Los	st
Last login date (UCT): 81/81/	1986 , 00:00 🔽 Enabled
Token start date: 85/14/	/1999 , 05:00
Token shutdown date: 12/31/	2002 . 05:00 🗵 New PIN mode
Resynchronize Token	Cigar PIN
Set PIN to Next Tokencode	Edit Assigned User
Aroign Token	Unassign Tokon
Delete Token	Edit Lost Status
Edit Token Extension Data	Assign Replacement Token
Convet Cond Convertings	

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:

a rita to ne.	a rokencoue.	
Serial Nu	nber: 000002738665	
Enter the	code displaying on the token.	
	905528	
he PIN wil	l be the first 4 digits of the next tokenco	ie.
OK	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 <code>aceclnt.dll</code> from the <code>\ACE\prog</code> directory to the <code>\WINNT\system32</code> directory.

xx. Click on 'Start -> Settings -> Control Panel. Double-click on the ACE Server icon:

ACE/Server	<u>></u>
	The second se
Start stop	OK
Automatic ACE/Server startup.	
- ACE/Broker	Help

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 1.1 – 30 September, 2002

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:

IBM Tivoli Access Manager 3.9 – Cookbook

Policy Director Login - Nat	cape ex lite	215 IN
a a Bay		N
🚮 Bockmatts 🥀 Jene:	er (Plotol/Happenies April & ter bena 483)	V 💓 VF AN Robin
Policy Director	Login	
handard Authentication		
• Usiciona		
• Fineword		
loken Authentication		
• Estime	asers	
 FASSCODE 	mmm.	
ال وقت		
	: wer 5 we	135 Ma #2 #2 w

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
11/27/2000	17:22:370	SYSTEN	>/
11/27/2008	17:22:37L	Admin Server Started	harperv.welwyn.uk.ibm.com
11/27/2000	17:34:270	usera/harperv.welvyn.uk.ibm.com	000002738665/Vaughan Harp
11/27/2008	17:34:27L	Node Secret Sent to Dlient	harperv.welwyn.uk.ibm.con
11/27/2000	17:34:270	usera/harperv.welwyn.uk.ibm.com	000002738665/Vaughan Harp
11/27/2008	17:34:27L	PASSCODE Accepted	harpers.welwyn.uk.ibm.con
11/97/2008	17:35:070	Administrator	
11/2//2000	1/:35:0/L	Sdadmin Started	harperv.weluyn.uk.ibm.con
11/27/2000	17:35:400	Administrator	
11/27/2000	17:35:40L	Printed Activity Report	harperv.weluyn.uk.ibm.com

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.

29. Useful LDAP commands

For a full treatment of LDAP, see the excellent red book SG24-5110 *LDAP Implementation Cookbook.* But in the meantime, the following commands may prove useful:

• ldapsearch -h *hostname* -b "C=US" "objectclass=*" "*" this lists all attributes for all directory entries with a base of "C=US"

• ldapsearch -h *hostname* -b "C=US" "objectclass=*" "modifytimestamp" this lists the time stamps for all directory entries with a base of "C=US"

• ldapsearch -t -h *hostname* -b "C=US" "objectclass=*" "*" useful for binary objects - this writes all attributes to files, and displays the names of the files created, for all directory entries with a base of "C=US"

• ldapsearch -h *hostname* -b "" -s base "objectclass=*" this lists all the base objects within the directory

30. 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.

Access Manager 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 Access Manager 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 webseald the following process should be listed: webseald.

If not, look at the appropriate log files.

Issue netstat -a to see whether anything else is listening on the ports which WebSEAL is wanting to listen on.

If under UNIX the Access Manager 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 Access Manager 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.)
- Switch on the LDAP auditing. If you are using the IBM SecureWay Directory, using the LDAP web administration interface, select Logs -> Audit log -> Settings, then select Enable audit logging=Yes, Operations to log=all, Type logging = All attempts.
- 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 Version 3.2.2 for AIX Installation and Configuration guide – this is on the Tivoli Access Manager Base for AIX Version 3.9 CD at /doc/Directory/aparent.pdf (or the corresponding manuals for the other platforms). There are other SecureWay Directory product manuals in the same directory.

You can try issuing the following:

ldtrc on slapd -h 65535 2>&1 | tee ldap.out

Version 1.1 – 30 September, 2002

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 Access Manager in debug mode.
- Try running PD services in the foreground with the '-foreground' parameter
- If you suspect LDAP problems (on Windows), you can sometimes find useful information by going to Start -> Programs -> Administrative Tools (Common) -> Event Viewer, and clicking on Log -> Application.

Page Not Found problems...

- Try running an IP trace between WebSEAL and the back-end web server.
- Try specifying -j when creating the junction, and (optionally) specify script-filter=yes in the [script-filtering] stanza of webseald.conf, or try setting up the Junction Management Table.
- 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.

Other problem determination ideas - AIX

1. Verify LDAP is running

ps -ef | grep slapd

2. Stop PD services

iv stop

3. Start PD

iv start

4. Verify PD is running # iv status

Part VI - 3.9 Beta Workshop Hands-on Labs Guide

This section was written by Oleg Bascurov, Gianluca Gargaro and Jeff Miller under the leadership of Avery Salmon and Jon Harry from the PIC, Hursley, as a Lab Guide for the 3.9 Beta Workshop. Some of the information here is no longer relevant as it relates to the Beta code rather than the GA code or it duplicates information covered elsewhere within the cookbook. However much of the information here will be useful as it covers other configurations, other user registries, AM WAS, etc.

31. Introduction

This hands-on lab was written for use in the Policy Director v3.9 workshop. It covers some of the major new functions introduced in PD v3.9 including J2EE integration with WebSphere Application Server v4.0.2, Web server plug-in, new Directory support, and WebSEAL enhancements.

The labs (each of which is represented by a section in this document) should work independently of the others but are written with the intention that this document will be followed from beginning to end.

The labs follow this overall flow:

- Installation and Configuration
- WebSEAL Enhancements
- Policy Director Integration with WebSphere
- Form-based Single Sign-on
- Policy Director Web Server Plug-in

There are also several appendices at the end of this lab workbook that contain installation procedures that either have been done in advance or are alternatives to the lab-specified methods for performing various tasks.

31.1 Style conventions

A number of text styles have been used in this document:

Syle	Purpose
pdadmin> user list * 100	Shaded text represents a screenshot or the contents of a text file. The bold text is user input.
What does this mean?	The large question mark symbol indicates a question or something for you to try to test your understanding.

Read this. It could be useful information that you won't see anywhere else.

The solid bar on the left of the text indicates that the text contains hints and tips beyond the instructions for completing the lab exercises.

31.2 Addition information resources

If you want additional information while you are going through these labs then please refer to the PD v3.8 TOI class notes or the product publications. Beta copies of the Policy Director publications are available in **D**:\AMPublications directory.

31.3 Machine hostnames and DNS names

For these lab exercises you will need to know the full DNS names of the machines you are using. To determine this open a command window and issue the command:

C:\>ipconfig

Note the IP address of the machine and then use the following command to get the DNS name:

 $C: \setminus ping -a x.x.x.x$

Where x.x.x.x is the IP address from the *ipconfig* command.

31.4 Lab Environment

These lab exercises were written assuming the lab environment described below.

The lab PCs are preloaded with the following software:

- Microsoft Windows 2000 Server Service Pack 2
- Microsoft Internet Explorer 5.5 SP2
- Netscape Navigator v4.77
- Winzip
- Java 1.3 SDK
- Adobe Acrobat v4.05

Before starting the Policy Director exercises you need to install and configure the prerequisite software. The instructions for these are in Appendix A:

- 1) IBM HTTP Server 1.3.19
- 2) GSKit 5
- 3) DB2 UDB 7.2 plus Fixpack-4
- 4) User Registry

Of course Policy Director also requires a User Registry, so you must install and configure one of the below. The instructions to install & configure these are also in Appendix A.

Note: Not all components are supported with all registry types. For maximum test-case coverage use IBM Directory Server 3.2.2

Version 1.1 – 30 September, 2002

- IBM Directory Server 3.2.2
- Lotus Domino Server 5.0.9
- MS Active Directory

Many of the labs use a sample J2EE application called *Banker 2001*. You'll use it to test role-based authorization in WebSphere, particularly when Policy Director makes the authorization decisions for WebSphere. The banking functions of the application are the protected ones. These are creating accounts, viewing accounts, and transferring money. The other functions are primarily used to test various lab features.

To install & configure WebSphere 4.02 use the instructions in Appendix B.

31.5 Default Configurations

File Locations

Option	Value
DB2	C:\SQLLIB
IBM HTTP Server	C:\Program Files\IBM HTTP Server
Policy Director	C:\Program Files\Tivoli\Policy Director
WebSphere Application Server	C:\WebSphere\AppServer
IBM Java 2 v1.3.0	C:\WebSphere\AppServer\java
Hands-on files	D:\LabFiles

IBM Directory Server Configuration Options

Option	Value
Directory Administrator ID	cn=root
Directory Administrator Password	passw0rd
Directory Server Hostname	<yourhost>.pisc.uk.ibm.com</yourhost>
Suffix	o=ibm,c=gb
Directory Server Port	38900
Installation Directory	C:\Program Files\IBM\LDAP

Active Directory Server Configuration Options

Option	Value
Directory Administrator ID	Administrator
Directory Administrator Password	passw0rd
Directory Server Hostname	<yourhost>.pisc.uk.ibm.com</yourhost>
Suffix	dc= <yourhost>,dc=com</yourhost>
Directory Server Port	389
Installation Directory	(system)

Domino Server Configuration Options

Option	Value
Directory Administrator ID	Administrator
Directory Administrator Password	passw0rd
Directory Server Hostname	yourhost.pisc.uk.ibm.com
Directory Server Port	3890
Installation Directory	C:\Lotus\Domino

31.6 User IDs, Passwords and Ports

During the labs, you will set-up and use several user IDs, passwords and ports. To help you keep track of them, they're are listed here:

<u>User ID</u>	Password	Purpose
Administrator	passw0rd	Machine and directory passw0rd
db2admin	passw0rd	Administer DB2
sec_master	passw0rd	Policy Director administrator
wasadmin	passw0rd	WebSphere administrator
pdwas	passw0rd	Represents the WebSphere JVM in PD

You will also use several ports for HTTP. For reference, here are the lab defaults:

<u>Port</u>	<u>Purpose</u>
80	Port for WebSEAL
82	TCP Tunnel input port
443	Port for WebSEAL SSL
888	Port IIS
4444	Port for IBM HTTP Server SSL
8000	Domino HTTP port number
8888	Port for IBM HTTP Server
9080	Port for WebSphere embedded Web server

31.7 Banker 2001 Users and Roles

Throughout the labs you will use a sample application called Banker 2001 to configure and test application security. The application has 9 users and 2 groups. You will configure these in the directory you choose for the labs. (When you work with these users and groups, all names should be fully lower case, without accented characters.) The mappings look like this:



Two of the users do not belong to groups.

31.8 Useful utilities

In order to make the most of these labs the following utilities can be used. Some are available on the desktop and some are copied when the lab setup batch file is run after the installation section of the labs:

WordPad	Unless a better text editor is available Wordpad is recommended for editing text configuration files
Tail	This utility allows a text file to be monitored in real time. It is very useful for viewing log files. Log files can be dragged onto the icon from Windows Explorer. Located in the $D: \LabFiles$ directory.
Base64	This utility converts text into Base64.
You may want to create a couple of BAT files yourself that make it easier to CD to the PD directories.	
pd.bat	This could be a batch file that changes the working directory to the default PD install directory, <i>C:\Program Files\Tivoli\Policy Director</i>
pdweb.bat	This could be a batch file that changes the working directory to the default WebSEAL install directory, C:\Program Files\Tivoli\PDWeb

32. Installing Policy Director

32.1 Setup

Version 1.1 - 30 September, 2002
Installation of Web Portal Manager requires that WebSphere Application Server be installed on your machine. This should already be done (per the procedure in 47 Appendix B -- WebSphere Installation). To check WebSphere, open a DOS window and enter

C:\>**echo %WAS_HOME%** C:\WebSphere\AppServer

If the WAS_HOME environment variable is not set, talk to your instructor.

Use Windows Explorer to open the drive where the *Policy Director* CD images are located under the *D:\LabFiles\PDImages* directory. This directory has three subdirectories:

- pd_*
 - Policy Director disk images directory
- pdweb*
 - PD Web Portal Manager setup directory
- PDWebPI*
 - o PD Web Plug-in disk images directory

Under Policy Director\Disk Images\Disk1 launch the Setup.exe file by double-clicking on it.

Select all the components and click Next to start the install of the Policy Directory files on your machine.

When asked, do not reboot now but navigate to *WebSEAL\Disk Images\Disk1* and double-click *Setup.exe* to install WebSEAL, too.



Select all the components for WebSEAL. This will install the Policy Directory files on your machine.

The products are now installed but still need to be configured. Reboot your machine.

33. Configure Policy Director with Your User Registry

There are five Policy Director installed packages and each needs to be configured for full PD functionality. All but the first, PDRTE, are the same regardless of the directory server underneath. In this lab, choose the PDRTE section that corresponds to your directory server. Do that part and then skip to section Part VI - 33.4 Finishing Policy Director Configuration on Your Directory Server that covers configuring the four remaining packages.

33.1 Configuring PDRTE with IBM Directory Server

Considerations

IBM Directory Server 3.2.2 should already be installed and configured to listen on port 38900 as per the instructions in section 46.4 Installing IBM SecureWay Directory Server 3.2.2. All the Policy Director components should also be installed in order to start the configuration process.

First start your user registry.

Configuration of PDRTE using IBM Directory Server 3.2.2

To begin configuration, select START->Programs->Policy Director->Configuration.

Policy Director Configuration			×
Select a package in the list then click Configure or U	nconfigure.		Close
Installed Packages	Configured		Refresh
Policy Director Runtime Environment (PDRTE) Policy Director Management Server (PDMg) Policy Director WebSEAL (PDWeb) Policy Director Authorization Server (PDAcId) Policy Director Web Portal Manager (PDWPM)	No No No No No	-	View log Configure Unconfigure
(Þ	

This displays the Policy Director Configuration dialog. Select PDRTE and click Configure....

🏠 User Registry Selection	×
User Registry Selection	
EDAP	
C Active Directory	
C Domino	
Next > Cancel	

Select LDAP as user registry. Click Next.

M LDAP Server Information	×
LDAP Server Information	
LDAP Host Name	
secureway6	
LDAP Port Number	
38900	
LDAP DN for GSO Database	
o=ibm,c=gb	
< Back Next > Cancel	

Provide the information as per the table in section 31.5 IBM Directory Server Configuration Options. Set the LDAP Host Name to that of your machine. Note that the default port of 389 is changed to 38900. This is because it can be. Active Directory also uses 389 by default and it is unable to use another. So to keep all the lab machines consistent, 389 is reserved for Active Directory, 3890 for Domino, and 38900 for IBM LDAP.

Click Next.

🍄 SSL Communication with the LDAP Server	×
Enable SSL Communication with the LDAP Server	
C Yes 💿 No	
LDAP SSL Client Information	
Port number	
636	
Key file with full path	
Certificate label	
Key file password	
< Back Next > Cancel	

These labs don't require SSL for communication between the LDAP client and server, hence disable this feature. Click Next.

Policy Director Configuration Review	×
Management Server Host: secureway6 User Registry Selection: Idap LDAP Host Name: secureway6 LDAP Port Number: 38900 LDAP DN for GSO Database: o=ibm,c=gb Enable SSL Communication with the LDAP Server: No	

At this point the configuration procedure has all the info required to start and will show you what provided, simply click on Finish to proceed. Now go to section Part VI - 33.4 Finishing Policy Director Configuration on Your Directory Server to continue.

33.2 Configuring PDRTE with Active Directory

Considerations

Active Directory should already be installed on your machine with a DNS fully configured. Policy Director should also be installed but not configured. These instructions start with Policy Director configuration and use Active Directory as the LDAP server.

Configuration

To begin configuration, select START->Programs->Policy Director->Configuration.

n Policy Director Configuration		X
Select a package in the list then click Configure or Uno	configure.	Close
Installed Packages	Configured	Refresh
Policy Director Runtime Environment (PORTE) Policy Director Management Server (PDMgr) Policy Director WebSEAL (PDWeb) Policy Director Authorization Server (PDAcId) Policy Director Web Pontal Manager (PDWPM)	No No No No No	View log
		Unconfigure
•	Þ	

This displays the Policy Director Configuration dialog. Each entry must be configured in order, from top to bottom. Select PDRTE and click Configure....

🔞 User Registry Selection 🔀
User Registry Selection
C LDAD
O LDAP
Active Directory
C Domino
Next > Cancel

Select Active Directory and click Next.

Active Directory server information
Active Directory server information
- Multiple domains
C Yes © No
Host name (e.g. adserver.tivoli.com)
secureway7.secureway7.com
Primary domain name (e.g. dc=tivoli,dc=com)
uc-secureway/,uc-com
Enable encrypted connection
C Yes © No
< Back Next > Cancel

Enter the information for your host and domain names as shown above.

To find out the Host name and the Primary domain name of your machine right-click on "My Computer" icon on your Desktop and choose the tab "Network Identification."

Select No for both Multiple domains and Enable encrypted connection. Click Next.

Active Directory administrator information
Active Directory administrator information
Administrator ID
Administrator
Password

< Back Next > Cancel

Enter the Administrator ID and passw0rd as the Password and click Next.

Active Directory data information
Active Directory data information
Policy Director data location Distinguished name (e.g. dc=tivoli,dc=com)
dc=secureway7,dc=com
< Back Next > Cancel

Here, *dc* stands for *domain controller*. Set the portion shown as secureway7 above to <your hostname>.



Wait until the configuration finishes. Now go to section Part VI - 33.4 Finishing Policy Director Configuration on Your Directory Server to continue.

33.3 Configuring PDRTE with Domino

Considerations

Click Finish.

In order to configure Policy director to use Domino as the directory server, you first need to check that the prerequisites are met. The following components have to be installed, properly configured and **running (Lotus Domino Server)** prior to Policy Director (the whole package) configuration:

- IBM GSKit latest available version
- DB2 7.2 + Fixpack 4
- WebSphere Application Server 4.0.2 Advanced Edition or Advanced Edition Single Server Version
- IBM Directory Server 3.2.2 Client
- Lotus Domino Server 5.0.9
- Lotus Notes 5.0.x

Check the user using the Notes client. This may not be the correct user. You can click cancel on the Notes client login, and change to user PDaemon, whose ID file will be located under the Notes directory in ids/people/PDaemon.id.

Procedure

Run Start -> Programs -> Policy Director -> Configuration. Select "Policy Director Runtime Environment" (PDRTE) and click on Configure.

📴 User Registry Selection 🔀 🔀
User Registry Selection
C LDAP
Active Directory
O Domino
Next > Cancel

1) Select Domino as the User Registry. Click Next.

Nomino Server information	×
Domino Server information	
Fully qualified domino server name	
secureway5/secureway	
Domino server TCP/IP hostname	
secuerway5.pic.uk.ibm.com	
Domino LDAP server port	
3890	
< Back Next > Cancel	

2) Enter the fully qualified Domino server name. This includes the name of the server and the Notes domain.

3) Enter the full DNS name of the Domino server.

4) Enter the port number that the Domino server TCP LDAP interface is listening on. This must match that which was configured on the Domino server, normally 389 by default. However, in these labs 389 is the Active Directory port, even though you may not be using Active directory. So set the Domino port to 3890. Then click Next.

	C Yes	No	
AP SSL Clien	t Information		
Port number	_		
636]		
Key file with	full path		
Cartificate la	hal		
Key file pas:	sword		

5) Specify if SSL should be used for communication with the Domino LDAP interface. SSL does not need to be enabled for the labs. Click Next.

👘 Notes client password	×
Notes client password	

< Back Next > (Cancel

6) Enter the password of the PD Privileged User. This password will be used by Policy Director to log into the Notes client in order to communicate with the Domino Server. This password is the one that was given when creating the PD Privileged user, *passw0rd*. Click Next.

Policy Director Configuration
Domino Address Book database name
names.nsf
Policy Director meta-data database name
PDMdata.nsf
< Back Next > Cancel

7) Specify the filename of the Domain Address book on the Domino Server. By default this will be *names.nsf* and is pre-filled with that value. This filename is relative to the server Data directory.

8) Specify the filename of the PD metadata database on the Domino Server. By default this is *PDMdata.nsf* and is prefilled with that value. This filename is relative to the server Data directory and will be used to create the PD metadata database when PDMgr is configured. Click Next.

Confirm by clicking Finish that the information you provided is correct. The configuration of the Policy Director RTE on Domino is completed.

You may take a look at the *domino.conf* file (under *C:\Program Files\Tivoli\Policy Director\etc*), which contains the configuration information entered by the administrator. All of the information is visible in this file with the exception of the Notes client password, which is obfuscated so that it cannot be read.

You may also take a look at the client's *notes.ini* file (by default under x:\Lotus\Notes). It was modified during the PD configuration by adding a line that allows Policy Director to silently log into the Notes client using the password stored in the *domino.conf* file.

🛃 notes.ini - Notepad				
File	Edit	Format	Help	
EXT	MGR_	ADDINS	5=pdextmgr.dll	

The configuration of other Policy Director components corresponds to that with IBM Secureway Directory or Active Directory.

Note: make sure the IBM Directory Server client is installed on the Management Server machine. Continue with PD configuration in the following section.

33.4 Finishing Policy Director Configuration on Your Directory Server

After you've installed PDRTE on your directory server, continue here.

1	Policy Director Configuration		X
	Select a package in the list then click Configure or Unconfi	gure.	
			Close
			 Befresh
	Installed Packages	Configured	Henesit
	Policy Director Runtime Environment (PDRTE)	Yes	Viewlog
	Policy Director Management Server (PDMgr)	No	view log
	Policy Director WebSEAL (PDWeb)	No	
	Policy Director Authorization Server (PDAcId)	No	
	Policy Director Web Portal Manager (PDWPM)	No	
			 Configure

Configure each package in turn.

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

Password confirmation

OK Cancel

Enter passw0rd as the Administrator Password and click OK.

Note: The type of user registry chosen during the configuration of PD Runtime Environment changes slightly the dialogs displayed during configuration of the PD Servers (PDMgr, PDAcl, WebSEA). The dialogs shown in the remainder of this section are for IBM SecureWay LDAP.

10 LDAP Administrator Login	×
LDAP Administrator Name	
cn=root	
LDAP Administrator Password	
******* I	
ОК	Cancel

On this dialog enter *cn=root* and *passw0rd* to specify the user name and the password of the directory administrator during both PDMgr and PDAcl configurations.

n PDMgr SSL parameters	×
Specify the SSL connection parameters for th Management Server.	e Policy Director
CCL listoping part number	74.05
aac instelling purchalitier	/135
SSL Certificate lifetime	365
SSL connection timeout	7200
Enable root CA Certificate download	Γ
ОК	Cancel

Since you are installing on a single machine, you do not need to enable download of the root CA Certificate – other components can use the file directly from the hard drive. Accept the defaults and click OK. This takes a few minutes to complete. Wait until the configuration finishes.

Information				
•	PDMgr configuration completed successfully. The Manager's CA certificate is base64-encoded and saved in text file C:\Program Files\Trubil\Policy Director\\keytab\pdcacert.b64 You must distribute this file to each machine in your secure domain. It is needed for successful configuration.			
	ОК			

You now have a base64-encoded root CA certificate available in the file C:\Program Files\Tivoli\Policy Director\keytab\pdcacert.b64. Click OK. Now configure WebSEAL.

Select a package in the list then click Configure or Un	configure.	
		Close
Installed Packages	Configured	Refresh
Policy Director Runtime Environment (PDRTE) Policy Director Runtime Environment (PDRTE) Policy Director WebSEAL (PDWeb) Policy Director Authorization Server (PDAcld)	Yes No No	View log

Click Configure....



Leave the WebSEAL ports at the standard defaults. (The IBM HTTP Server HTTP ports should be set to 8888 and SSL at 4444 in *C:\IBM HTTP Server\conf\httpd.conf*.) Click OK.



Enter *passw0rd* as the Administrator Password and click OK. After a moment the configuration will start. Wait until the configuration finishes.

	×
Startup of the Access Manager WebSEAL (PDWeb)	Service
ОК	

Click OK. (If this fails, unconfigure and try it again.)

Policy Director Configuration		
Select a package in the list then click Configure or Un	configure.	Class
		Close
Installed Pack ages	Configured	Refresh
Policy Director Runtime Environment (PDRTE)	Yes	Viewlog
Policy Director Management Server (PDMgr)	Yes	view log
Policy Director WebSEAL (PDWeb)	Yes	
Policy Director Authorization Server (PDAcId)	No N-	
Folicy Director web Fortal Manager (PDWPM)	NO	Configure

Click Configure to start configuration of PDAcld.

🏘 Policy Director Administrator Password	×
Specify the password for the Policy Director Administrator (sec_master).	
Administrator Password	

Enter passw0rd and click OK. Wait until the configuration finishes.

Policy Director is now fully configured.

NOTE: The WebSEAL service has been renamed to "Access Manager WebSEAL" and will appear at the <u>top</u> of the services list like this:

64	Access Manager WebSEAL	Started	Manual	LocalSystem
----	------------------------	---------	--------	-------------

34. Installing and Configuring Web Portal Manager

By default, you won't be able to successfully configure Web Portal Manager installing it into WebSphere Application Server 4.0.2, because the labs use WAS Advanced Edition (WAS AE) for Multiplatforms and the beta configuration script only supports the Single Server version of WAS. So there is an extra BAT file you must run that will setup

Version 1.1 – 30 September, 2002

simulated commands so that WPM configuration will work with WAS AE.

34.1 Initial Procedure

Make sure WebSphere Admin Server and Admin Console are running. In the Admin console, make sure the Default Server is started. Open a DOS window and change to *D:\LabFiles\WPM* and run *SetupWPM.bat*. This will copy the simulation files to their proper directories. *PDWPM.xml* and *pdwpm.ear* are copied to WAS_HOME%\InstallableApps. These are the XMLConfig script and the application EAR, respectively.

The three BAT files copied are

- StopServer.bat does nothing but represents the command used to stop WAS Single Server version
- SEAppInstall.bat represents the file used to install applications into WAS Single Server version, and here uses XMLConfig and PDWPM.xml to install pdwpm.ear into WAS AE
- *StartServer.bat* does nothing but represents the command used to start WAS Single Server version. It's not necessary to stop and start WAS AE when installing an application

The PD Configuration GUI calls these three BAT files in this order. By copying these, you provide the Configuration GUI what it expects to find with WAS Single Server version.

Now back in the Policy Director Configuration dialog, select PDWPM and click Configure....

When the configuration completes, in the WebSphere Admin Console expand Enterprise Applications you should see Policy Director Web Portal Manager. Check if is running. Right mouse click on it and select Show Status.

Module	Status	Server
Policy Director We	Stopped	Default Server(Secureway7
PDWPM Delegate	Stopped	Default Server(Secureway7
PDWPM Self Regi	Stopped	Default Server(Secureway7

You need to start it if its status is Stopped. Close the status dialog and right mouse click on Policy Director Web Portal Manager again, and select Start. Click OK to dismiss the completion dialog. Show status again to verify it is running.

🌍 Module Status		_ 🗆 ×
Application - Policy D	irector Web Por	tal Manager
Module	Status	Server
Policy Director We	Running	Default Server(Secureway7)
PDWPM Delegate	Running	Default Server(Secureway7)
PDWPM Self Regi	Running	Default Server(Secureway7)

The dialog shows all three Web modules in the application are running. Now it can be tested to make sure the installation succeeded. Enter <u>http://<your</u> hostname>:9080/pdadmin in the browser of your choice. You should see the login screen for the Web Portal Manager.



Next go to <u>http://<your</u> hostname>:8888/pdadmin to include IBM HTTP Server in the path. You should see the same screen.

34.2 Enable SSL

The configuration of WPM adds a localhost stanza in the IHS configuration file, *C:\IBM HTTP Server\conf\httpd.conf*. Edit this file.

```
### BEGIN PDUMM CONFIG ENTRY ###
Listen 4444
LoadModule ibm_ssl_module modules/IBMModuleSSL128.dll
<VirtualHost secureway6:4444>
SSLEnable
SSLClientAuth none
DocumentRoot "C:\Program Files\IBM HTTP Server\htdocs"
ErrorLog logs\error.log
TransferLog logs\access.log
</VirtualHost>
SSLDisable
Keyfile "C:\PROGRA~1\Tivoli\POLICY~1\\keytab\pdwpm.kdb"
SSLV2Timeout 100
SSLV3Timeout 1000
#### END PDWPM CONFIG ENTRY ###
```

Find the PDWPM configuration stanza at the bottom and change the SSL port number from 443 (the default) to 4444, for the Listen entry and the <VirtualHost> entry. 4444 is the default IHS SSL port for the labs. Restart IHS to enable the change.

 \mathcal{V} Can you connect to Web Portal Manage using a secure SSL connection?

If you have a problem, check that WebSphere has a virtual host alias of 4444.

35. Verify the Configuration with PDADMIN and WebSEAL

35.1 Starting PDAdmin

Enter

C:\> **pdadmin** pdadmin>

> On Windows you can also start PDADMIN by clicking: START->Programs->Policy Director->Administration Command Prompt

Unauthenticated access

While you are still an anonymous user:

 $\ref{eq: 1}$ Issue help command, which commands are listed

 $\ensuremath{\widehat{\ensuremath{\mathbb{P}}}}$ Which commands can you execute as an anonymous user

 $\ensuremath{\widehat{\mathbf{v}}}$ What happens if you try listing the users and groups

Login as 'sec_master'

```
pdadmin> login
Enter User ID: sec_master
Enter Password: passw0rd
pdadmin>
```

 $\widehat{\ }$ How do you start and log into PDAdmin all on the same line?

35.2 Creating Users with PDAdmin

Create a user with user create. The format of the user distinguished name depends on the user registry you are using.

Using IBM SecureWay Directory Server

```
pdadmin> user create user1 cn=user1,o=ibm,c=gb user1 user1 passw0rd
pdadmin>
```

Try creating a user with a DN like cn=Avery Salmon,o=ibm,c=gb

Poes it work? If not, why not? (try "" for parms with blanks)

Try creating a user with DN like cn=Jon Harry,ou=pic,o=ibm,c=gb

Version 1.1 – 30 September, 2002

Does this work? If not, why not? (remember that all entries in LDAP require a parent entry)

Using Active Directory

pdadmin> user create user1 cn=user1,dc=<your domain name>,dc=com user1 user1 passw0rd

pdadmin>

Try creating a user with a DN like cn=Avery,dc=secureway7,dc=com

Poes it work? If not, why not? (try "" for parms with blanks)

Try creating a user with DN like cn=Jon,ou=pic,dc,secureway7,dc=com

² Does this work? If not, why not? (remember that all entries in LDAP require a parent entry)

Using Domino

There are some minor differences from the standard way (IBM Directory or MS Active Directory) in operating Policy Director based with Domino.

You should not use the Domino Administrator, while Policy Director Services are running. In particular, avoid changing the administrator identity, as Policy Director always uses the last identity with which a Lotus client has been closed. That applies to any Lotus client -- Domino Administrator, Domino Designer, Lotus Notes -- as they all share the same notes.ini (configuration file) and DLLs.

While creating or importing users and groups in Policy Director use the Domino-style Distinguished Names, rather than LDAP-style:

LDAP-DN:	cn=hugo,o=secureway
Domino-DN:	hugo/secureway

1. Create a user in Policy Director (don't forget to set account-valid to yes)

pdadmin> user create [-gsouser] [-no-password-policy] <user-name> <dn> <cn> <sn> <pwd> pdadmin> user create hugo hugo/secureway hugo user passw0rd

2. Import a user in Policy Director

First create a Domino Directory user using Domino Administrator or Lotus Notes client. In Policy Director:

pdadmin> user import [-qsouser] <user-name> <dn> pdadmin> user import hugo hugo/secureway

The same applies to the creation and import of groups.

35.3 Connect to WebSEAL

Start a browser and connect to one of your WebSEAL servers. Try to authenticate with one of your new users

> Are you able to successfully access the WebSEAL homepage? If not, why not? (is the account-active flag set to yes?) Use

pdadmin> user mod hugo acc yes

36. Configure WebSphere with Your User Registry

36.1 Objectives

In this lab you will create an administrator user for WebSphere in your user registry directory server, named *wasadmin*. This will be the user ID with which you'll log into WebSphere after you turn on WebSphere security. You will create users and groups for the Banker 2001 application that you'll run in WebSphere. The users you'll create for this application are

Users toto casey francoise maurice jean-paul sergei claude igor

Groups employees bank_clients

Some of the users will be members of the groups according to this illustration:



In the next sections there will be instructions to create these users and groups – one section per registry type. However, if you don't want to do this manually a command file has been provided to create all the users and groups with one command.

The command file is *D:\LabFiles\create_users-groups.bat*. It takes one parameter, the base DN of your directory' name context.

For IBM LDAP, enter o=ibm, c=gb

For Active Directory enter cn=users,dc=<your domain name>,dc=com

For example, cn=users, dc=secureway7, dc=com

For Domino enter <your domain name>

```
For example, secureway (note no "o=")
```

From a DOS prompt, run D:\LabFiles\create_users-groups.bat <base-DN>

This will create the Users and Groups to the directory of your choice. To verify success use a registry tool to confirm that the users and groups have been created.

The last steps are to configure WebSphere for your directory and to map the users and groups to the application security created in WebSphere for the Banker 2001 application.

36.2 Adding Groups and Users to IBM Directory Server

Note: This section provides instructions for manually creating Users and Groups in IBM LDAP. This is, obviously, not necessary if you have already used the **D:\LabFiles\Create_users-groups.bat** command file to create these Users & Groups. You may wish to confirm that these have been created successfully.

To do this, start the DMT (Directory Management Tool):

Start->Programs->IBM SecureWay Directory->Directory Management Tool

Add server		?
Ready		ibm.
Connect to directory serve	r	
Server name : Idap://	secureway6	
Port :	38900	
Use SSL :		
Certificate name :		
Authentication type :	O None I Simple I SASL External I O CRAM MD5	
User DN :	cn=root	
User password :	******* I	
Keyclass file name :		
Keyclass file password :		

When the DMT is loaded, add your server name and port, and bind as administrator filling in the fields.

Idap://secureway6:38900	Browse	tree	
Introduction	Ready		
B Status Administration Rebind	୦ ନ୍ତୁ Search	🛟 Expand	눱 Add
□- 😋 Schema □- D. Refresh schema 00- C. Object classes 00- Attributes □- D. Matching rules □- D. Datemage	Idap://sec secautho G o=ibm, - cn=localh	ureway6:3890 rity≔default c=ub osk	0
Directory tree			

Explore the three entries. Select the suffix o=ibm,c=gb and click on Add to create an LDAP user named *wasadmin* with the password *passw0rd*. This will be the user that is the WebSphere administrator.

🔹 Add an LDA	P Entry
Select an En	iny type, enter the Parent DN, modify the Entry RDN, then click OK.
Entry type	User 🗾
Parent DN:	o=ibm,c=gb
Entry RDN:	cn=wasadmin_
	OK Cancel Help

Fill in the fields and click OK. The next screen it is opened to provide further information such as the second name and password.

IBM Tivoli Access Manager 3.9 – Cookbook

				_
Ś	Add an LDAP User			×
T C	'o add a new user, enter a Co lick Add.	mmo	on name, Last name, and any other information for the use	r, then
0	bjectClass (Object class):		inetOrgPerson	Ŧ
d	in (DN):		cn=wasadmin,o=ibm,c=gb	
s	n (Last name):	2	wasadmin	
ir	nitials (Initials):	2		
С	n (Common name):	2	wasadmin	
l	Business Personal Other	1		
Γ	Loudiologiumor (Eurolo		annwory.	
	employeeType (Employee ty	pe):	2	
	mail (E-mail):		2	
	manager (Manager):		2	
	pager (Pager number):		2	
	roomNumber (Office numbe	r):	2	
	secretary (Secretary):		2	
	telephoneNumber (Office ph	none	e): 🖉	
	title (Title):		2	
	userPassword:		2 ******	
L	•			Þ
		A	dd Cancel Help	

Enter *passw0rd* as the password per the convention throughout these labs. In order to properly use the user with WebSphere you must also set the *uid* attribute with the same name you give for the *cn* attribute. Click on the *Other* tab.

Business Personal Oth	er	
street:	2	
teletexTerminalIdentifier:	2	
telexNumber:	2	
thumbNailLogo:	<u></u>	Type is binary no data defined
thumbNailPhoto:	<u>—</u>	Type is binary no data defined
uid:	2	wasadmin
uniqueldentifier:	2	
userCertificate:	<u>—</u>	Type is binary no data defined
userPKCS12:	<u>—</u>	Type is binary no data defined
userSMIMECertificate:		Type is binary no data defined
	Add	Cancel Help

Set the uid: field to wasadmin.

You should repeat all these steps for each user you need to create for the Banker 2001 application. Create a group and add some users on it. Always select the suffix o=ibm,c=gb first and then click on Add button. Select *Group* as entry type.

elect an En	try type, enter the Parent DN, modify the Entry RDN, th	nen click OK.
Entry type	Group 🔽	
Parent DN:	o=ibm,c=gb	
Entry RDN:	cn=employees	

Fill in the fields and click OK. In the next screen provide further information such as the group's member users.

🚸 Add an LDAP Group	×
To add a new group, enter a Cor click Add.	mmon name, and the members you want to add to the group, then
objectClass (Object class):	groupOfNames 🔽
dn (DN):	cn=employees,o=ibm,c=gb
General Other	
cn (Common name):	employees
member (Group members):	cn=claude,o=ibm,c=gb
description:	Ø

Click on the blue dot and a panel will open allowing you to import multiple users into the group.

😵 Edit multi-valued attribute men ber 🛛 🗵		
Enter one attribute value per line. 🖄 👘		
cn=claude,o=ibm,c=gb		
cn=sergei,o=ibm,c=gb		
cn=maurice,o=ibm,c=gb		
OK Cancel		

Add a user for each line and click OK when done.

If you do not use the BAT file to import all users and groups, repeat these steps for the other group, *bank_clients*, which you need to create for the Banker 2001 application.

36.3 Adding Groups and Users to Active Directory

Considerations

Note: This section provides instructions for manually creating Users and Groups in Active Directory. This is, obviously, not necessary if you have already used the D:\LabFiles\Create_users-groups.bat command file to create these Users & Groups. You may wish to confirm that these have been created successfully.

In order to provide authentication and authorization for applications running in WebSphere, users and groups need to be created in Active Directory. You will create the users and group using the Active Director console. Later you will import those users and groups into Policy Director.

Using the Active Directory GUI

Start the Active Directory console by running Start->Programs->Administrative Tools->Active Directory Users and Computers.

🗳 Active Directory Users and Computers			
Console Window Help			
Action ⊻iew	× 🖆 🖬 🖫 🛿 🦉	2 💆 🏷 V 🍕 🗑	
Tree	Users 20 objects	<u>z</u>	
Active Directory Users and Computers	Name	Type Type	verschpuon
🗄 🗊 secureway7.com	🕵 Administrator	User	Built-in account for administering the
🗄 🖳 Builtin	Cert Publishers	Security Group - Global	Enterprise certification and renewal a
🗄 💼 Computers	😰 db2admin	User	
🕀 🧭 Domain Controllers	5 DnsAdmins	Security Group - Domain Local	DNS Administrators Group
ForeignSecurityPrincipals	2 DnsUpdateProxy	Security Group - Global	DNS clients who are permitted to per
E	💯 Domain Admins	Security Group - Global	Designated administrators of the don
	Domain Computers	Security Group - Global	All workstations and servers joined to
Hard Tivoli PD Domains	💯 Domain Controllers	Security Group - Global	All domain controllers in the domain
Users	💯 Domain Guests	Security Group - Global	All domain guests
	💯 Domain Users	Security Group - Global	All domain users
	Enterprise Admins	Security Group - Global	Designated administrators of the ent
	Group Policy Creator Owners	Security Group - Global	Members in this group can modify gro
	5 Guest	User	Built-in account for guest access to t
	🥵 krbtgt	User	Key Distribution Center Service Acco
	😰 Idapdb2	User	
	🕵 RAS and IAS Servers	Security Group - Domain Local	Servers in this group can access rem
	🕵 Schema Admins	Security Group - Global	Designated administrators of the sch
	😰 superAdmin	User	-
	•		

First select the Users folder under your hostname. Then click the Create a new group icon.

ew Object - Group		X
Create in: securew	ay7.com/Users	
Group name:		
employees		
Group name (pre-Windows 2000)	ŀ	
employees		
Group scope	Group type	
C Domain local	Security	
Global	C Distribution	
C Universal		
] [
	ОК	Cancel

Enter *employees* as the Group name and click OK. Do the same for a group named *bank_clients*. Now you will add users and make some of them members of these groups.

Click the Create a new user icon just next to the Create group icon.

ew Object - User	X
Create in: secure	way7.com/Users
First name: jeff	Initials:
Last name: jeff	
Full name: jeff	
User logon name:	
jeff	@secureway7.com
User logon name (pre-Window:	\$ 2000):
SECUREWAY70\	ieff
	< Back Next > Cancel

Add a user named *jeff*. Use the same values for First name, Last name, and User logon name. Change the Full name back to a single *jeff*. Click Next.

New Object - User	X
Create in: secureway7.com/Users	
Password:	
Confirm password:	
User must change password at next logon	
User cannot change password	
Password never expires	
C Account is disabled	
< Back Next>	Cancel

Enter passw0rd as the Password and click Password never expires. Click Next and Finish on the confirmation dialog.

Repeat the process for all the users. See the beginning of section 36.1 for the list of users and groups, and their memberships. (All lower case letters, using *passw0rd* as the password.)

Now you need to add the users to groups as previously indicated. Some users are not in any groups and it is not required that a user belong to a group. In the Active Directory console right mouse click on user *jeff* and select Properties. On the Properties dialog click the Member Of tab and the Add... button.

Name	In Folder
🕫 remote-acl-users	secureway7.com/Tivoli PD Domains/default/syst
🕫 su-admins	secureway7.com/Tivoli PD Domains/default/syst
🕫 su-excluded	secureway7.com/Tivoli PD Domains/default/syst
🕫 employees	secureway7.com/Users
🕫 bank_clients	secureway7.com/Users
🐼 RAS and IAS Servers	secureway7.com/Users
🕺 DnsAdmins	secureway7.com/Users

Scroll down and highlight *bank_clients*, click the Add button. In this dialog you can add users to multiple groups if desired by multiply selecting the groups while holding the Control key down. Click OK. Click OK on the Properties

dialog.

Before you do the same for each user you've created, adding them to the group(s) according to the picture above, is there an easier way when several users belong to a group.

Yes. double-click on the bank_clients group, click on the Members tab, click the Add... button below, and Ctrl-click to select multiple users. Then click OK, and OK again. This is easier.

Now create a user in Active Directory named *wasadmin* with the password *passw0rd*. This will be the user that is the WebSphere administrator.

36.4 Adding Groups and Users to Domino Server

Note: This section provides instructions for manually creating Users and Groups in Domino. This is, obviously, not necessary if you have already used the **D:\LabFiles\Create_users-groups.bat** command file to create these Users & Groups. You may wish to confirm that these have been created successfully.

WebSphere Application Server Advanced Edition can use users and groups defined in the Domino Directory (aka NAB – Name and Address Book) for authentication and role definitions. The users **do not** have to be "Registered Users." They may be created as "Directory Users" or imported from an external source without necessarily being registered in Domino. The Directory Users can not access the Domino Server using a Lotus Notes Client, as they are not certified and do not have an ID file.

Creating Domino Directory Users

To create a Domino Directory User start the Lotus Domino Administrator and connect to your Domino Server. Navigate to "People & Groups" -> <Domain> 's Address Book -> People and click



Fill in the user information.

Name	
First name:	^ຕ maurice _
Middle initial:	r J
Last name:	[┏] maurice _
User name:	[™] maurice/secureway ₂
Alternate nam <u>e</u> :	
Short name/UserID:	^r maurice _
Personal title:	ſ J 🗖
Generational qualifier:	ſ . I
Internet password:	^r passw0rd_

Important: use syntax "<user name>/<domain name>" for the "User Name" field. This corresponds to the Distinguished Name: cn=maurice,o=secureway in the sample.

"Save & Close" the User Document.

The LDAP interface provided by the Domino Server does not support LDAP commands **ldapmodify** or **ldapadd**. So the creation or modification of the users through the LDAP interface is not possible.

Create all Domino users according to "Banker 2001 Users and Roles" using the Lotus Administration Client. Set all the passwords to passw0rd.

Now create a user in Domino named *wasadmin* with the password *passw0rd*. This will be the user that is the WebSphere administrator.

Creating Domino Groups

To create a Domino Group navigate to "People & Groups" -> <Domain> 's Address Book -> Groups and click



Fill in the Group information. You can immediately assign the users to the group according to "Banker 2001 Users and Roles". The syntax of the "Group Name" is here also important.

Group name:	$^{\mathbb{P}}$ employees/secureway _
Group type:	🖥 Multi-purpose 🛛 💌
Description:	r _
Members:	¹⁷ claude/secureway sergei/secureway maurice/secureway francoise/secureway _
Internet Address:	Г

Some useful LDAP commands

Important: Use the IBM LDAP client and its commands to search the Domino Directory. By default, the client is located under C:\Program Files\IBM\LDAP\bin.

```
To list all the users in the LDAP directory:
```

```
C:\Program Files\ibm\LDAP\bin>ldapsearch -h <LDAP host name> -p <LDAP port> -b "o=<Domino domain>" objectclass=inetorgperson
```

Use an administrative user account to get more detailed information (more attributes are visible):

```
C:\Program Files\ibm\LDAP\bin>ldapsearch -h <LDAP host name> -p <LDAP port> -D
"<Admin user>/<Domino domain>" -w passw0rd -b "o=<Domino domain>"
objectclass=inetorgperson
```

Get information about available Organization (aka O=...) entries. Policy Director creates one (O=Policy Director) to store information about its domain-wide users.

C:\Program Files\ibm\LDAP\bin>ldapsearch -h <LDAP host name> -p <LDAP port> -D "<Admin user>/<Domino domain> " -w <password> -b "" objectclass=organization

Take a closer look at a user entry (e.g. for user igor):

C:\Program Files\ibm\LDAP\bin>ldapsearch -h <LDAP host name> -p <LDAP port> -D "<Admin user>/<Domino domain> " -w <password> -b "o=<Domino domain>" cn=igor

36.5 Configuring WebSphere Security with Your User Registry

Considerations

This lab contains instructions for all three user registries. Where they differ each will be described in turn.

To use each user registry for authentication with WebSphere Application Server, there are some specific steps you must take. By default, none of the directories allows anonymous LDAP queries. To make LDAP queries or browse the directory, an LDAP client must bind to the LDAP server using the distinguished name (DN) of an account that has administrative rights on the directory.

Setting up the Registry in WebSphere

Make sure you've created a user named *wasadmin* with the password *passw0rd* in your user registry as described previously. This user is the WebSphere administrator account, the user ID you'll use to log into WebSphere after you've enabled WebSphere security. See the appropriate earlier section on this chapter for instructions on how to do this.

There are two types of accounts you need for this process. One is the administrative account with which WebSphere binds to the directory using an LDAP client. This is the *Bind Distinguished Name*. The other is an account already existing in the user registry that will become the WebSphere security administrator. This is the *Security Server ID*.

Make sure the WebSphere Admin Server is running and start the WebSphere Admin Console. Choose Console->Security Center... and click on the Authentication tab.

😭 Security Center		
General Authentication Role Mapping Run As Role I	Mapping Administrative Role	
Authentication Mechanism: 🔿 Local Operating Sy	stem	
Lightweight Third P	arty Authentication (LTPA)	
LTPA Settings		
* Token Expiration: 120 minutes		
✓ Enable Single Sign On (SSO)		
* Domain: secureway7		
Limit to SSL connections only		
Enable Web trust association		
Generate Keys Import Key	Export Key	
LDAP Custom User Registry		
LDAP Settings		
* Security Server ID: wasadmin	Port:	389
* Security Server Password: ********	Base Distinguished Name:	ecureway7,dc=com
* Host: secureway7	Bind Distinguished Name:	cureway7,DC=com
Directory Type: Active Directory 💌	Bind Password:	*******
Advanced SSL Configuration		
	OK Cancel	Apply Help

Click Lightweight Third Party Authentication to see the rest of the dialog. For labs coming up, click Enable SSO and enter your domain name (your hostname) as the Domain. Note that the Active Directory LDAP port is always 389 in these labs. The IBM Directory Server and Domino Server LDAP ports have been set to different values. Enter the following information in the LDAP settings fields:

• Security Server ID: wasadmin

This is the account ID of the user you created to be the WebSphere administrator.

• Security Server Password: *passw0rd* This is the password of the account chosen above.

• Directory Type: (choose yours) SecureWay / Active Directory / Domino 5.0

If you're using AD or Domino click on the Advanced... button. You can see that several of the LDAP Advanced Properties have changed to conform to the non-default directory. Temporarily set the Directory Type back to SecureWay to see the difference. Don't forget to set it back to Active Directory or Domino again.

If you are using IBM LDAP, you need to make the following change **IF** you want WebSphere to recognize groups created by Policy Director. (The create_users-groups.bat file uses PD, so you will need to complete this procedure if you did not create the users 'by hand' with the DMT).

This change is required because Policy Director creates groups of object class *accessGroup* and the default WebSphere search algorithm does not look for those type entries.

- 1) For 'Directory Type' choose Custom and click on Advanced
- 2) Change the 'Group Filter' to

(& (cn = %v)(|(object class = group Of Names)(object class = group Of Unique Names)(object class = access Group)))

I.e., add (objectclass=accessGroup) immediately after '...UniqueNames)'

3) Change 'Group Member ID Map' to

group Of Names: member; group Of Unique Names: unique Member; access Group: member; ac

I.e., add *accessGroup:member* to the end.

- 4) Click OK
- Host: <your registry hostname> This is the DNS name of the machine running your registry, e.g. secureway7.

Base Distinguished Name:

- For IBM Directory Server: *o=ibm,c=gb*For Active Directory: *DC=<your domain name>,DC=com*For Domino: (leave blank)
 The domain components of an account in the Administrators group in your registry, e.g.
- dc=secureway7,dc=com for Active Directory.

Bind Distinguished Name:

For IBM Directory Server: *cn=root* For Active Directory: *CN=Administrator*, *CN=Users*, *DC=<your hostname>*, *DC=com* For Domino: *cn=wasadmin*, *o=<your domain name>* The full DN of the account chosen just above from the Administrators group.

• **Bind Password**: *passw0rd*

The password of the account in the Administrators group used just above.

Now click on the Security Center General tab to display the first page of the wizard. Enable global security by checking the Enable Security checkbox. If you are asked to enter the LTPA password, enter *passw0rd*.

Click **OK** button to save the changes. Then Stop and restart the administrative server to make the changes take effect. Later, when you install an enterprise application into WebSphere, you'll be able to select users and groups from Active Directory to map to the enterprise application's configured security roles.

36.6 Mapping Users and Groups to Roles with the WebSphere Admin Console

Considerations

In J2EE, a security role is the central object in the configuration of application security for access control. On the application side when the application is assembled, permissions are granted to roles to execute methods on resources such as servlets and EJBs. On the user side at deployment time, users and groups are mapped to those roles. The net result is that users and groups now have the permissions.

When you install an application into WebSphere you can map users and groups to roles that are defined by the application assembler. You can also do this after the application has been installed. The Banker 2001 application has been preinstalled into WebSphere for you. (See section 47 Appendix B -- WebSphere Installation for reference.) You've defined users above that you will assign to roles already defined in Banker 2001.

Configuring the Banker 2001 Application

Start the WebSphere Admin Server and Admin Console if they're not already running. Expand WebSphere Administrative Domain, Nodes, your hostname, and Application Servers, and stop the Default Server by selecting it and clicking the Stop icon in the menu bar. (Stopping and restarting the Default Server may not be necessary.) Expand Enterprise Applications and select the Banker 2001 application. On the right side, click on the User/Role Mappings tab. This is where you will map users and groups to roles according to the associations in the following picture:



The WebSphere console allows you to select each role and assign users and groups.

IBM Tivoli Access Manager 3.9 - Cookbook

WebSphere Advanced Administrative	Console		- D ×
Consule view roots rielp Consule view roots rielp Consule view roots rielp			
🖻 🍿 WebSphere Administrative Domain		Name	
Server Groups	LI EJB Modules		
Gereway7 Gereway7 Gereway7 Gereway7			
Generic Servers	General User/Role Mappings Run/	As Mappings	
☐ ☐ Enterprise Applications ⊕ ☐ Secureway7_sampleApp	Roles	Users/Groups	Select
Policy Director Web Portal M Banker 2001	i customer janitor		48
H-C Resources	teller		
<u>ا</u>		<u>Apply</u> <u>R</u> eset	Help
Type Time	Event Message	Source	Options
08/02/02 11:45 SRVE0170I: Stoppi 08/02/02 11:45 SRVE0170I: Stoppi	ng web module: PowPM Delegate Admi ng Web Module: Policy Director Web Port	com.ibm.servlet.engine.ServletEn	Details
08/02/02 11:45 Command "Default	Server.stop" completed successfully.	-	

Highlight the *customer* role and click Select.... It turns out that all members of the *bank_clients* group have the permissions granted to the customer role.



Click the Select users/groups checkbox. The Search field will be enabled. Enter * and click Search. You should see a list of users and groups in user registry. (The picture above shows Active Directory entries.) Scroll down, highlight the bank_clients group, and click ADD >>. (You can hold down the Shift or Ctrl keys for multiple selections.) Bank_clients will be selected on the right. Click OK. Back in the Admin Console you should see *Selected users/groups* next to the *customer* role.

Repeat the above steps mapping *janitor*, *manager*, and *teller* roles to both groups and individual users per the picture. When you've finished all four roles, click Apply. Don't forget!

In WebSphere, after you modify the security of an application you need to restart the application for the changes to take effect. So select the Banker 2001 application, click the red "x" in the menu bar to stop it, and when it is stopped, click the green arrow to restart it.

36.7 Testing Banker 2001 Security

Starting the Application

Make sure WebSphere is running, Global Security is enabled, and that the Banker 2001 application is running. Open a browser and go to <u>http://localhost:9080/Banker2001</u>. (Case sensitive!)

? Why use port 9080? Where is the request received?

The Banker 2001 application welcome screen should display. At the bottom, select the <u>Users and Roles</u> link. You should see a picture in a second browser window showing the complete configuration of users, groups, roles, and methods. You can use this as a guide for testing which users can perform which tasks.

Other Application Functionality

Banker 2001 has some useful functions. Besides the banking functions of

- creating accounts,
- transferring funds, and
- viewing account balances, you can also
- view the headers the browser's request passed to the application,
- fill out a sample form to view the request parameters passed to the application,
- force a reauthentication (doesn't work with WebSEAL), and
- view the users, roles, and methods for which security has been configured.

Testing Security

In general, security is applied when you actually perform the task. For example, if you are user Igor and try to <u>View</u> <u>Balances</u>, you will be permitted to see the screen where you can enter an account number. But when you enter a valid number and click Get Balance, the application will tell you you are not authorized.

Review the Users and Roles screen and try various combinations of users and methods. At any point you can <u>View</u> <u>Request Headers</u> to see the basic auth header, decoded from base64.

Logged in as different users, try to create some accounts, try to transfer funds, and try to view balances to prove that WebSphere is providing the proper security.

When testing Banker 2001, if you receive "authorization failed" messages from the browser, return to the Admin Console and double-click on the last "authorization failed" message in the messages pane. You will see more detail about your error message. This might help to diagnose the problem.

Importing Banker 2001 Users and Groups into Policy Director

To prepare for labs to come, you need to import users associated with Banker 2001 from your standard user registry into PD. First make sure PDMgrd is running.

Import_users-groups.bat is in the *D:\LabFiles* directory. To run this you need to enter your directory's Base DN. For IBM LDAP, enter

o=ibm,c=gb

For Active Directory enter

Version 1.1 – 30 September, 2002

IBM Tivoli Access Manager 3.9 – Cookbook

cn=users,dc=<your domain name>,dc=com

For example, cn=users, dc=secureway7, dc=com

And for Domino enter

<your domain name>

For example, secureway (note no "o=")

From a DOS prompt, run D:\LabFiles\Import_users-groups.bat <GSO>

This will copy all the Banker 2001 users and groups to the PD domain. Wow! To verify that your import came off well, you can check using the Web Portal Manager by clicking on User->Search and searching for 100 users. You should see the Banker 2001 users in the list.

37. Multiple WebSEAL Servers on the Same Machine

This lab is the first of the WebSEAL enhancements. In this lab you'll configure WebSEAL to server multiple hosts on the same machine. Because WebSEAL doesn't offer true virtual hosting, it's necessary to configure multiple WebSEAL server instances to achieve this. In this lab, you'll do that in a couple of different ways. First, you'll configure a second WebSEAL server (named webseal1) with the same IP address as the first, but listening on different ports. Next, you'll configure a third WebSEAL server (named webseal2) with a different IP address.

37.1 Configuring a Second WebSEAL Server to Listen on Different Ports Using the Same IP Address as the Initial WebSEAL Server

[?] How many WebSEAL servers are configured in your environment? Hint: use a pdadmin server command to find that out.

The environment currently contains one WebSEAL server and one Authorization Server:

webseald-secureway5
ivacld-secureway5.secureway5.com

Configure a new WebSEAL Server (webseal1) listening on the ports 801 (HTTP) and 4431 (HTTPS) and communicating on port 7337 with the Management Server, as shown in the picture:



What command do you issue in order to configure the new WebSEAL server? Hint: Change to *PDWeb\bin* and run **ivweb_setup** to see which options you have.

```
C:\Program Files\Tivoli\PDWeb\bin>ivweb setup /?
       ivweb setup
Usage:
                      options
Options:
    -?
                        Print this usage
    -q
                        Silent mode. No message boxes only stderr
    -u yes|no
                        Allow unsecure HTTP access
    -r http port
                        Port for unsecure HTTP access
    -U yes|no
                        Allow HTTPS access
    -R https port
                        Port for HTTPS access
                        sec master password
    -m pdadmin pwd
    -i instance instance name
    -M mts listen port mts listen port
                       interface
    -n interface
```

Ultimate hint:

```
C:\Program Files\Tivoli\PDWeb\bin>ivweb_setup -u yes -r 801 -U yes -R 4431 -m passw0rd -i webseal1 -M 7337
```

It may take a couple of minutes -- be patient or get a cup of coffee (or both).

Use *pdadmin server show webseald-<your-host>-<instance-name>* to see, if the new WebSEAL instance has been registered in the PD Domain and see its configuration. The output will look like this:

```
webseald-secureway5-webseal1
Description: webseald/secureway5-webseal1
Hostname: secureway5.secureway5.com
Principal: webseald/secureway5-webseal1
Port: 7337
Listening for authorization database update notifications: yes
AZN Administration Services:
webseal-admin-svc
azn admin svc trace
```

Make sure that the new WebSEAL is listening on the specified ports. Hint: point the browser to the ports you expect the new WebSEAL server to respond on.

Can you figure out the WebSEAL HTTP and HTTP/S listening ports by using a pdadmin command? How can you check that? Hint: configuration files might be very helpful.

Create a junction to IBM HTTP Server running in front of your WebSphere Application Server.

```
pdadmin> server task webseald-secureway5-webseal1 create -t tcp -h localhost -
p 8888 /ihs
```

What parameters have you used? Fill in the parameters:

WebSEAL server name:

Name of the junctioned server:

Port of the junctioned server:

Junction name:

Hint: Take a look at httpd.conf located in *<IBM HTTP Server-home>\conf* and search for "port" to find out the IBM HTTP Server listening port.

Point your browser to the junction you have created to check that it works. Hopefully it does. Otherwise try to restart the WebSEAL instance you have created.

R How can you stop the instance? _____

What is the name of the Windows Service representing the new instance?

37.2 Configuring a Third WebSEAL Server to Listen on Ports 80 and 443 Using a Different IP Address than the Initial WebSEAL Server

For testing purposes you may not always have a physical network interface configured on your machine. Windows also supports virtual IP addresses, which you will use in the lab to configure the third WebSEAL instance, binding to it and listening on default ports 80 for HTTP and 443 for HTTP/S.

This section will only work for computers using static IP addresses - not DHCP.

It should also be possible to install the Loopback adapter and configure it to use IP.

Create a new virtual IP-address

On the Windows Desktop right-mouse click on "My Network Places."



Select Properties.



Select the icon representing the Token-Ring Adapter and right-mouse click on it.

耳 IBM PCI Toker	n-Ring Adapter		
		Configure	
Components checked are used by this connection:			
Client for Microsoft Networks			
File and Printer Sharing for Microsoft Networks			
Network Monitor Driver			
, ,			
Install	Uninstall	Properties 🙀	

Select TCP/IP Protocol and click on Properties.

Advanced...

Select the "Advanced" button near to the bottom of the window.

- IP addresses		
IP address	Subnet mask	
9.180.180.24	255.255.254.0	
,	Add Edit Remove	

One IP-Address is already configured (e.g. 9.180.180.24). Click on Add to create a virtual IP-address.



Choose an IP address of '10.10.10.x' where 'x'= the 4th number of the existing IP address. This will ensure that all machines on the subnet have a unique IP address.

The example shown here uses '24'.

Fill in the new IP-address using subnet mask of '255.255.254.0' click on "Add."

Close all windows by clicking OK buttons. The new virtual IP address is configured. You can now ping it (from your machine only).

Configure the Third WebSEAL Instance

Configure the new WebSEAL instance to bind to the new IP-address (10.10.10. x), listen on ports 80 and 443, and communicate through port 7437 with PDMGRD as shown on the picture.



Run

```
C:\Program Files\Tivoli\PDWeb\bin>ivweb_setup -u yes -r 80 -U yes -R 443 -m passw0rd -i webseal2 -M 7437 -n 10.10.10.x
```

After this command completes, point your browser to https://10.10.10. x or http://10.10.10. x to see whether the new WebSEAL instance responds on the ports 80 and 443 as configured.

Are you sure which WebSEAL instance is responding? Is that the one you expect? Hint: of course, there are many possible ways to figure it out. Here's an interesting one: try to edit index.html located in*PDWeb\www-webseal2\docs* with Notepad and substitute *iv30.gif* with *ivlogo.gif*. Try to access webseal2 once again.

Take a look at the configuration file of webseal2 in ... \PDWeb\etc

Which parameter lets WebSEAL listen only on the specified port? Hint: search for *network*.

[?] Can a WebSEAL instance be configured to listen on 2 of 3 available IPaddresses (if you would create one more virtual IP-address)?

37.3 Changing the Configuration of the Primary WebSEAL Instance

Why do we need this? Hint: The initial webseald instance is currently listening on all local machine IP addresses, and ports 80 and 443. You've just added the new webseald2 server instance that is listening on IP address 10.10.10.10 and the same ports.

Stop "Policy Director WebSEAL" Service.

Open the configuration file of the primary WebSEAL instance (...\PDWeb\etc\webseald.conf) in an Editor. You need to restrict the initial webseald instance to listen not on all IP addresses, but only your host's default IP address. This will avoid a conflict with webseald2.

Go to the *[server]* stanza and **add** a new *network-interface* option inside the stanza specifying the primary IP address (e.g. 9.180.180.24). Webseald2 is listening on the single virtual IP address you have added.

Hint: use *ipconfig /all* command to find out which IP addresses are configured on your machine.

Start all the configured WebSEAL instances and try to connect to them on configured ports and interfaces.

The Name and IP address resolution of MS Internet Explorer does not always work as expected. Often it is worth trying the same operation with Netscape.

37.4 Final Question

Can multiple WebSEAL instances on the same machine belong to different Policy Director Domains?

Hint: are they all not using the same RTE?

38. HTTP 1.1 Support

Among the enhancements to WebSEAL with Policy Director 3.9 is WebSEAL's ability to support HTTP 1.1 to the back-end Web server. Previously WebSEAL only handled HTTP 1.0 regardless of the Web server's capabilities. In

order to see the difference you need to be able to monitor the contents of the request as it is forwarded by WebSEAL to the Web server, and the subsequent response from the Web server back to WebSEAL.

To that purpose you will use a small Java application called **TCP Tunnel**. TCP Tunnel is packaged with Apache SOAP to monitor SOAP-based network traffic, but it can also monitor plain HTTP. TCP Tunnel allows you to view both the headers and the body content of the HTTP request and response. It listens to HTTP messages arriving on a particular port, displays them in a window, and then forwards the messages to their ultimate destination. The same happens with the returned result.

Running TCP Tunnel

TCP Tunnel is part of the SOAP classes that come with WebSphere.

? What does SOAP stand for and with what technology is it used?

To setup TCP Tunnel, open a new command prompt window and navigate to the $D:\LabFiles\TCPTunnel$ directory. Copy the contents to a new directory called $C:\TCPTunnel$. Run *setup.bat* to set the classpath correctly. Then to run TCP Tunnel, enter the following command:

C:\TCPTunnel\tunnel 9080

This is the equivalent of **java org.apache.soap.util.net.TcpTunnelGui 82 localhost 9080** inside the *tunnel.bat* file. The first parameter (82) is the port the tool listens on for new HTTP messages; the second and third parameters indicate the host and port that the request will be forwarded to. You can enter (and change) all parameters on the Java command line if you don't use the *tunnel.bat* file with its presets. You can reuse tests from previous exercises; the only change is the hostname or port number. In the above case you are going directly to WebSphere's embedded Web server from the browser.

You should see the TCP Tunnel application window open and ready to display requests and responses as they pass through. Make sure the IBM HTTP Server and WebSphere are running and in a browser enter

http://localhost:82/Banker2001/

Your TCP Tunnel window should look something like the following:

📓 TCP Tunnel/Monitor: Tunneling localhost:82 to localhost:9080			
From localhost:82	From localhost:9080		
GET /Banker2001/ HTTP/1.1 Host: localhost:82 User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.0 Accept: text/xml, application/xml, application/xhtml+xml Accept-Language: en-us Accept-Encoding: gzip, deflate, compress;q=0.9 Accept-Charset: ISO-8859-1, utf-8;q=0.66, *;q=0.66 Keep-Alive: 300 Connection: keep-alive Pragma: no-cache Cache-Control: no-cache	HTTP/1.1 200 OK Server: WebSphere Application Server/4.0 Content-Type: text/html last-modified: Mon, 04 Feb 2002 14:29:00 GMT Content-Length: 3272 Content-Language: en HTML PUBLIC "-//W3C//DTD HTML 4.0//E<br <html> <head></head></html>		
	<title>Banker 2001 Introduction</title>		
Listening for connections on port 82			
Using TCP Tunnel to monitor WebSEAL

Now you know TCP Tunnel is setup properly. But to use it to test WebSEAL-Web server communication, you need to set up a WebSEAL junction that points to localhost:82, the port on which you will have TCP Tunnel listening. In pdadmin, enter the following command to create a junction between WebSEAL and TCP Tunnel:

pdadmin> server task webseald-<your host name> create -t tcp -h <your host name> -p 82 /TCPTunnel

Created junction at /TCPTunnel pdadmin>

where webseald-<your host name> could be webseald-secureway7 for example.

You have TCP Tunnel forwarding requests to port 9080 already, so the overall flow is

Browser \rightarrow WebSEAL \rightarrow TCP Tunnel \rightarrow WebSphere Embedded Web Server

Now in the browser enter <u>http://localhost/TCPTunnel/Banker2001</u>/. You should be presented with WebSEAL's **Forbidden** page suggesting you re-access the page using HTTPS. Do that and you should be redirected by WebSEAL to

https://secureway7.secureway7.com:443/TCPTunnel/Banker2001/ or something similar where *secureway7* represents your host and domain names. Now take a look at what is displayed in TCP Tunnel.

👹 TCP Tunnel/Monitor: Tunneling localhost:82 to localhost:908	
From localhost:82	From localhost:9080
GET http://Secureway7.secureway7.com:80/Banker2001/ HTT via: HTTP/1.1 Secureway7:443 user-agent: Mozilla/5.0 (Windows; U; Windows NT 5.0; en-US accept-charset: ISO-8859-1, utf-8;q=0.66, *;q=0.66 host: Secureway7.secureway7.com accept: text/xml, application/xml, application/xhtml+xml, text/htr keep-alive: 300 connection: close accept-language: en-us pragma: no-cache cache-control: no-cache accept-encoding: gzip, deflate, compress;q=0.9 referer: http://localhost/TCPTunnel/Banker2001	HTTP/1.1 200 OK Server: WebSphere Application Server/4.0 Content-Type: text/html last-modified: Mon, 04 Feb 2002 14:29:00 GMT Content-Length: 3272 Content-Language: en Connection: close HTML PUBLIC "-//W3C//DTD HTML 4.0//EN" HTML PUBLIC "-//W3C//DTD HTML 4.0//EN" <head> <title>Banker 2001 Introduction</title></head>
	ear
Listening for connections on port 82	

Some of the headers shown that are new to, updated for, or required by HTTP 1.1 are

- via: HTTP/1.1 Secureway7:443
 - 1.1 as the HTTP protocol version number
- accept-*:
 - formalized in HTTP 1.1
- **host:** Secureway7.secureway7.com
 - mandatory in HTTP 1.1, servers must check for its presence
- **connection:** close
 - different from Keep-Alive
- cache-control: no-cache
 - forces end-to-end reload, addition to HTTP 1.0 pragma: no-cache

? What are some of the other new features HTTP 1.1?

Try the direct Java command line invocation of TCP Tunnel with different hosts and port numbers:

java org.apache.soap.util.net.TcpTunnelGui 82 <target host> <target port>

and check out the request and response headers when you access the host using

http://localhost/TCPTunnel/<URL>.

39. Forced Re-authentication, Constant Session ID and Session Termination

39.1 Enable Forms-Based Login

Since forced re-authentication won't work with Basic Auth, you need to change the authentication type to forms-based. It is possible to set up forms-based login for HTTP requests and leave BA for those over HTTP/S.

Locate the configuration file of WebSEAL server at ... *PDWeb\etc\webseald.conf* and open it in edit mode. Find the *[ba]* stanza.

[ba] #------# BASIC AUTHENTICATION #------# Enable authentication using the Basic Authentication mechanism # One of <http, https, both, none> ba-auth = https

Change it as shown to enable BA for HTTP/S connections only. Then find the [forms] stanza.

[forms]
#----# FORMS
#----# Enable authentication using forms
One of <http, https, both, none>
forms-auth = http

Enable it for HTTP connections.

Restart WebSEAL and call *http://<hostname>:<HTTP port>* from the browser. You should be presented with the WebSEAL login form.

39.2 Configure Forced Re-authentication

Assume that you want to enforce user re-authentication as the user accesses the chpwd.exe script to change their GSO

user IDs and passwords. The script is located in WebSEAL's cgi-bin directory.

What is the management entity that forces the user to re-authenticate while accessing an object:

- □ ACL
- □ POP
- Configuration file:

First create a POP.

pdadmin> pop create reauth

Call it reauth, for example.

pdadmin> pop modify reauth set attribute reauth yes

Set the POP attribute to enable forced re-authentication.

To enable the POP, attach it to the selected object (e.g. for WebSEAL on a server *secureway5*): /*WebSEAL/secureway5/cgi-bin/update pwd.exe*

pdadmin> pop attach /WebSEAL/secureway5/cgi-bin/update_pwd.exe reauth

You can attach the ACL to an object using pdadmin or WPM. The pdadmin command is shown.

Point your browser to the WebSEAL's entry page using HTTP (since forms-based login is configured for HTTP only) and login as the user of your choice, for example, *igor*.

Note: you might need to click the refresh button on your browser to display the page correctly.

Browse to any links on your WebSEAL server you are aware of, such as *HTTP://<your WebSEAL>:<port>/pkmshelp*

Point the browser to the URI on which you have applied the POP: http://secureway5/cgi-bin/update_pwd.exe

You should be presented with the login form again.

Can you continue browsing other pages you are authorized for even if you do **not** re-authenticate?

You are not allowed to use a user ID other than the one you have used for initial login (e.g. *claude*). But go ahead and try it to see what happens.

39.3 Constant Session ID

WebSEAL maintains a constant session ID throughout the lifetime of the user credential. This session ID is contained in the EPAC (PD credential), which can be transferred to a junctioned server as the value of the CGI-variable *iv_creds*. *iv_creds* can be parsed with aznAPI. But an easier way to retrieve the session ID on the back-end is to let WebSEAL insert it as the value of the CGI-variable *pd_session_id*.

Configure WebSEAL to Transmit the Session ID to the Junctioned Server

To enable the transmission of the WebSEAL session ID to the junctioned server, add the HTTP-Tag-Value attribute to the object representing a junction. You can do it via pdadmin or PD WPM.

Connect to PD WPM and authenticate as sec_master.

Object Space Browse

Click on *Object Space -> Browse* and navigate to the object representing a junction to WebSphere Application Server (e.g. junction1).

+ junction1

Click on the junction name to see the properties of the junction.

Extended Attributes

Object Name: /WebSEAL/secureway5/junction1

Click on *Extended Attributes*.

/WebSEAL/secureway5/junction1

Create New Attribute

Click on *Create New Attribute*.

Attribute Name: HTTP-Tag-Value

Attribute Value: user_session_id=PD_SESSION_ID

And fill in the fields as shown.

Finally, click on *Create*. From now on WebSEAL will be set up to transmit the session ID on *junction1*, as long as you have not turned off the parameter *user-session-id* in the *[session]* stanza of WebSEAL's configuration file.

Parsing the HTTP Request Header using Banker 2001

You can use a servlet in the Banker 2001 application that you should have deployed previously, to show the content of the HTTP Request Headers. Go through the junction1 that points to WAS to the initial page of Banker 2001: http://<hostname>:<port>/junction1/Banker2001.

Click on "View Request Headers." Depending on the application security configuration you may be prompted for authentication.

The direct URI of the servlet is

http://<hostname>:<port>/junction1/Banker2001/servlet/com.ibm.jeff.HeaderDumperServlet

Locate the variable containing the PD session ID.

What is the name of the variable?

It consists of two parts. The first (before the equals sign) represents the base64-encoded name of the WebSEAL server. The second part (after the equals sign) is the PD session ID. You can see the values just underneath.

The long, unintelligible PD session ID string can be used to terminate a user's session. You'll do that shortly.

39.4 Configure a Constant Session ID on WebSEAL

Reduce Session-Inactivity Timeout

For testing purposes you will reduce the session inactivity timeout for WebSEAL sessions from 600 (default) to 30 seconds.

Open webseald.conf in editing mode and locate the [session] stanza.

```
# inactive-timeout = 600
inactive-timeout = 30
```

Change *inactive-timeout* value to 30. Then restart WebSEAL (stop it and give a short grace period before starting again).

Point your browser to the HeaderDumperServlet going through WebSEAL, at http://<hostname>:<port>/junction1/Banker2001/servlet/com.ibm.jeff.HeaderDumperServlet

What is the displayed session ID? It is usually enough to note the first six characters of the ID.

Po you expect the session ID will change, if you reconnect to the URI after 30s? Why?

Try it again in just over 30 seconds and compare the session ID displayed with the one noted previously.

Turn on REAUTH-FOR-INACTIVE

By default, WebSEAL 3.9 (also all previous releases) deletes the session from its cache, if the session becomes inactive. To configure WebSEAL to <u>mark</u> inactive sessions rather than <u>deleting</u> them from the credential cache, find the *[reauthentication]* stanza.

reauth-for-inactive = no
reauth-for-inactive = yes

Change the reauth-for-inactive parameter to yes in the [reauthentication] stanza.

Restart WebSEAL in order to make the changes effective and call the servlet again at http://<hostname>:<port>/junction1/Banker2001/servlet/com.ibm.jeff.HeaderDumperServlet

Note the session ID displayed (first 6 characters)

Do you expect the session ID will change this time, if you reconnect to the URI after 30s? Why?

There are other parameters that manage the behaviour of the credential lifetime after successful re-authentication. They are also located in the *[reauthentication]* stanza.

? Can the same session ID be preserved over the lifetime of the credential?

You may want to restore the original value of *inactivity timeout* at the end of this lab. Otherwise you will be often forced to re-authenticate.

39.5 Terminating a User Session

Terminate a Specific User Session

Have you ever wanted to secretly kick yourself out of your own session? Given the known session ID (from the previous lab) you can terminate that session.

Open pdadmin CLI and login as sec master.

```
pdadmin> server task webseald-secureway5 terminate session
_bjxxPAQAAAAwAAAAEJ6XA3FaMjRmODJ6Z0lrUlNoczA1VGZDU1kyMnlkdC1wZVlmUWczOW5ab29wL
WdBQUFBQQ==
```

Issue the command to terminate the session, using the long session ID (after the equals sign) from the previous section. Replace the long session identifier shown here with your own.

Refresh the browser. If using forms-based login you will be prompted for re-authentication again. If you're using BA login you will just see that the session ID has been changed.

Terminate All Sessions of a Particular User on a WebSEAL Server

You can terminate all sessions of a particular user. Connect to WebSEAL and authenticate as a user of your choice, for example *igor*.

Open pdadmin CLI and login as sec master.

pdadmin> server task webseald-secureway5 terminate all sessions igor

Issue the command to terminate the session.

Refresh your browser to observe the same behaviour as described in the previous sample.

40. Switch User

40.1 Objectives

In this lab you will configure, enable and test the new Switch User functionality of WebSEAL 3.9.

40.2 Scenario

Let us declare that the user *igor* is assigned to the role *Manager* in *Banker2001*, and to be the supervisor in charge. The big boss. The head honcho. El capitan. Le PDG. He is allowed to act on behalf of *Employees* and *Customers*. However, he must not be allowed to act on behalf of other *Managers* (*Claude, Maurice*).

In terms of "switch-user" functionality, this scenario results in the assignment of users and groups as shown on the picture:



40.3 Assigning Users to the Groups

To start configuration of this scenario, add *igor* to the *su-admins* group but exclude *claude* and *maurice* from being switched to.

pdadmin> group modify su-admins add igor
pdadmin> group modify su-excluded add claude
pdadmin> group modify su-excluded add maurice

Members of *su-excluded* cannot be the target of a switch user.

Do you need to include the user *igor* to the group *su-exluded* to prevent a switch to that user?

40.4 Enabling the Switch User Functionality on WebSEAL

Edit webseald.conf and locate the [authentication-mechanisms] stanza.

[authentication-mechanisms]
su-password = C:\Program Files\Tivoli\PDWeb\bin\suauthn.dll

Add the su-password entry shown and restart WebSEAL.

40.5 Using the Switch User Function

If you have completed lab 39 Forced Re-authentication, Constant Session ID and Session Termination, you already have WebSEAL configured for forms-based login for HTTP connections, and BasicAuth login for HTTPS.

Make sure WebSphere Application Server is running and check whether you have a junction to WAS.

pdadmin> server task webseald-<hostname> create -t tcp -h <hostname> -p 9080 c all /junction1

If you don't already have one, you can use this command to create a junction (*junction1*) to WAS that will also supply the user ID, groups and PD credential. If you already have a junction, modify it (use –f option) to supply the additional information accordingly.

It would be useful to have the *Banker2001* application up and running. If you don't, use the Snoop servlet (*http://<wasserver>:9080/servlet/snoop*) to look into the HTTP request headers.

Point the browser to the WebSEAL that is listening for HTTP. You will be presented with a login form.

Authenticate as user igor

Point your browser to the HeaderDumperServlet, i.e.

http://<hostname>:<port>/junction1/Banker2001/servlet/com.ibm.jeff.HeaderDumperServlet

or click on View Request Headers on the Banker 2001 welcome page.

What user is authenticated as iv-user?

What is the session ID (first 6 chars)?

Call the switch-user URL at *http://<hostname>:<port>/switchuser.html*

Username sergei
 Destination URL /
 Authentication method su-forms

Fill out the fields where

- *Username* is the ID of the user to which you want to switch
- **Destination URL** is the URL you want to be redirected to and is relative to WebSEAL, i.e. "/" will bring you to the main WebSEAL page
- *Authentication method* corresponds to one of the configured *Authentication Mechanisms*. since you have configured only the *su-password* Authentication Mechanism, the password-based Authentication Methods are available: *su-ba* and *su-forms*

² In what directory can you find the file *switchuser.html*?

Point your browser to the *HeaderDumperServlet* at http://<hostname>:<port>/junction1/Banker2001/servlet/com.ibm.jeff.HeaderDumperServlet

You may need to refresh the browser window because the page may have been cached

What user is authenticated as (iv-user)?

? What is the session ID (first 6 chars)?

Now you have switched to another user (i.e. sergei) and have access only to the resources permitted for that user. You can set up an appropriate ACL in order to check it.

Proceed to pkmslogout at *http://<hostname>:<port>/pkmslogout*

Point your browser to the HeaderDumperServlet.

What user is authenticated as (iv-user)?

What is the session ID (first 6 chars)?

Since you have rolled-back to igor your permissions are restored and you can access resources available for igor.

Call the switch-user URL again and try to switch to user claude.

You are still *igor*. What prohibits you, as a member of the group *su-admins*, from switching to *claude*?

41. Caching data on POST method

There used to be a problem with WebSEAL that if

- 1) you were unauthenticated and filling in a form,
- 2) you tried to submit it with a POST to a protected resource and were sent to a login page where you authenticated,
- 3) and you then were redirected back to the form page,

the form data was lost. This could also occur if you were filling out a very long form and your session expired. In WebSEAL 3.9 the form data is now cached so that it is still present when the form is resubmitted. You'll test this in this lab.

For these lab exercises you will need to set up a junction to your IBM HTTP Server (IHS) on which WebSphere runs. Open a DOS prompt.

 $C: \ pdadmin - a \ sec_master - p \ passw0rd$

```
pdadmin> server task webseald-yourhost create -t tcp -h yourhost -p 8888
/websph
pdadmin> quit
```

Enter the commands to create the junction named /websph. 8888 is the IHS HTTP port. Quit pdadmin.

Because the problem of lost data on the POST method affects only form-based authentication, you need to enable this option in the *[forms]* stanza of webseald.conf file as shown.



Add the highlighted line.

In order to cause faster SSL session expiration change the default value for the SSL timeout to 30 seconds, unless you'd have a couple of coffees in the middle of each of the experiments in this lab!

#	Session	timeout	for	SSL	v3	connections	(range:	1-86400	secs)
#:	ssl-v3-ti	imeout =	7200)					
88	sl-v3-tim	neout = (30						

Restart WebSEAL to enable the changes.

```
http:// yourwebseal/wbsph/Banker2001
```

Connect to the main page of the Banker 2001 application using the junction you just created, and authenticate to Policy Director using one of the pre-existing accounts (for example toto/passw0rd)



Follow the link to this lab's the test page. Don't panic if you are asked to authenticate again; probably you have exceeded the SSL timeout. You are now in the main part of the lab.



In this sample page select and copy in the clipboard all the text in the 4000-byte column.

Cut + Paste here :		
Global Sign-On grants users	access to	th
authorized to use - through	a single l	og
consisting of multiple syste	ms and app	li
distributed computing enviro	nments, GS	0
manage multiple user names 🛛	, Undo	þз
creating ~GSO aware~ junctio		W
resources and GSO resource (Cut	f
Manager.When WebSEAL receive	Copy	È.
junctioned server, WebSEAL (Paste	P
authentication information.	Dajete	۴V
	Select All	

Paste in the text area above and wait for at least 30 seconds before submitting the data to be sure that session expires.

If the session has successfully expired, as soon as you submit the data you should be redirected to the Policy Director login form page. Login again you will see that all your data has been successfully sent to the server, which is so happy to show you what has been sent!

Now submit more data so that you overflow the caching capacity. Going back with your browser to the submission form page, clear the form with the button.

X Clear the form		
	5000 byte:	5
Global Sign-On Grants Users Ac To Use — Through A Single Lo Multiple Systems And Applicati Environments, GSO Eliminates And Passwords. The Integration 1 WebSEAL And Back-End Web First Be Created Using The Web For A Resource Located On The	cess To The Comput gin. Designed For L Cut Cot Naste Select All	ing Resources They Are A arge Enterprises Consisting erous, Distributed Compu ers To Manage Multiple ng "GSO Aware" Junction 'es And GSO Aware" Junction tes And GSO Resource GA webSEAL Resource GA 'ebSEAL Asks The GSO
The Appropriate Authentication Mappings—For Each Registered	Print) Server Contains A Datab Alternative User Names

Copy 5000 bytes in the clipboard paste the data into the form again. Again wait at least 30 seconds before submitting to be sure the session expires. Login again to recover the SSL session when requested.

[?] Does it still work? What happened?



Policy Director shows you this screen. In order to again have a kiss from Banker 2001, change the amount of the data that WebSEAL will cache by editing the *[server]* stanza in the webseald.conf file.

<pre># request-body-max-read = 409</pre>	96
request-body-max-read = 5096	т
	1
# When a user is prompted to	authenticate before a request
# can be fulfilled, the data	from that request is cached
# for processing after the co	ompletion of the authentication.

Change the buffer size to 5096, save the file, restart WebSEAL, and try repeating the submission of 5000 bytes. Don't forget to wait a while before clicking on the submit button!

You should now be able to see that the backend server has received all the 5000 bytes and is offering you a kiss in gratitude!

You've completed this lab. Be sure to restore the default values for the parameters you've changed (SSL timeout and Form Based login) in the webseald.conf file to continue with the successive labs.

42. TLS support

By default, WebSEAL is configured to support all three kinds of SSL protocols,

- SSL v2
- SSL v3
- TLS v1

This can be verified in the SSL stanza of webseald.conf, where all three kind of SSL protocols are enabled.



Force WebSEAL to use only TLS by modifying the webseald.conf, disabling SSL.

Restart WebSEAL and try to connect to it with IE5.

 $\ensuremath{\widehat{}}$ Can you do it? If not, why not?

By default IE5 is not configured to use TLS, so this feature must be enabled in the advanced property page of the browser. In IE select

Tools->Internet Options->Advanced.



Check the TLS checkbox and click OK.

Now try to connect to WebSEAL and after authenticating, right-click with the mouse on WebSEAL's home page.



You should see the properties window that shows the protocol in use.

Re-edit webseald.conf and turn back on SSL v2, SSL v3 and TLS, like the original configuration. Save the file and restart WebSEAL.

Again point your browser (where TLS is still enabled) to WebSEAL. Right-click on the HTML page and you should see that with all three protocols enabled both on server and client, the handshaking procedure always selects the strongest security protocol, in this case TLS.

43. Integration of Policy Director and WebSphere Application Server

43.1 Objectives

Using WebSEAL, Tivoli Policy Director can provide authentication for J2EE applications running in WebSphere. Policy Director can also provide programmatic authorization for applications running in WebSphere. Now Policy Director 3.9 can be integrated with WebSphere Application Server to externalize and centralize authorization of J2EE applications. In this exercise you will install, configure, and test this integration.

There are two overall software components in this integration, PD for WAS and the Migration Tool.

The overall process will be to

- 1. Install PDWAS
- 2. Install and setup the migration tool
- 3. Migrate the WAS Admin Server application security to PD
- 4. Tell WAS to use PD for authorization

- 5. Test PD and WAS integration
- 6. Migrate the Banker 2001 application security to PD
- 7. Test it all

In more detail, you will

- 0. Unzip the PDWAS 3.9 classes
- 1. Perform PDWAS installation and configuration
 - a. Install PDWAS
 - Run Install_PDPerm.bat
 - b. Create a user in PD to represent the WAS JVM & add it to the remote-acl-users group - For example, name the user pdwas or wasjvm
 - c. Run configure_PDPerm.bat or manually run pdjrtecfg and SvrSslCfg
- 2. Install and setup the migration tool
 - a. Run install.bat in "migrate" directory. This
 - Creates PDWAS/migrate Directory in same place as Policy Director
 - Copies files to that directory

b. Create a PD User for WebSphere Administrator (or an Import the user if already in LDAP)

- For example, the user wasadmin
- 3. Migrate the WAS Admin Server application
 - a. Edit migration script (run_WIN32.bat on Win32) to set it up for your machine and point the ear name to the WAS Admin Server ear
 - b. Migrate the WAS Admin Server application by running run_WIN32.bat
- 4. Tell WAS to use PD for authorization
 - a. Activate PD authorization in WAS by modifying the WAS sas.server.props files
- 5. Test PD and WAS integration
- 5. Migrate Banker 2001
 - a. Export Banker2001.ear (No. Due to a bug, use the installable one without user-role mappings)
 - b. Edit run_WIN32.bat to point it to the Banker 2001 ear file
 - c. Migrate Banker2001 security to PD
- 6. Test it all

Initial Setup

You've already installed Web Portal Manager. Now you will install the additional files and do some setup necessary to enable integration. Navigate to *D:\LabFiles\PD39WAS* and double click on *PDWAS39_Windows.zip*. Unzip the files to the same directory, creating the *websphere* folder.

Perform PDWAS Installation and Configuration

🔍 websphere		
File Edit View Favorites Tools Help		100 A
📙 🖨 Back 🔹 🤿 🕣 📩 🔯 Search 🛛 🔂 Folders	(∰History 🔤 📴 🗦	< m III.
Address D:\LabFiles\PD39WAS\websphere		▼ @Go
Folders	× 🝙 🌔	
🖃 🛅 properties		
😟 💼 💼 com	bin lib	install_PDPerm uninstall_PD
🗄 💼 logbr		.bat
🕀 💼 temp		
🗀 tranlog		

Open the websphere folder and double click on install_PDPerm.bat. This will copy the PDWAS runtime components

in the bin and lib directories to their corresponding directories below *C:\WebSphere\AppServer* (%WAS_HOME%). Files copied are

- WebSphere LIB directory
 - o jaas.jar, PDPerm.jar, PDWASAuthzManager.jar, application_1_2.dtd
- WebSphere BIN directory

 configure_PDPerm config script

Check that PD Management and Authorization Server are running.

The configure PDPerm.bat file still has some problems. You will run its commands manually.

```
In case configure_PDPerm is fixed, it will be run like so:
C:\WebSphere\AppServer\bin>configure_PDPerm pdwas passw0rd <auth server
hostname> <mgt server hostname>
But don't do this now.
```

Run

```
C:\Program Files\Tivoli\Policy Director\sbin>pdjrtecfg -action config -
java_home %was_home%\java\jre
```

This copies newer versions of the necessary files including .jar files to their proper directories for use by WAS. It also creates a *PolicyDirector* directory under %WAS_HOME\java\jre\lib.

Next, run the Java class manually that is run normally by configure_PDPerm.bat

C:\WebSphere\AppServer\bin>java com.tivoli.mts.SvrSslCfg pdwas passw0rd secureway7 secureway7

This creates a new Policy Director URAF user named pdwas-secureway7 in your user registry. In Active Directory, for example, the user has the following DN: CN=pdwas-secureway5,CN=users,CN=default,CN=Tivoli Policy Director Domains,DC=secureway5,DC=com.

This user appears to be different from the pdwas user created above. We do not need to create that pdwas user in advance though, since the SvrSslCfg command will do it. The new user is not in the normal AD users group, only in PD's group.

Take a look at the files created:

%WAS_HOME%\java\jre\lib\security\pdperm.ks %WAS_HOME%\java\jre\pdperm.properties

pdperm.ks is the key file.



pdperm.properties describes the configuration of how WebSphere will use the PD Java API to authenticate to PD.

Setup the Migration Tool

Policy Director needs to be able to handle authorization for the WebSphere Admin application application itself. You will import a user that is authorized to run the Admin Console and then you will migrate the Admin Server application authorization to Policy Director.

The *wasadmin* user ID is the one used to log into the WebSphere Admin Console. Import the user *wasadmin* already defined in the directory you are using into Policy Director domain. In pdadmin, enter the following two commands. If you're using the IBM LDAP server, enter

pdadmin> user import wasadmin cn=wasadmin,o=ibm,c=gb
pdadmin> user modify wasadmin account-valid yes

For Active Directory enter

pdadmin> user import wasadmin cn=wasadmin,cn=users,dc=<domain name>,dc=com pdadmin> user modify wasadmin account-valid yes

For Domino enter

pdadmin> user import wasadmin wasadmin/<domain name>
pdadmin> user modify wasadmin account-valid yes

Run D:\LabFiles\PD39WAS\migrate\install.bat. This will create a new migration directory called C:\Program Files\Tivoli\PDWAS\migration and copy all the files in the migrate directory to it. These files are

• migrate.jar, PDPopulate.dll (JNI file), Scripts for running Migration Tool, dtd files

Migrate the WAS Admin Server Application

Change to this new directory and with a text editor edit the file *run_WIN32.bat*. This is the BAT file used to perform the actual migration.

🕐 UltraEdit-32 - [C:\PROGRAm files\Tivoli\PDWA5\MIGRATion\run_WIN32.bat]
🗾 Eile Edit Search Project View Format Column Macro Advanced Window Help
D 😅 🗗 💕 🅦 🐘 🖩 🗊 🕼 🖷 🥵 📴 🕸 📾 🎇 🎇 端 🐴 🕾 🔩 🖓 👙 🙆 🔕 🗈 🌘
Import_users-groups.bat updatePD java files.txt run_WIN32.bat
<pre>set XML_PARSER_PATH=*was_home*/lib/xerces.jar set JDK_PATH=*WAS_HOME*/java/jre/lib/src.jar set JDK_DIR=*WAS_HOME*/java/jre set CACF_DIR="C:/Program Files/Tivoli/PDWAS/migration/migrate.jar" set CLASSPATH=*UJK_PATH*;*XML_PARSER_PATH*;*CACF_DIR*;. set PATH=*PATH*;C:/Program Files/Tivoli/PDWAS/migration/ set EAR_NAME=*WAS_HOME*/config/admin.ear</pre>
java -classpath %CLASSPATH% com.tivoli.pdwas.migrate.Migrate -j %EAR_NAME% -a sec_master

Change the first line to set the correct path for *xerces.jar*, the XML parser. Verify that all other parameters point to the right paths as shown on the screenshot above. (You're using the JDK that comes with WebSphere.) If it doesn't already, set the EAR_NAME variable to point to the Admin Server ear file, *admin.ear*.



Add the highlighted portions of the line above to specify the WebSphere administrator name. The above illustration shows the IBM LDAP suffix. For Active Directory, use

sec_master -p passw0rd -w wasadmin -d dc=<your domain name>,dc=com

For example

```
sec master -p passw0rd -w wasadmin -d dc=secureway7,dc=com
```

For Domino, enter

sec master -p passw0rd -w wasadmin -d <your domain name>

For example,

```
sec master -p passw0rd -w wasadmin -d o=secureway
```

Save the file and close the editor.

Check that you have java.exe in your PATH environment variable. Type **java** at a command prompt. If the command is not recognized, add *%WAS HOME%javabin* to your system path, close the DOS window, and open a new one.

Open a DOS prompt and navigate to the migration directory you created just above, *C:\Program Files\Tivoli\PDWAS\migration*. Run *run_WIN32.bat* to perform the migration. You may ignore the warning about current members of pdwas-admin.

Tell WAS to use PD for authorization

Now PD knows about WAS, but on the other side, you need to tell WebSphere that it is to use Policy Director for authorization. Navigate to the *%WAS_HOME%*/*properties*/ directory and with a text editor edit the files *sas.server.props* and *sas.server.props.future*.

Read the comments at the top of either of these files to learn their purpose. If you search through these files for "auth," you'll see several mentions of "authentication" but none for "authorization." That's because until now WebSphere has been able to use an external authentication service but not an external authorization service. Not any more...!

Add the following line to the bottom of each file:

com.ibm.websphere.security.authorizationTable=com.tivoli.pdwas.websphere.PDWAS
AuthzManager

Save both files and close the editor.

Known Problem: At the time of this writing there can be a problem with the ACL attached to the \WebAppServer\deployedResouces\AdminRole\admin object. You may need to manually attach the _WebAppServer_deployedResources_AdminRole_admin ACL to replace the _WebAppServer_deployedResources_AdminRole_admin_ACL ACL. Migrating another application will also fix the problem.

You will take the first approach and manually attach the replacement ACL in *pdadmin*. (Enter the next command all on the same line. There's a space between admin and _WebAppServer....)

```
pdadmin> acl attach /WebAppServer/deployedResources/AdminRole/admin
_WebAppServer_deployedResources_AdminRole_admin
```

43.2 Testing PD and WAS Integration

Restart WebSphere. Policy Director will now be used to authenticate and authorize the administrator (wasadmin) when you start the WAS Admin Console. In the Admin Console you should see a message after you log in that says a vendor authorization table has been loaded. WebSphere will now use this external service for authorization decisions.

To prove this, add a new temporary administrator for WAS by adding another user to the *pdwas-admin* group, using **pdadmin**. Start pdadmin and if you're using IBM LDAP enter

```
pdadmin> user create tempwasadmin cn=tempwasadmin,o=ibm,c=gb tempwasadmin
tempwasadmin passw0rd pdwas-admin
pdadmin> user modify tempwasadmin account-valid yes
```

If you're using Active Directory, enter

```
pdadmin> user create tempwasadmin cn=tempwasadmin,dc=secureway7,dc=com
tempwasadmin tempwasadmin passw0rd pdwas-admin
pdadmin> user modify tempwasadmin account-valid yes
```

where secureway7 should be replaced with your domain name. If you're using Domino, enter

pdadmin> user create tempwasadmin tempwasadmin/<Domino domain name> tempwasadmin tempwasadmin passw0rd pdwas-admin pdadmin> user modify tempwasadmin account-valid yes

For example,

pdadmin> user create tempwasadmin tempwasadmin/secureway tempwasadmin tempwasadmin passw0rd pdwas-admin

Restart the WebSphere Admin Console and log into the Admin Console as *tempwasadmin*. The Console should start just the same. You've convinced WebSphere to trust a different administrator than the one with which it was originally configured. Policy Director has authenticated and authorized this user to WebSphere because the user is also a member of the *pdwas-admin* group. (You can verify that *wasadmin* is still configured in WebSphere by opening the Security

Center and selecting the Authentication tab. Security Server ID should still be set to wasadmin.)

You could, for example create a time-restricted administrator for WebSphere that is only authorized during the

afternoon.

```
pdadmin> group create night-pdwas-admin cn=night-pdwas-admin,o=ibm,c=gb night-
pdwas-admin
pdadmin> pop create pdwas_admin_time_control
pdadmin> pop modify pdwas_admin_time_control set tod-access anyday:1200-
1600:local
pdadmin> pop attach /WebAppServer/deployedResources/AdminRole/admin
pdwas_admin_time_control
pdadmin> acl modify _WebAppServer_deployedResources_AdminRole_admin set group
pdwas-admin TB[WebAppServer]i
pdadmin> acl modify _WebAppServer_deployedResources_AdminRole_admin set group
night-pdwas-admin T[WebAppServer]i
pdadmin> user create time-wasadmin cn=time-wasadmin,o=ibm,c=gb time-wasadmin
time-wasadmin passw0rd night-pdwas-admin
pdadmin> user modify time-wasadmin account-valid yes
```

The example above is for the IBM LDAP server. Just change the distinguished name in the user create command. Now

try to log in as time-wasadmin. If it's already after the valid time, wait till tomorrow and test to see if you can log into

the WebSphere Admin Console at various times of the day to test this functionality.

43.3 Migrate the Banker 2001 Application Security to Policy Directory

Objectives

Now you will migrate the security management of a real application from WebSphere into Policy Director. Back in section 36.7 you imported the Banker 2001 users and groups from your user registry into Policy Director. Now it's time for the Banker 2001 application roles.

The Banker 2001 application has four roles configured: *manager*, *teller*, *customer*, and *janitor*. Associated with these roles are users and groups. These associations were created when users and groups were selected for each role in the WebSphere Admin Console. When this was done, WebSphere did not modify the original EAR file.

Normally in order to include the user-to-role mappings, you need to export the application back out from WebSphere as an EAR. That one will contain the user-to-role mappings and these should be migrated to PD. However, at the time of this writing the PD Migration application cannot import the roles and associations with users and groups properly.

Procedure

The following section, delimited by ###### characters, is left here for reference but should not be performed. It may be

re-included when the PD Migration Tool can correctly import WAS user/group-to-role mappings.

Make sure the Policy Director services are running, that the WebSphere Admin Server service is running, and start the WebSphere Admin Console if necessary. Create a directory called *C:\export*. In the Admin Console expand WebSphere Administrative Domain and Enterprise Applications, right mouse click on the Banker 2001 application and select Export Application....

To Export Applicat	tion
This application is Select a node fron export the applicat exported under the file name as Bank	; installed on following node. In the list, and give the directory to tion. The application will be e selected directory with the EAR ter_2001.ear.
Node:	Secureway7
Export directory:	C:\export
]	OK Cancel

Go to the *C:\export* directory and open *Banker_2001.ear* with WinZip. Extract *application.xml* and *ibm-application-bnd.xmi*also to the *C:\export* directory also. These will extract into the *meta-inf* subdirectory. Open application with a text editor and verify near the top of the file that the <display-name> element value of Banker 2001 is exactly the same as that shown for the enterprise application in the WAS Admin Console.



The name in each is **Banker 2001**. Consistent. If it is not, you need to rename one or the other. The easiest is to rename the enterprise application in WebSphere. Click on the application in the WebSphere Admin console, select the General tab, change the name, and click Apply.

Due to the bug with user/group-role migration, you'll migrate the Banker 2001 application using the existing Banker2001.ear located in C:\Websphere\AppServer\installableApps\Banker2001.ear. Navigate to C:\Program Files\Tivoli\PDWAS\migration. Edit run_WIN32.bat. In run_WIN32.bat change the line that sets the EAR NAME value to

Set EAR_NAME=%WAS_HOME%/InstallableApps/Banker2001.ear

Run run WIN32.bat.

You may get an error message like this

User already defined in the URAF Registry.

The reason for this behaviour is an unexpected response after running a pdadmin command that adds a user to a group already containing that user. The workaround is to remove the user *wasadmin* from the group *pdwas-admin* e.g. by issuing this command:

pdadmin> group modify pdwas-admin remove wasadmin

Then run run WIN32.bat again.

To verify the command succeeded, open Web Portal Manager, browse the object space, expand Root->WebAppServer->deployedResources, and notice that you've got the four roles that are part of the Banker 2001 application, namely *customer*, *janitor*, *manager*, and *teller*.

Now you need to modify the ACLs separately to associate users and groups with those roles. To make life easier, there is a BAT file that will do this. Navigate to *D:\LabFiles* and run *Import_users_groups_to_ACL.bat*. This will create a temporary file named *import_users_groups_to_ACL.list* that will be used by the BAT file to set up the ACLs of users and groups in Policy Director for each of the Banker 2001 roles. (If you want to see the .list file REM out the deletion of it in the BAT file.)

Testing Banker 2001 Security with Policy Director

Using the same procedure you used when you first tested users and groups in Banker 2001, test security now that Policy Director is in charge. See section 36.7 Testing Banker 2001 Security for those instructions.

- Wow that Policy Director is managing authorization, what happens if you remove one or two of the user/group-to-role mappings in the WebSphere Admin Console?
- [?] If you add a new user in PD and map that user to one of the Banker 2001 roles, will this mapping show up in WebSphere?

44. Form Based Single Sign-On

In this lab you will learn how to configure the form-based single sign-on facility of WebSEAL for two applications already installed in WebSphere. These apps make use of a form-based login page for authentication purposes. The first application for which you will create a FSSO facility is the Web Portal Manager.

So with this exercise you will achieve two goals:

- 1) Protect WPM access with WebSEAL just like any other application on the back-end WebSphere, and
- 2) Make the Policy Director user *igor* able to administer Policy Director using WPM as if he were the *sec_master* user. Heady stuff, no?

44.1 Part 1

To achieve these two goals, login to pdadmin as *sec_master* and run the following commands. The first creates a GSO resource named *wpm_sso*. The second creates a GSO credential for user *igor*, for that GSO resource.

pdadmin> rsrc create wpm_sso -desc "resource for WPM Single Sign On login"
pdadmin> rsrccred create wpm_sso rsrcuser sec_master rsrcpwd passw0rd rsrctype
web user igor

Now create a config file that will be used by the FSSO procedure to retrieve information for any form-based login you want to use. Open a text editor and create a file with the following entries:

```
[forms-sso-login-pages]
login-page-stanza = wpm
```

```
[wpm]
login-page = /*/auth/handleLogin.jsp
login-form-action = handleLogin.jsp
gso-resource = wpm_sso
argument-stanza = wpm-login
[wpm-login]
```

```
userid = gso:username
password = gso:password
```

Save the file as *fsso.conf* in C:\Program Files\Tivoli\PDweb\etc\.

It is important to notice that in the *[wpm-login]* stanza there are two arguments that WebSEAL should look for in the login page. WebSEAL should replace them with two gso values: username and password.

Now modify the junction you have already created for WebSphere in order to include this new config file.

```
pdadmin> server task webseald-yourhostname create -t tcp -h yourhostname -p
8888 -f -S "C:\Program Files\Tivoli\PDweb\etc\fsso.conf" /websph
```

If the fsso.conf is error-free your junction should be created successfully.

Open a browser and point to <u>http://yourhost/websph/pdadmin</u>, and login using *igor* and *passw0rd*. You should now get into the WPM main page without authenticating as *sec_master*.

What happens if you login to WebSEAL as *toto*?

44.2 Part 2

THE FOLLOWING SECTION, 44.2, IS TEMPORARILY BROKEN DUE TO A BUG IN THE BETA OF THE SELF-REGISTRATION WEB APPLICATION, WITHIN THE WEB PORTAL MANAGER. YOU ARE THEREBY EXCUSED FROM DOING THIS LAB SECTION.

In the second part of this lab you will describe a sample application that allow administrators to easily create users by providing only their user name, surname and password. Before doing this though, a login page for the administrator is required.

This application is already loaded on your WebSphere machine and you can access it directly without WebSEAL by pointing your browser at *http://yourhost:8888/register*.

Address 🙋 http://secureway6:8888/register/register/regControl.jsp?method=cł	neck 💽 🤗 Go
Administrator Information	
This is a sample web application used for Policy Director User Se The Administrator information is required the first time the applicat NOTE: The information is NOT stored in a secure manner and sho environment.	If Registration. tion is run. ould NOT be used in a production
Administrator Name: sec_master	*
Password: *******	*
LDAP DN: o=ibm,c=gb	*
Submit User	_

Fill in the fields as shown and you should now be able to access the next page, where you can create a new user.

Address 🙋 http://secureway6:8888/register/register/regControl.jsp	
User Self Registration	
This is a sample web application used for Policy Director Us The User information is used to create a user in Policy Direc <first name=""><last name="">.</last></first>	er Self Registration. tor with a user ID of
First Name: new_	*
Last Name: user	*
Password: *******	*
Verify Password: *******	*
Submit User	_

Fill in the fields and click Submit.

Address 🙋 http://secureway6:8888/register/register/regControl.jsp		•	∂Go	🧲 DA
User Self Registration				
now upor : Upor registered que	accef			
new_user . Oser registered succ	.6221	uiiy		
First Name: Last Name: Password:	* * *	4		
Verify Password:	*			
Submit User				

Your successful submission is confirmed.

Now add some more lines to the fsso.conf file as described below:

```
[forms-sso-login-pages]
login-page-stanza = slfreg
[slfreg-login]
admin = string:sec_master
password = string:passw0rd
suffix = string:o=ibm,c=gb
```

Save the file. In order to make this new data available to WebSEAL, reload the junction using pdadmin command line

```
pdadmin> server task webseald-yourhostname create -t tcp -h yourhostname -p
8888 -f -S "C:\Program Files\Tivoli\PDweb\etc\fsso.conf" /websph
```

Open your browser, point to <u>http://yourhost/websph/regiser</u> and login as any of the users defined in Policy Director (e.g. *toto/ passw0rd*) to see what has changed.

? By itself now, can this Policy Director user create a new PD user?

We have any user not yet defined in PD able to create an account for themselves, and be sure that no one can sniff their password when they create the account?

45. Installation and Configuration of the Policy Director Web Plug-In for Microsoft Internet Information Server (IIS)

45.1 Objectives

As you know, Policy Director now can run in the form of a plug-in to popular Web servers. The first Web server supported on Windows is IIS. In this lab you will install, configure, and test the new Policy Director Web plug-in with IIS.

Important: When you install IIS you must be disconnected from the network. Otherwise, you-know-what will happen!

45.2 Prerequisites

Check the prerequisites for configuring and running Policy Director Web Plug-In for IIS - PD WebPI:

- Policy Director Run Time Environment (PDRTE) and Policy Director Management server (if it is to be installed on the local machine) must be installed and configured.
- There must be an installed and configured WWW-Service on the IIS Server.

- To install the WWW-Service, go to Control Panel -> Add/Remove Programs -> Add/Remove Windows Components. Select and configure Internet Information Service. Be sure to disconnect you machine (unplug the cable) from the network while doing this. Before it is patched, IIS is a magnet for viruses of various kinds.
- Stop the IIS Service if it has started
- Apply the Win2K Fix Pack and the IIS Patch
- Reconnect to the network
- o Restart the Web Server Service

45.3 Installation of Policy Director Web Plug In for IIS

Navigate to the Policy Director WebPI image location at

D:\LabFiles\PDimages\PDWebPI_020207\Disk Images\Disk1



Run setup.exe to start InstallShield.

Choose English as the language for the installation on the next screen and click OK.

Click Next to confirm installing Access Manager Plug-in for Web Servers and click Yes agreeing with the IPLA on the next screen.

Access Manager Plug-in for Web Servers

Access Manager Plug-in for Microsoft Internet Information Services

Choose both packages to install the Plug-in for Web Servers and the Plug-in for Microsoft IIS as shown. Click Next.

The installation routine will present you with a couple of familiar screens where you click

Next for the 1st screen, Yes for the 2nd, Next for the 3rd confirming the install of the package to its default location, *C:\Program Files\Tivoli\PDWebPI*, and Next for the 4th choosing *Typical* as the type of the installation.

Click Finish after the short splash showing the progress of the installation.

Repeat these installation steps for the next package.

The Policy Director Web Plug In for IIS is now installed.

45.4 Configuring new Virtual Hosts on IIS

Considerations

At the time of this writing the WebSEAL plug-in had some known problems remaining with the default virtual hosts defined in IIS. Names containing spaces, such as "Default Server" (the default IIS server) and "Default Administration Server," were not processed correctly. So for testing purposes and to avoid these problems, you should create a virtual host that directly accesses the test directory that will be used.

Procedure

1) Run Start -> Programs -> Administrative Tools -> Internet Services Manager

📲 Internet-In	formationsdienste					_ 🗆 🗵
	v] 🗢 🔿 🔁 🖪	1 🗗 🗗 🛼 😫] 💂 🕨 🔳	II		
Tree		Description	Sta	ate	Host Header Name	IP Address
🝓 Internet-Info	ormationsdienste	🧶 Default Web Site	Ru	inning		* All Unas:
🗄 🖳 * secure	wav9	Administration Web :	5ite Ru	inning		* All Unas:
🕀 🚷 Def	Connect					
🗄 🔂 Adır	Disconnect					
	Backup/Restore Confi	guration				
	Restart IIS					
	New	ETD Site				
	14677	Web Site				
	View	· · · · · · · · · · · · · · · · · · ·	-, , ,			
	Refresh					
	Export List					
	Properties					
	Help					
<u> </u>		•				F
New Web Site						

2) Right-click on the server -> New -> Web Site



 Fill in the name of the Virtual Host. Because the intent of the lab is to serve the content of the IBM Directory Server Manual, which is by default part of the LDAP Client installation, name the virtual host LdapDocs.



4) Fill in the port. The labs use port 888 (IIS labs default), since the default of 80 is used by WebSEAL. Leave the Host Header field empty.

Web Site Creation Wizard	
Web Site Home Directory The home directory is the root of your Web content subdirectories.	
Enter the path to your home directory.	
Path:	
G:\PD\LDAP\web\enus1252	Browse
Allow anonymous access to this Web site	

5) Enter the path to the directory containing your Web site files. As the IBM Directory Server Client is installed on every machine, we use the html manual files for our web site. Navigate to the location of the LDAP client manual (e.g. c:\Program Files\ibm\ldap\web\enus1252). Allow anonymous access to this Web site. In the next dialog allow read and execute access and finish the wizard.

The new virtual host is now defined in IIS and is listening on port 888.

6) You might want to set up the default Web page pointing to an existing file.



On Internet Services Manager Console right-click on the virtual host LdapDocs, then Properties. Click on the "Documents" tab and the Add... button. Fill in the name of an existing file (e.g. *getting_started.htm*). You've now configured a new virtual host and setup a default Web page for it that points to the IBM LDAP Directory Server documentation.

Now check that it works by pointing your browser to http://<hostname>:888.

45.5 Configuring the Policy Director Web Plug-In for IIS

1) Use the configuration tool shipped with the Policy Director WPI to install the plug-in and protect the new virtual host. Run the configuration tool by selecting

```
Start -> Programs -> PDWPI -> Configuration
and go through the configuration steps:
Access Manager Web Plug-In Configuration
 Please enter 'u' for unconfiguration or 'c' for configuration : c
Gathering the necessary configuration information...
Which virtual hosts are to be protected:
         1. Default Web Site
         2. Administration Web Site
         3. LdapDocs
Menu choice [?,??,all] > 3
 Enter the Access Manager Administrator ID : sec_master
 Enter the Access Manager Administrator password : passw0rd
 Enter the port number to listen on for AZN updates [7237] :7737
Do you want to enable SSL communication between the
Access Manager server and the LDAP server (y/n) [y]
                                                       : n
Configuring the Web Plug-In (this may take a few minutes)...
```

Starting the server.

Note: The Web server must be restarted before the changes will take affect.

The plug-in configuration was successful.

🍇 Services						Ľ
] <u>A</u> ction ⊻iew] ← →	· 🛍 🖪 🚰 🔂 🖧 🔮 🗍	▶ ■ ■	5			
Tree	Name 🛆	Description	Restart Ser	vice tup Type	Log On As	
Services (Local)	Reformance Logs and Alerts	Configures		Manual	LocalSystem	
	🍓 Plug and Play	Manages d S	Started	Automatic	LocalSystem	
	Policy Director Auto-Start Service			Manual	LocalSystem	
	Relicy Director Web Plug In	S	Started	Automatic	LocalSystem	
	Rint Spooler	Loads files S	Started	Automatic	LocalSystem	
	Rotected Storage	Provides pr S	Started	Automatic	LocalSystem	_

2) In order to load the plug-in, first start the plug-in service as shown, and then restart the IIS Web Server by either restarting the "IIS Admin Service"



or using the MMC for IIS.

* securewa	y9 Properties	? ×
Internet Infe	ormation Services	
Master I	Properties Edit the properties inherited by all sites created on this computer.	
	Master Properties: WWW Service Edit	

3) Check that the plug-in is installed and configured. Click on the server and then on Properties. Choose the "WWW Service" and click on Edit.

W Service	Master Prop	erties for	securewa	iy9			
Documents Web Site	Directory S Operators	ecurity Perfo	HTTP He mance	aders ISAPI	Custom Filters	Errors Home	Service Directory
Filters insta executed i web sites.	alled here are a n the order liste	ctive for all d below. 1	web sites o These filters	in this co are not	omputer ar displayed	nd are on individ	lual
[Status F	ilter Name		Priority		Add	
T	1 SS Ci	pifilt ompressior	1	High High		Rem	ove
ţ	n pr	lwebpi d5filt		High Low		E dit Ena	ble
Details—							
Filter Nam	ie: pdwebp						
Status:	Loaded						
Executab	le: G:\PRO	GRA~1\	pdwpi-iis.dl				
Priority:	High						
		OK	Cano	el	Apply		Help

Click on to the "ISAPI Filters" tab, which shows installed IIS plug-ins. It should contain "pdwebpi," for Policy Director Web Plug In Filter.

4) Configure forms-based login for Policy Director WebPI. Modify the PDWebPI configuration file. It is located by default at *C:\Program Files\Tivoli\PDWebPI\etc\pdwebpi.conf*.

```
# authentication = BA
authentication = forms
session = session-cookie
# session = BA
post-authzn = forms
post-authzn = tag-value
post-authzn = acctmgmt
```

Go to [common-modules] stanza and modify it as shown (changes are in bold).

Important: be sure to comment out the line beginning with session = BA as shown.

Save the file and close the editor.

No Services					×
🛛 Action View 🗍 🖛 🖻) 🗈 💽 🗳 🚱 😫 🗍	▶ ■ II ■►			
Tree	Name 🛆	Description Restart S	ervice tup Type	Log On As	
Services (Local)	Rerformance Logs and Alerts	Configures	Manual	LocalSystem	
W	🍓 Plug and Play	Manages d Started	Automatic	LocalSystem	
	Relicy Director Auto-Start Service		Manual	LocalSystem	
	Relicy Director Web Plug In	Started	Automatic	LocalSystem	
	Rrint Spooler	Loads files Started	Automatic	LocalSystem	_
	Rotected Storage	Provides pr Started	Automatic	LocalSystem	-

5) Restart the PD WebPI Service.

The PD Web Plug-in is now installed and configured.

45.6 Using Policy Director WebPI for IIS

The PDWPI can be managed using the Web Portal Manager. How about protecting resources served by IIS?

At the time of this writing if you run PDWebPI as a service it won't show you the objectspace. In order to view the objectspace you may need to run PDWebPI in the foreground. The command is

C:>\Program Files\Tivoli\Policy Director\PDWebPI\bin\pdwebpi.exe -foreground

Procedure

1) Point the browser to *http://<your_hostname* >:888 (e.g. <u>http://secureway9:888</u>), the IIS port for the labs. By default (at the time of writing) the server is not protected, so this request is to the IIS default page.

2) Connect to PD Web Portal Manager or, if you prefer CLI, use pdadmin CLI to perform the following operations. Point the browser to the PD WPM and authenticate as **sec_master**. Navigate to Object Space -> Browse.

	Path	ACL	POP
Ξ /		default-root	
- +	Management	default-management	
	PDWebPI	default-pdwebpi	
H	🛨 Default		
4	EdapDocs		
	🛨 config		
	🛨 dmt		
	- 🛨 doc		
	_ <u>+</u> getting_started.htm		
	+ help		
	└── readme		

3) New object entries have appeared. As PD WebPI works on a virtual host basis, there is no notion of the server that PD WebPI is running on, rather just virtual host names. Take a look at the default-pdwebpi ACL by clicking on it.

Cre	eate New Ent	rγ	
	Entry Name	Туре	Permissions
	<u>sec_master</u>	User	Tcmdbva[PDWebPl] rmdNRM
	<u>iv-admin</u>	Group	Tcmdbva[PDWebPl] rmdNRM
		Any-other	T[PDWebPI]rmdNRM
		Unauthenticated	T[PDWebPl]rmdNRM

4) Unauthenticated users are granted the permissions to access the Web resources on the Web server protected by PD WPI. The permissions to access IIS resources protected by PD WebPI are put together in a separate Action Group. In order to see it navigate to

ACL ->List Action Group -> PDWebPI

PD	WebPl		
Cre	eate Ne	ew Action	
	Name	Label	Туре
	r	Read	PDWebPI
	m	Modify	PDWebPI
	d	Delete	PDWebPI
	N	Create	PDWebPI
	R	Property Read	PDWebPI
	M	Property Modify	PDWebPI

5) Protect the IIS server on your machine from the unauthenticated access modifying the default-pdwebpi ACL.

default-pdwebpi

		Set Desc	ription
Cre	eate New Ent	rγ	
	Entry Name	Туре	Permissions
	sec_master	User	Tcmdbva[PDWebPl] rmdNRM
	<u>iv-admin</u>	Group	Tcmdbva[PDWebPl] rmdNRM
		<u>Any-other</u>	T[PDWebPl]rmdNRM
		Unauthenticated	Т

Change the permissions for Unauthenticated as shown.

6) Point the browser to *http://<your hostname>:888*. You are presented with the login page of PD WebPI. Log in providing the user ID and password of any valid user.

– Cookie Infi	ormation		
Name	PDWPI-SESSION-COOKIE		
Domain	localhost		
Path	/		
Expires	End of session	Secure	No
Data	lu9wX6ZzEnb23fxELQo1cS9EsNYFyCto	gyPX2jeyjwv	vo= 🔺

7) If you turn on warnings when receiving cookies on your browser, you will see the cookie from PD WebPI. Navigate to *http://<your hostname>:888/pkmshelp* to see available pkms options like

- pkmspasswd for password change
- pkmslogout for logout

8) Log out by clicking on pkmslogout.

9) You can start the PD WebPI in foreground mode rather than as a Service. Consider the order of the actions as follows:

- stop PD WebPI Service - stop IIS (WWW Service)

- navigate to the PD WebPI "bin" directory and issue

c:\Program Files\Tivoli\PDWebPI\bin>pdwebpi -foreground

- start IIS (WWW Service)

45.7 Unconfiguring Policy Director WebPI for IIS

Considerations

At the time of the writing of these labs, creation of additional virtual hosts in IIS was not automatically propagated to PD WebPI. If you want to add additional virtual hosts that you have created in IIS, you have to completely unconfigure PD WebPI and configure it again specifying the virtual hosts of your choice.

By unconfiguration of PD WebPI the modifyed configuration file (*PD WebPI home>\etc\pdwebpi.conf*) is deleted. To preserve the modifications, backup the file before unconfiguring the PD WebPI.

By unconfiguration of PD WebPI the object corresponding to the IIS virtual hosts previously configured is removed from the object space.

Procedure

To unconfigure PD WebPI run Start -> Programs -> PDWebPI -> Configuration

Access Manager Web Plug-In Configuration

Please enter 'u' for unconfiguration or 'c' for configuration : ${\tt u}$

That's all there is to it. Now you can reconfigure, including other virtual hosts required.

45.8 What You Did in this Lab

In this lab you installed the Policy Director Web Plug-In into IIS. You created a virtual host to bypass problems the plug-in had with virtual host names having spaces. You configured PD WebPI and turned on security for IIS-served resources. Then you unconfigured PD WebPI so that you could have it support additional virtual hosts.

46. Appendix A -- Installation

46.1 Installing IBM HTTP Server 1.3.19

Install IBM HTTP Server 1.3.19

Use Windows Explorer to go to D: Lab Setup HTTP-1-3-19 and launch the setup.exe..



Accept English as the language and the license agreement. As the destination folder select *C:\Program Files\IBM HTTP Server*.

Compact Custom Turpical
Typical

Select *Custom* as the installation type. click Next.

🗸 HTTPServer base	23786 K	Application Files	3995
Base Extensions	1362 K	Apache Source	3107
Machine Translation	32 K	Documentation	16103
HTTP Administration	17362 K	Additional Modules	536
		✓ Icons	44

Select all components (unless you do not have enough space on the system). Click Next.



Enter "Administrator" and "passsw0rd" for user id and password used to start the server as a service.

Do not reboot now when asked and click on Finish.

Configure IBM HTTP Server 1.3.19

Since you are going to be installing WebSEAL on the same machine it would be good to change the HTTP Port for the HTTP Server at this point

Open the server's main config file, C:\Program Files\IBM HTTP Server\conf \httpd.conf, with a text editor find the Port entry.

Port: The port the standalone listens to.
Port 80

Change it to 8888, the default IHS port for the labs.

Port: The port the standalone listens to.
Port 8888

Save the changes and close the file.

46.2 Installing GSKIT

It is a good idea to install the latest GSKIT, necessary to correctly run PD 3.9 later. Doing this now will avoid the

automatic installation of an older version with other packages requiring SSL (for example, the IBM SecureWay Directory Server).

Use Windows Explorer to open D: Lab Setup GSKIT 5.0.4.56. Drag-and-drop setup.ini on top of setup.exe.

This unusual procedure is required because we are using a package that it is usually part of an automatic installation.

Accept all the default options than click on finish. Should you need to uninstall GSKIT from your machine, use this command:

C:\>isuninst -f"C:\Program Files\ibm\gsk5\gsk5BUI.isu"

46.3 Installing DB2 7.2

In order install WAS 4.0 later, you should install *DB2 7.2 Enterprise Edition* with *FixPack 4*. If you were just planning to run *IBM Directory Server 3.2.2*, the *DB2 7.2 Personal Edition* would suffice.

Use Windows Explorer to open D:\Lab Setup\db2_7.2_Base and launch the setup.exe. Then click on Install.



You do not need to install the application development client. Select the other two. Click Next.



Perform a custom installation to install some administration components that could be helpful to have when working with WebSphere.



Select the indicated components. The gray'd out components are always installed anyway, so deselect everything else except Administration and Configuration Tools. Click Next.



Choose to create a DB2 instance. Click Next.



Choose to configure the three default services and click Next.

	Username	db2admin
	Password	********
A state	Confirm password	
	Use the same values for the remaining DB2 Username and Password settings	

Enter *db2admin* as the user ID and *passw0rd* for the password. Select the option to use these values also for the other DB2 services.

You probably haven't defined a db2admin user on the system already, so you will be asked if the setup procedure should create it for you. Say yes unless you have some other reason to create it manually. continue with the installation. When the installation finished, skip the registration procedure.

Installing DB2 FixPack4

Use Windows Explorer to open D: Lab Setup db2 7.2 Base and launch setup.exe.

It is good practice to stop all the DB2 services before launching the installation program. Otherwise, the installation program will force all the DB2 processes to shut down before proceeding. Accept this since you don't have any applications still running that rely on DB2. Next accept all the other defaults to complete the installation.

Configure DB2 to use JDBC 2

WebSphere 4.x uses the JDBC 2.0 database drivers, but DB2 installs the JDBC 1.1 drivers by default. You need to change to the JDBC 2.0 drivers for DB2. Open the Services panel.

Sec	Automatic	LocalSystem	
DB2 JDBC Applet Se	Manual	.\db2admin	

If running, stop the DB2 processes that use JDBC as shown. Open a DOS prompt and go to *C:\Program Files\SQLLIB\java12*.
Run *usejdbc2.bat* and be sure that all the files are correctly copied as shown. Your DB2 is now ready to be used by WAS 4.0, and even by IBM Directory Server in case you plan to use this as your user registry for PD 3.9.

46.4 Installing IBM SecureWay Directory Server 3.2.2

Use Windows Explorer to open the drive where the D: Lab Setup | dap 322 | dap 32 u and launch the setup.exe.

Accept English as installation language, and accept the licence agreement and the default installation directory.

The set-up procedure should find DB2, the GSKIT and the IBM HTTP Server already installed, if all the steps described before have been successfully completed. Select Custom Installation.

Custom Installation	2	×
	The following components are not currently installed.	
	Components ✓ Client 3.2.2 40358 K ✓ Server 3.2.2 22416 K DB2 V7 2 0 K	

By selecting a custom installation you can verify that only the components not yet installed, such as the LDAP Server and Client, are selected. Click Next.



Accept the creation of a program folder in the Programs menu. When asked, select all three options to configure as shown. Click Next.



Enter *cn=root* and *passw0rd* for the Administrator DN and password. Click Next.



Select the default DB2 database (non-UTF8) and click Next.

 $\ref{eq:constraint}$ What is UTF-8 and how does it affect the format of the database contents?

If you've got multiple drives available, select drive C if there is enough space free.



Since you may have multiple Web servers configured on your machine (IBM HTTP Server, Internet Information Server and/or Domino) select IBM HTTP Server for directory administration. Click Next.



Verify that the IHS configuration file is in the right path. Click Next and proceed with the installation.

Restart the machine and after rebooting, log in as *Administrator*. You will see that the configuration of the LDAP database takes some time. If the configuration completes successfully you can go on to configure of the directory for Policy Director. If not, run the installation again using Start->Programs->IBM SecureWay Directory->Directory Configuration. Select the same options you selected in this lab. And good luck!

Configuring IBM SecureWay Directory Server 3.2.2 for PD 3.9

Now it's time to perform some management tasks on the LDAP server. Ensure that IBM HTTP Server and the LDAP Server are running



Point a browser to <u>http://yourhost:8888/ldap</u> and Logon as cn=root and passw0rd.



Expand Settings and click on General. In the General Settings page change the port the Server listens on from the default 389 to 38900, as per the table in section 31.5 IBM Directory Server Configuration Options. Click Update. Then on the left click on Suffixes.

Address 🛃 http://secureway6:8888/	dap/cgi-bin/ldacgi.exe?Action=Start		
Directory Server Introduction Settings General Performance Transactions Event notification Suffixes Referrals Security Replication Database Current state Data	Suffixes secureway6 The list was successfully up To add a suffix, enter the d Suffix DN secAuthority The table below displays so checkbox and click Updat beneath that suffix, however	dated. You must <u>restart the server</u> for istinguished name of the suff /=Default uffixes defined to this server, e. Removing a suffix elimina r the data is not removed fro	or this change to ix, then click To remove tes access to om the direct
Dogoff	Current server suffixes	Comment	Remove?
	cn=localhost	System suffix	
	o=ibm, c=gb	Contains no directory data	

Add the Suffix DN o=ibm, c=gb (as per conventions for this lab) and the Policy Director suffix, *secAuthority=Default*. Click Add after entering each one.

Restart the server by clicking on the restart the server link. The LDAP server is ready to be used by Policy Director 3.9.

46.5 Installing Active Directory

Before You Start Installation

Active Directory can be used as the user registry with Policy Director

It is best to have the Active Directory installation process create and configure the DNS automatically. If you've already created a DNS manually that you want AD to use, you must change the DNS to allow dynamic updates before starting the AD install. The default is to only allow secure updates and the AD installation will not be able to update the DNS. To change this, select the DNS management console from Start->Programs->Administrative Tools->DNS.



From the right mouse click Properties.



Change Allow dynamic updates to Yes and click OK. Now the Active Directory install wizard should be able to properly configure the DNS.

Note that if you proceed through Active Directory installation with a manually created DNS and you have not made this change, you may see the following dialog at the end of AD installation:

Error! Objects cannot be created from editing field codes.

Active Directory installation was successful but has not been able to finish the DNS configuration. However, it will have created a text file with all the necessary information you need to update the DNS yourself. The file is *C:\WINNT\system32\config\netlogon.dns*. The information in this file must be concatenated with the existing DNS settings and the combination used to reconfigure the DNS. *C:\WINNT\system32\dns\samples192.DNS* is a sample file you can use to see which entries must be set for your DNS.

Installation of Active Directory

Now, to begin the Active Directory installation, select

START->Programs->Administrative Tools->Configure Your Server. When the dialog comes up click on Active Directory on the left side.



IBM Tivoli Access Manager 3.9 - Cookbook

Scroll down and click on Start the Active Directory wizard. The wizard leads you through Active Directory installation. When the Welcome to Active Directory Installation wizard opens, click Next.



Select Domain controller for a new domain and click Next.



Select Create a new domain tree and click Next.

A domain tree is a hierarchical grouping of domains that have contiguous DNS domain names, e.g. tivoli.com, child.tivoli.com, grandchild.child.tivoli.com, etc.



Select Create a new forest of domain trees.

A forest is one or more domains that share a common schema and global catalog. A forest can contain one or more domain trees.

New Domain Name Specify a name for the new domain.
Type the full DNS name for the new domain.
If your organization already has a DNS domain name registered with an Internet naming authority, you can use that name.
Full DNS name for new domain:
secureway7.com

Enter a name, such as <yourhost>.com, for the DNS of the new domain and click Next.

You might see a message that another NetBIOS name was selected due to name conflicts on the network. Accept this by clicking OK.

ctive Directory Installation Wizar	d	×
NetBIOS Domain Name Specify a NetBIOS name for the	new domain.	X
This is the name that users of ea domain. Click Next to accept the	rlier versions of Windows will use to identify the new name shown, or type a new name.	
Domain NetBIOS name:	SECUREWAY7	_

You may see this dialog. Click Next.

Active Directory Installation Wizard	×
Database and Log Locations Specify the locations of the Active Directory database and log.	Se la companya de la
For best performance and recoverability, store the database and the lo hard disks.	g on separate
Where do you want to store the Active Directory database?	
Database location:	
C:\WINNT\NTDS	Browse
Where do you want to store the Active Directory log?	
	Dama I
C. WINNENT DS	Browse

Take the defaults for the database and log locations, and click Next.



Take the defaults for the Shared System Volume folder location and click Next.



The DNS server is not yet available and configured, so just click OK.



Accept the default to configure the DNS and click Next.

Active Directory Installation Wizard
Permissions Select default permissions for user and group objects.
Some server programs, such as Windows NT Remote Access Service, read information stored on domain controllers.
Permissions compatible with pre-Windows 2000 servers Select this option if you run server programs on pre-Windows 2000 servers or on Windows 2000 servers that are members of pre-Windows 2000 domains.
Anonymous users can read information on this domain. Permissions compatible only with Windows 2000 servers
Select this option if you run server programs only on Windows 2000 servers that are members of Windows 2000 domains. Only authenticated users can read information on this domain.
< Back Next > Cancel

Accept the default permissions and click Next.



Enter "passw0rd" twice and click next.

IBM Tivoli Access Manager 3.9 - Cookbook



Review the summary and click Next. Wait while the configuration process runs.

Active Directory Installation	Wizard	×
	Completing the Active Directory Installation Wizard	
	< Back Finish Cancel	

Congratulations! You've installed Active Directory. Click Finish.

46.6 Installing Domino Server

Domino Server Configuration Options

Install the Domino Server 5.0.9 on Windows 2000 Server using the defaults. It installs the package into *C:\Lotus\Domino* and creates a menu in the "Start-Menu:"

Start -> Programs -> Lotus Applications -> Domino

In order to configure Domino Server and run it with Policy Director it is necessary to have these components installed: Lotus Domino Server Lotus Domino Administrator (usually, but not necessarily, a part of the Lotus Notes Client package) Lotus Notes Client (usually part of the Lotus Notes Client package)

Basic Configuration of Domino Server

Run Start -> Programs -> Lotus Applications -> Domino -> Lotus Domino Server.

.damiwa	1234	Save & Quit
	This 4-step server configuration tool will assist you in configurir Advance through the screens with the > (next) button. Back	ng your Domino server. up with the
and the A	1. Create a New Domino Server	Quick Help
Welcome to	Is this the first or additional Domino server?	First Domino
Domino	First Domino Server	Select this option if this
Server Setup	O Additional Domino Server	are setting up in your organization, or if you are creating a new domain.
		Additional Domino Server Select this option if this is a new server which has already been defined in an existing organization. You will only need to supply a few ken pieces of
	I	information.

Select First Domino Server and click the right-arrow button. For the purposes of a test installation it is sufficient to choose "Quick and Easy Installation" and to leave the check boxes in the 3rd screen unchecked.

On the 4th screen click Edit to set passwords.

Quick and Easy - E	dit					×
4.Quick and Ea	asy Configuration - A	dministration Se	ettings - Edit			
After making char	iges, click the OK buttor	n to accept cha	anges.			<u> </u>
To disregard any o	changes, click the Canc	el button.				Cancel
- For Help , click (on the item's label. For b	etter securit	y , please provide your	own passw	ords.	
Organization Ide	ntity:					
Domain Name:	[₽] secureway _]				Required	
Certifier Name:	P secureway				Required	
Certifier ID:	Create new certifier ID)			Required	
	O Use existing certifier I	D				
Certifier Password:	₽passw0rd _				Required	
New Server Iden	tity:					
Server Name:	[™] secureway5 _]				Required	
Server's Hostname:	[™] secureway5 _]			T	Required	
Server ID:	Create new server ID			1	Required	
	O Use existing server ID					
Administrator's	Identity:					
Administrator's Name:	First:	M.L: P	Last: ©oleg _		Required	
Password:	[™] passw0rd _1				Required	
Administrator's ID:	Create new administr	ator ID			Required	
	O Use existing administ	rator ID				
Communication	s Port Options					
Serial Port:	r -None- এ				Setup	
Modem:	🖗 . Auto Configure (for un	listed modems o	nly) 🗾 💌		Script	

Enter passw0rd twice, and fill in other required parameters and note them for the future use.

Domain Name:

IBM Tivoli Access	Manager 3.9 -	Cookbook
-------------------	---------------	----------

Certifier Name (the same as Domain Name):	
Server Name:	
Server's Hostname (the same as the Server Name):	
Administrator's Name:	

Important: The Domain Name, Certifier Name, Server Name, Server's Hostname as well as Administrator's Name should be yours.

Click OK. Then click Finish.

Configure Access Control Lis	ts
You can add an entry with Mana templates which were installed o 'Anonymous' to the Access Cont accessing your server via the Int	ager access to the Access Control List for all databases and r created by configuring your server. You can also add rol Lists with No Access. This will prevent anonymous users ernet or via Notes from opening databases or templates.
It is recommended that the entry	you add is a group since it offers the greatest flexibility.
Note: If you add a group, it will b name will be listed as a member.	be created in the Directory automatically and the administrator's
Set Access Control List Entry	

Note the location of the ID files created during the configuration of the Domino Server. By default they are located in *C:\Lotus\Domino\Data*. You can prohibit anonymous access to the Domino Server resources by setting an ACL. Click on the button "Set Access Control List Entry" and check the appropriate checkbox.

The Domino configuration will finish. Click Exit. The Domino Server process will start. You can also start it manually at any time by running

Start -> Programs -> Lotus Applications -> Domino -> Lotus Domino Server

A healthy Domino Server provides console output like this:

🛃 Lotus Domino Server: secureway5/secureway	
Lotus Domino ® Server, Release 5.0.9a , January 7, 2002 Copyright © 1985-2002, Lotus Development Corporation, All Rights Reserved 06/02/2002 12:48:09 Server started on physical node SECUREWAY5 06/02/2002 12:48:09 Informational: The registry value HKEY LOCAL MACHINENSUStem/CurrentControlSet/Control/Session Manager/Memory 06/02/2002 12:49:08 Database Servery started	
>	-

The LDAP server (in Domino, the LDAP task) does not start automatically by default. To start the LDAP task manually issue this command from the Domino Server console:

>load ldap

To set the LDAP task to autostart, modify notes.ini located in C:\Lotus\Domino.

🖉 notes.ini - Notepad	_	
File Edit Format Help		
NAMEDSTYLE2_FACE=Default Sans Serif DefaultMailTemplate=mail50.ntf ServerTasks=Router,Replica,Update,Amgr,AdminP,CalConn,Event,Sched,St ServerTasksAt1=Catalog,Design	ats,maps, <mark>ld</mark>	
↓		

Configuration of Domino Administrator

To manage Lotus Domino you need to install and configure Lotus Domino Administrator. In this section, the Domino Administrator client application. In this section, the example Domino administrator user account name is "oleg." The application is usually, but *not necessarily*, a part of the Lotus Notes client package.

To configure Lotus Domino Administrator run

Start -> Program Files -> Lotus Applications -> Lotus Domino Administrator

This will present a number of dialog windows, where you choose the following:

I want to connect to a Domino server, and Set up a connection to a local area network (LAN)

Domino server name	
secureway5/secureway	

Domino server name:

<Server name>/<Domain name>

•	Use my name as identification.	
	User name	
	oleg	

Use a name as identification. User name:

<Administrator's name>

Domino server name	
secureway5/secureway	
If the server name above is network information to help	correct, please provi locate this server.
TCP/IP	•
Server address (for example	e host name or IP add
secureway5	

If Domino server could not be contacted, fill in the server name or IP address manually in the window (this option may not appear). Click Next after each of these.

After the connection to a Domino server is set up, the client connects to the Domino server and retrieves the ID file of the administrator. You will be prompted for the password to logon as the administrator (user ID that was filled in in the previous step, e.g. "oleg").

Configuring Lotus Domino Server to Run with Policy Director

Domino Administrator	_ 🗆 🗵
File Edit View Create Actions Administration People Help	۴
Administration 🛛 🖄 Welcome to Domino Administrator R5	administrator
😰 💌 SECUREWAY Domai 🛓 Messaging Replication Configuration	
Image: Secure way5/secure way ay Image: Secure way5/secure way) Image: Secure way5/secure w	✓ Tools > People > Groups

Modify Domino LDAP configuration

You may want to modify the LDAP configuration of the Domino LDAP server. If you have configured Active Directory, it always listens on port 389, and so does Domino LDAP by default. It is easier to modify the port used by Domino LDAP, rather than AD.



Change the TCP/IP port number to 3890, the port you will use for Domino throughout the labs. Apply the change by restarting the Domino LDAP task using the Domino Server Console:

```
> tell ldap quit
> load ldap
```

Modify Domino HTTP Server Configuration

You may want to modify the HTTP server configuration that is set to autostart by default. The SSL port is disabled by default, so it does not need to be modified.

Basics	Security Ports Serv	ver Tasks Internet Protocols M
Note	s Network Ports] Interne	et Ports Proxies
SS	L settings	
SS	L key file name: 👘 🦻	keyfile.kyr_n
SS with HT	L protocol version (for use h all protocols except TP):	Negotiated
Ace	cept SSL site certificates: () Yes 🖲 No
Aci	cept expired SSL 🤇 🕅	🖲 Yes 🔿 No
We	eb Directory News	Mail IIOP
	SSL ciphers:	RC4 encryption with 128-bit key and MD5 MAC RC4 encryption with 128-bit key and SHA-1 MAC Triple DES encryption with 168-bit key and SHA-1 MAC
3	Enable SSL V2: (SSL V3 is always enabled)	T Yes
		Web (HTTP/HTTPS)
	TCP/IP port number:	⁶ 8000 ₈₁
	TCP/IP port status:	Enable
-	Authentication options:	
1	Name & password:	ſYes▼
1	Anonymous:	r Yes⊿ ▼
_	SSL port number:	₽ 443. ₁
1	SSL port status:	

Set the TCP/IP port number to 8000 and restart the HTTP task using the Domino Server Console:

```
> tell http quit
> load http
```

Configure the PD Privileged User in Domino

In order to give Policy Director the authority it requires to configure itself in the Domino domain, a user must be created in the Domino environment. This user, whom we will call the PD *Privileged User*, must be configured before Policy Director configuration is started.

The PD Privileged User identity is used during configuration. All Policy Director servers also use this identity in order to access the Domino environment – this is different from an LDAP environment where each server has its own identity to access the registry.

To create the PD Privileged User, use Lotus Domino Administrator (GUI).



Navigate to the Domino server, go to the "People & Groups" tab and right click on the People object in the domain's Address Book (there also may be the personal Address Book, we don't want use that). Select "Register Person..."

You may be asked for the ID file of the certifier (essentially the Certification Authority in Domino).

Administration 🛛 🖄 Welco	ome to Domino Administrator R5
People & Groups Files Se	erver Messaging Replication Configuration
Server: secureway5/sec	ureway
🔻 🛈 Domino Directories	Choose Certifier ID
♥ 1 secureway's Addres ▲ People	s Bo Look in: 🔁 Data 💽 🔶 🖽 🕬
👬 Groups 🥩 Mail-In Databas 🔝 Setup Profiles 🗟 Certificates 👬 Deny Access Gro	a doc a W32 a domino a cert.id belp a dolcert.id iNotes a server.id a mail bups modems
	File name: Dent.id
	Files of type: ID Files Cancel
	Help
	04/02/2002 19:47:50 1909 bytes

Find the ID file in *C*:*Lotus**Domino**Data*. The password for this ID file corresponds to Certifier Password provided for the Organisation Identity (4th step while configuring Domino Server – see earlier screenshot). Click Open.

A 🖌	First name	MI	Last name	Short name
asics	PD		Daemons	PDaemons
<u> </u>	Password		Password 0	Quality Scale
	passw0rd	w	eak 🗍 🗕 🚽	Strong
Mail	🔲 Set internet p	assword	Password is opti	onal (0)
	Internet address		Internet Demain	
) Info	Internet address			Format
00				1 with which
\mathbf{n}	- C		9	
	The Internet add	lress (above) i	s created using the pe	rson's name (above),
roups	The Internet add the internet dom edit the internet a	lress (above) i ain and interne address direct	s created using the pe at address format com y. It must be unique i	rson's name (above), ponents. You can also n the address book.
roups	The Internet add the internet dom edit the internet d	Iress (above) i ain and interne address direct	s created using the pe et address format com y. It must be unique in	rson's name (above), ponents. You can also n the address book.
roups	The Internet add the internet doma edit the internet a	Iress (above) i ain and interne address direct person	s created using the pe et address format com y. It must be unique in Import Text file	rson's name (above), ponents. You can also n the address book.
istration queu	The Internet add the internet dom edit the internet d Add ; e:	Iress (above) i ain and interne address direct person	s created using the pe t address format comy y. It must be unique ii Import Text file Status	rson's name (above), ponents. You can also n the address book. Migrate people.
Dither istration queu	The Internet add the internet dom edit the internet a Add r e: e	Iress (above) i ain and interne address direct person Registration	s created using the pe t address format com y. It must be unique in 	rson's name (above), ponents. You can also n the address book. Migrate people.
Inter Sither Inter Istration queu	The Internet add the internet dom edit the internet a Add r e: e	ress (above) i ain and interne address direct person Registration	s created using the pe t address format comm y. It must be unique in 	rson's name (above), ponents. You can also n the address book. Migrate people.
Toups Toups Differ istration queu User Nam	The Internet add the internet dom edit the internet a edit the internet a Add p e: e	tress (above) i ain and intern address direct person Registration	s created using the pe t address format com y. It must be unique in 	rrson's name (above), ponents. You can also n the address book. Migrate people.

Fill in the basic information about the new user as shown. The name of the PD Privileged User is not restricted – it can be anything that is valid in Domino. In this example, PDaemons is the identity of Policy Director in Domino.

To disable Mail for that user, click on the Mail button.

Register Person PD Daemons	?×
Advanced	Mailsystem:
Basics	None ▼

Select None in the Mail system drop-down. Then click the ID Info button.

Register Pers	on PD Daemons			?×				
Advanced	Certifier ID infor	nation						
លិ	Certifier ID) /secureway						
Basics	Security type Certificate expiration date							
North American 05/02/2004 09:20:35								
Mail	Mail Location for storing user ID							
	🔽 In Domino di	rectory						
ID Info	🔽 In file: C:\Lo	tus\Notes\Data	vids\people\pdaemons.id					
ជំរំ	Sel	ID File						
Groups								
S								
Other	Add	person	Import Text file	Migrate people				
Registration qu	ieue:	N2.						
▲ User N	ame 🔺	Registration St.	atus 🔺 I	Date				
	1							
Register All	Register	Delete	Options	Done				

Select the option to save the ID file to disk and put the registration into the queue. Click the "Add person" button.

User Name		Registration Status	 Date
Daemons , I	PD	Ready for registration	05/02/2002 09:27
 •			

Next register the user by pushing the "Register All" button.

The PD Privileged User requires Manager access (including delete) to the domain NAB. To grant this user the permissions, navigate to the "Files" tab. (You were previously in the "People & Groups" tab.)

Administration	🖄 We	elcon	ne to l	Dom	iino Administrator R5						adm	ninistrator			
People & Groups	Files	Sen	/er	Mes	saging Replication C	Configuration									
Server: secure	eway5/s	secu	reway	•				Show me	Databases only	•	→ Tools				
🔝 🗁 C:\Lotus\Dorr	nino\Dat	ta	1	•	Title 🔺	Filename 🔺	Physical Path 🔺	File Format 🔶	Size 🔺	Max Size		Disk Space			
🗀 doc			1		Administration Requests (R	admin4.nsf	C:\Lotus\Domino\Data\	R5 (41:0)	838,656	Nol	/				
🕨 🗀 domino					Java AgentRunner	agentrunner.nsf	C:\Lotus\Domino\Data'	R5 (41:0)	393,216	Nol	\rightarrow Ca	Folder			
D help				Q.	bookmark.nsf	bookmark.nsf	C:\Lotus\Domino\Data\	R5 (41:0)	1,520,640	Nol	-				
C iblates				Q.	Local free time info	busytime.nsf	C:\Lotus\Domino\Data\	R5 (41:0)	327,680	Nol	V V	Database			
				Š.	Catalog (R5)	catalog.nsf	C:\Lotus\Domino\Data'	R5 (41:0)	1,350,144	Nol	Manago				
🛄 mail				Ő.	Server Certificate Admin	certsrv.nsf	C:\Lotus\Domino\Data'	R5 (41:0)	1,184,256	No I	manage	······································			
🛄 modems	IS	0000	Š	Domino Server. Planner Sar	cpa.nsf	C:\Lotus\Domino\Data\	R5 (41:0)	2,883,584	Nol	Create R	eplica(s)				
🗀 W32				Š	l 🗳	l 👗	Statistics & Events	events4.nsf	C:\Lotus\Domino\Data'	R5 (41:0)	7,077,888	Nol	Compact		
					8	homepage	homepage.nsf	C:\Lotus\Domino\Data'	R5 (41:0)	458,752	Nol	Full Text	Index		
			Š	Š		Š	Notes Log (secureway5/se	log.nsf	C:\Lotus\Domino\Data'	R5 (41:0)	663,552	Nol	T GILT FOR		
											Š	Lotus MTA Tables (v1.7)	mtatbls.nsf	C:\Lotus\Domino\Data'	B3 (17:1)
				Š	secureway's Address Book	names.nsf	C:\Lotus\Domino\Data	R5 (41:0)	5,242,880	Nol	Advance	d Properties			
				Š	Reports for secureway5/se	reports.nsf	C:\Lotus\Domino\Data'	R5 (41:0)	944,640	Nol	Quotas				
				Š	secureway5 Stats/securew	statmail.nsf	C:\Lotus\Domino\Data ^v	R5 (41:0)	6.029.312	Nol					
				Š	Statistics Reports	statrep.nsf	C:\Lotus\Domino\Data	R5 (41:0)	838.656	Nol	Move				
				100							Sign				
											Replicati	on			
											Fixup				
											Cluster				
											Analyze.				
											Find Note	e			

Highlight your domain's Address Book, and select "Manage ACLs" from Tools. In the next dialog click "Add" under the list of People, Servers, and Groups.

Basics Basics Roles Log	-Default- Administrators Anonymous ILocalDomainServers Image: oleg/secureway Image: OtherDomainServers Image: OtherDomainServers Image: Secureway5/secureway Image: Secureway5/secureway	Access: Author Create documents Create documents Create personal agents Create personal folders/views Create shared folders/views Create LotusScript/Java agent Read public documents Write public documents Roles: [GroupCreator] [GroupModifier] [NetCreator] [Author The start of t
Advanced	Full name:	
Unsigned		OK Cancel Help
	Add User Person, server, or group:	

Then select the PD Privileged User from the Domain Address Book by clicking the small Person button.

 Administration Requests Administrators Daemons, PD LocalDomainServers oleg OtherDomainServers secureway5 Stats/secureway secureway5/secureway 	Add > Open New	
Copy to Local Address Book	Remove	Remove All

Click on the "Add" button, then OK on the Names dialog, and then OK again on the small Add User dialog.

٠		Access:	Author	-
Basics	-Detault- Administrators Anonymous LocalDomainServers oleg/secureway OtherDomainServers PD Daemons/secureway PC Daemons/secureway	Create docu Manager Delete doci Designer Create pers Author Create pers Author Create shar Create shar No Access Read public documents Write public documents Roles:		
Advanced	Add Rename Remove	[NetModif [ServerCr [ServerMo	ïier] eator] odifier]	•

Grant the Administrator user Manager access level as shown. After you select Manager make sure all the Access: checkboxes are checked. Click OK. Domino is now ready to host PD.

47. Appendix B -- WebSphere Installation

47.1 Prerequisites and Preparations

In order to successfully install WebSphere 4.02, verify that you already have the prerequisite software installed and configured. (In these labs we need latest GSKIT, currently 5.0.56 and DB2 7.2 FP4.) In case you have not updated the DB2 drivers to JDBC 2.0, do so following the instructions provided in section 46.3 Configure DB2 to use JDBC 2.

Before proceeding with the installation it is good practice to stop all Web servers you want to configure with WebSphere. In the labs you will use IBM HTTP Server. To stop it run

```
Start->Programs->IBM HTTP Server->Stop HTTP Server
```

47.2 Procedure

Use Windows Explorer to D:\Lab Setup\WAS402WIN and launch setup.exe. Accept English as installation language and continue until you are asked to choose the installation option. Select a Custom Installation. Click Next.

Select the components you want to install, clear the c want to install.	omponents you do not
Application and Administrative Server	31250 K
Administrator's Console	488 K
Application and Development Tools	488 K
Samples	488 K
Webserver Plugins	4 K
BM JDK 1.3.0	41015 K
IBM HTTP Server	οĸ

Choose to install all components except the IBM HTTP Server, previously installed. Click Next.



Select the IBM HTTP Server as the Web server to use with WebSphere so that the proper plug-in is installed. Click Next. When asked to specify a username and password for starting the services use *Administrator* and *passw0rd*. Accept the default installation folder *C*:*WebSphere**AppServer* unless you have some other reason to change it.

IBM WebSphere Application Serve	er uses a database repository to store information. Indicate	×
the type and name of the database and password for the database.	e you would like to use, along with the location, user name,	
Database Type	DB2 Remote Database	
Database Name	was40	
Database User ID	db2admin	
Password	XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	
Path	C:\Program Files\SQLLIB Browse	
URL		
Server		
Port		
	(Back Naut) Cancel	

Enter db2admin and passw0rd for the Database User ID and Password and fill in the other fields as shown.

Accept the default for creating a Program Folder and click on Next until the installation starts to copy all the files. When it completes accept to restart the machine.

After rebooting the machine the DB2 database *was40* is created and it will takes some minutes to complete initialization.

If everything is fine a "First Steps" control window appears, and from there you can start the Administrative Server. You can also start it with

Start->Programs->IBM WebSphere->Application Server V4.0 AE->Start Admin Server

or from the Services console by starting IBM WS AdminServer 4.0.

47.3 Configuring and Testing Your WebSphere Installation

After the server is started you can launch the Administrator's Console either using The First Steps window or in the following way:

Start->Programs->IBM WebSphere->Application Server V4.0 AE->Administrator's Console

Depending on the power of your machine, the console can take some seconds before it appears, so be careful not to launch multiple consoles. Just be patient for a few moments!

On the Admin Console select expand WebSphere Administrative Domain. Click on Virtual Hosts.

🚏 WebSphere Advanced Administrative Co	onsole
<u>C</u> onsole ⊻iew <u>T</u> ools <u>H</u> elp	
🖻 🍿 WebSphere Administrative Domain	Name
Virtual Hosts	🔚 default_host (*:8888,*
Server Groups	
Enterprise Applications	
E Resources	
	General Advanced
	Name: *default_host
	Aliases
	*Host Aliases Add
	*9080 Bomovo
	*:4444

Change the host alias from *:80 to *:8888 (use colons, not periods), the port on which your IBM HTTP Server is listening. Add a new host alias of *:4444. This will be for SSL access. Apply to make change to be effective. In general, when using the Admin Console, don't forget to click Apply to effect a change.

After this change you need to regenerate the Web server Plug-In.



Expanding Nodes and right-click on your *hostname* node. Select Regen Webserver Plugin. You will not receive a confirmation dialog for this, but there will be an event message in the message log box at the bottom of the screen.

From the Windows Services dialog, restart the IBM HTTP Server service to reload the new Web server plug-in.

In the WebSphere Admin Console, expand your hostname node, then Application Servers and you'll see the Default Server.



You can start it with a right-click and selection Start, or you can start by selecting it normally and then clicking on the green -> button in the button bar. Start the Default Server.

If it starts successfully you'll receive a confirmation message and next to the server's icon there will be a small green icon with an arrow.

The configuration is now complete. To check that is everything is working fine, open your browser and point it to <u>http://yourhost:8888/webapp/examples</u>. You should see a page with all the examples. If so, you have successfully installed WebSphere. Congratulations.

48. Appendix C -- Manual Installation of PD Web Portal Manager

48.1 Manually Installing PD WPM into WebSphere

This section is here for reference. This will normally be done in the labs using a BAT file. But if you would like to install the PD WPM manually, here are the instructions.

Considerations

This section describes how to install PDWPM into WAS manually using the WAS Admin Console application. You will still need to run the Configure... command in the Policy Director Configuration dialog because that adds the necessary stanzas to *httpd.conf*.

Procedure

Select Policy Director Web Portal Manager and click Configure ... to setup the IBM HTTP Server's httpd.conf file.

The Web Portal Manager is a Web application and does not use EJBs.

Start the WAS Admin Server by running Start->Programs->IBM WebSphere->Application Server V4.0 AE->Start Admin Server. (Note that you can also start the Admin Server from the Services window by running IBM WS AdminServer 4.0.) A DOS window will open and display messages as the Admin Server starts.

Next, start the WAS Admin Console by running Start->Programs->IBM WebSphere->Application Server V4.0 AE->Administrator's Console.

IBM Tivoli Access Manager 3.9 – Cookbook

Cone:	WebSphere Advanced Administrative Console						
	Western and a server servers Generic Servers Generic Servers Generic Servers Resources			Installed EJB Modules Installed Web Modules General Advanced File T Application Server name: Node: Environment: Working directory: Node startup state: Maximum startup attempts: Module visibility:	Name Transaction JVM Settings Ser Default Server Secureway7 Environment C::WebSphere/AppServer/bin Last state 2 Application	rices Custom	
•			Þ	_	<u>Apply</u> <u>R</u> eset	Help	
Туре	Time		Eve E: Sorviction	ent Message seke file dvinaceske vml net fau	Source	Options	
3	06/02/02 19	SRVE0169	L: Loading V	/eb Module: Default Application.	com.ibm.servlet.engine.Servl	Details	
3 3	06/02/02 19 06/02/02 19	Command SRVE0169	"Default Se I: Loading V	rver.start" completed successf /eb Module: Examples Applica	com.ibm.servlet.engine.Servl	Clear	

Expand WebSphere Administrative Domain, Nodes, <your host name>, and Application Servers. If there is a red X next to the Default Server instead of a green arrow, select the Default Server and click the green Start button as shown above. Click OK on the dialog that confirms starting the Default Server.

Test that WAS is running properly by opening Netscape (Netscape must be setup to not use a proxy for local addresses, etc.) or preferably IE and entering *http://localhost:9080/servlet/snoop*. You should see the output of the Snoop Servlet.

🔆 Snoop	Servlet -	Netscape							_ 🗆 🗵
File Edit	View Go	Communicator	Help						
aci Baci	Forwa	ard Reload	🔬 🥔 Home Sear	ch Netscape	a Print	💕 Security	🔕 Shop	3 Stop	N
T 💉	Bookmarks	🮄 Location:	http://localhost:9	080/servlet/sno	юр		-	👘 🐪 Whal	's Related
Sno Requ	oop S uested	Servle	t - Req	uest/	Clie	nt In	forı	nati	on [
Serv	let N:	ame:							
Serv	let In	itializati	on Para	meters	(
Param	1	100							
param	1	tes	i-value I						-
•									
a -		Documer	nt: Done			- E 🐝	🤸 📇 😸		炎 🕺

The port is 9080 because it is the port for WebSphere's own embedded Web server. Using the embedded Web server allows you to bypass the added complexity of a standalone Web server. Now to install Web Portal Manager....

	😭 WebSphere Advanced Administrative Console							
	<u>C</u> onsole <u>V</u> iew <u>T</u> ools <u>H</u> elp							
		S -						
	😑 🍿 WebSphere Administrative	Instal	Enterprise Applicati	on				
	🗖 Virtual Hosts	<u>C</u> reat	Application Server	14				
l	🗖 Server Groups	Creat	Create Server Group					
	🖻 🛄 Nodes	Creat						
I	🖃 💓 Secureway7	Creat	JMS Resources					
	Application Serv	Creat	ctory					
		Creat	Transac					
		Porfor						
	Generic Servers	eno			∬ [™] Defa			
	Enterprise Applications		Node:		Secu			
	🗄 🖽 Secureway7_sampl	eApp	Environment:					
	🗄 🛅 Resources		Environment.		E			
			Working directo	w.	0.40			

Click on the toolbar button on the right and select Install Enterprise Application. Next click Browse for the Install Application (*.ear) Path:.

		×
📄 pdwpm 💽	E	<u>*</u>
Program Files		
Policy Director		
🧰 java 💼 export		
🚞 pdwpm 🔊 D()		
pdwpm.ear		<u>Open</u>
JARS/WARS/EARS (.wa	r, ear, jar) 💌	<u>C</u> ancel
	pdwpm C1 Program Files Tivoli Policy Director java powpm D1 pdwpm.ear JARS/WARS/EARS (.wa	pdwpm ♥ C \ Program Files Tivoli Policy Director java export pdwpm D \ JARS/WARS/EARS (.war, ear, jar) ▼

Navigate as shown, select pdwpm.ear, and click Open.

🎁 Install Ente	erprise Application Wizard	<u>_ </u>
Specifying Specify If you in	the Application or Module the application(EAR file) or module(JAR or WAR file) that you want to insta stall a stand-alone module, you must specify a new application name.	all.
ii 🗗		
	Browse for file on node: *Secureway7	-
	Install Application (*.ear)	
	Path: */ Director/java\export\pdwpm\pdwpm.e Application name:	ar Browse
	○ Install stand-alone module (*.war, *.jar)	
	Path:	Browse
	Application name: Context root for web module:	
Help	< Back Next > Einish	Cancel

Click Next.

Click Next on the **Mapping Users to Roles** dialog. Click Next on the **EJB RunAs Roles to Users** dialog. Click Next on the **Binding Enterprise Beans to JNDI Names** dialog. Click Next on the **Mapping EJB References to Enterprise Beans** dialog.

Click Next on the **Specifying the Default Datasource for EJB Modules** dialog. Click Next on the **Specifying Data Sources for Individual CMP Beans** dialog. Click Next on the **Specifying Data Sources for Web Modules** dialog. Click Next on the **Selecting Virtual Hosts for Web Modules** dialog. Click Next on the **Selecting Application Servers** dialog. (Your host should be specified.) Click Finish on the **Completing the Application Installation Wizard** dialog after reviewing it. Click OK on the EnterpriseApp.Install completed successfully dialog.

Return to the Admin Console.



Right mouse click on your hostname node and select Regen Webserver Plugin. This will add the new application to *C:\WebSphere\AppServer\config\plugin-cfg.xml*, the file used by the Web server plug-in to determine whether a request should be sent to WebSphere.

The plug-in must now be reloaded by the Web server. From the Windows Services dialog, stop and restart the IBM HTTP Server.

49. Appendix D Banker 2001 Installation

49.1 Loading the Banker 2001 Application into Websphere

Importing the Application

In order to import the Banker2001 application into WebSphere it is be necessary to perform some operations manually. Because this application simulates a true banking environment it is necessary to create a DB2 database and tables for it. After doing this it is necessary to load the file *Banker2001.ear* into WebSphere and to regenerate the plug-in for your HTTP server so that your system is ready to run.

In order to automate all these steps there is a batch file that does all this good stuff for you. Before proceeding, make sure WebSphere is running, and use Windows Explorer to navigate to *D:\LabFiles\Banker2001*. Double-click on *setupBK2001.bat*.

The batch file will open another DOS shell and prompt you to continue for each sub-operation it is going to run. Of course monitor the proceedings and verify that each step completes successfully.

Don't worry if a window like the following shows you a warning about Restore, just proceed, and close it when the task has ended.



If everything goes fine an "installation completed" message will inform you of the end of the import procedure, and will remind you that the Banker 2001 application must be started in the WebSphere Admin Console.

Remember to restart the IBM HTTP Server service.

Starting and Testing the Application

To start the application open the WAS Admin Console as follows:

Start>Programs->IBM WebSphere->Application Server V4.0 AE->Administrator's Console

On the Admin Console expand the Enterprise Applications folder.



Right click on the Banker 2001 application and start it.

To check if everything is working point your browser to <u>http://yourhost:8888/Banker2001</u> and click on the View Balances link.

View Account Balances		
Account Number		
1		
Balance		
Get Balance		

Be a little bit curious and get the balance for account number 1. Can the account 1 owner buy a round for everyone?

Part VII - Additional Information

50. Publications

The majority of these publications should be read **before** reading this document! The Access Manager technical documentation can be found at

http://www.tivoli.com/support/public/Prodman/public_manuals/td/TD_PROD_LIST.html (which includes a link to the support pages for registered users). For internal users, 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 Access Manager 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.

Highly recommended at the **Access Manager Field Guides** – they are available for download from this internal site: http://www-

internal.tivoli.com/secure/support/documents/fieldguides/tech_info.html and (for registered users) from this external site:

https://www.tivoli.com/secure/support/documents/fieldguides/tech_info.htm 1

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

WebSphere

There's lots of useful information on WebSphere Application Server Advanced Edition at http://www.ibm.com/software/webservers/appserv/doc/v40/ae/infocenter/ and
on WebSphere Application Server Advanced Edition Single Server Edition at
http://www.ibm.com/software/webservers/appserv/doc/v40/aes/infocenter/.

and the WebSphere red books:

SG24-6176IBM WebSphere V4.0 Advanced Edition HandbookSG24-6520IBM WebSphere V4.0 Advanced Edition Security

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